ROSETTA STONE DATA PROCESSING ADDENDUM

This Data Processing Addendum (this "**DPA**") forms part of the order document(s) (each a "**Service Order**"), and the Enterprise License and Services Agreement for the Rosetta Stone products and services, and Services Agreement (collectively, the "**Agreement**"), entered into between the Customer named in the Agreement ("**Customer**") and Rosetta Stone LLC, or its subsidiary or affiliate named in the Agreement ("**Rosetta Stone**") (each a "**Party**", together the "**Parties**"), pursuant to which Customer has purchased subscriptions to Rosetta Stone's online, web-based subscription products and ancillary services (the "**Services**"), as further specified in the Agreement. The purpose of this DPA is to reflect the Parties' agreement with regard to the Processing of Customer Personal Data by Rosetta Stone as Processor on behalf of Customer and in accordance with Customer's instructions as Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. DEFINED TERMS

"Controller" means the entity that determines the purpose and means of Customer Personal Data Processing.

"Customer Personal Data" means any Personal Data received by Rosetta Stone from Customer relating to Customer's users authorized by Customer to use the Services ("Authorized End Users").

"**Data Protection Laws**" means: when applicable (i) the Regulation (EU) 2016/679 of the European Parliament and of the Counsel of 27 April 2016 ("GDPR"); (ii) the data protection laws of the relevant territories of the United Kingdom; (iii) the Swiss Federal Data Protection Act; (iv) any and all applicable national data protection laws made under or pursuant to (i), (ii), or (iii) in each case as may be amended or superseded from time to time; and (v) any other applicable national, state, or provincial data protection laws or regulations, including but not limited to the California Consumer Privacy Act (CCPA) and the Brazil General Personal Data Protection Law (LGPD).

"**EU Model Clauses**" means the Commission Implementing Decision (EU) 2021/914 establishing Standard Contractual Clauses for data transfers to Third Countries. For purposes of this DPA, the applicable modules within the EU Model Clauses are MODULE TWO (Transfer Controller to Processor) and/or MODULE THREE (Transfer Processor to Processor). For the avoidance of doubt, neither MODULE ONE (Transfer Controller to Controller) nor MODULE FOUR (Transfer Processor to Controller) shall apply to this DPA.

"Personal Data" means any information relating to an identified or identifiable natural person (also referred to as a data subject).

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

"Processor" means the entity Processing Personal Data on behalf of a Controller.

"Sub-Processor" means the entity appointed by or on behalf of a Processor to Process Personal Data on behalf of a Controller.

2. SAAS-BASED SERVICES DELIVERED BY ROSETTA STONE

a. The Parties agree that the Services are publicly available offerings of Rosetta Stone's SaaS-based subscription service and are provided in a multi-tenant, shared-database architecture and that individualized client-dedicated infrastructure and/or Processing is not part of the Services. Customer understands and agrees that user information, including Personal Data, is stored by Rosetta Stone in centrally organized data center facilities, for which client-dedicated user environments are achieved through logical segregation within a shared client infrastructure.

b. The Parties agree that, regardless of jurisdiction, the categories of data subjects and Personal Data to be Processed are as described in Appendix A of this DPA and the Processing shall be as required to provide the Services.

3. CUSTOMER'S OBLIGATIONS

a. Customer remains the responsible Controller (or similar term under Data Protection Laws) for the Processing of the Personal Data subject to this DPA as instructed to Rosetta Stone. Customer agrees that its provision of Personal Data to Rosetta Stone and its instructions to Rosetta Stone related to the Processing of Personal Data shall at all times be in compliance with all Data Protection Laws, in particular with any notice and/or consent requirements.

b. Notwithstanding anything to the contrary in the Agreement and as a supplement to, and not in

contradiction of the EU Model Clauses, Customer shall remain responsible for and protect, indemnify, defend, and hold harmless Rosetta Stone from any and all damages, losses, fees or costs incurred as a result of any third party claims or enforcement actions related to Rosetta Stone's Processing of Personal Data in accordance with Customer's instructions.

c. Customer shall not transfer or permit to be transferred to Rosetta Stone any sensitive Personal Data (i.e., social security number, tax identification number, end user financial information, or Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, health or medical data, or data concerning a natural person's sex life or sexual orientation).

4. ROSETTA STONE'S OBLIGATIONS

a. Rosetta Stone shall Process the Customer Personal Data on behalf of Customer, in compliance with Data Protection Laws and only for the purpose of fulfilling its obligations and to perform its Services under the Agreement or as otherwise instructed in writing by Customer, which instructions are defined in the Agreement and applicable order documents agreed to by the Parties, in accordance with the terms of this DPA.

b. With respect to the Customer Personal Data transferred to or received by Rosetta Stone under the Agreement, Rosetta Stone has implemented, and shall maintain, a written information security program that includes technical, organizational, and physical security measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, and unauthorized disclosure or access, as further outlined in Appendix B to this DPA.

c. Rosetta Stone shall notify Customer in writing immediately upon making a determination that it has not met, or can no longer meet, its obligations under Section 4(a) of this DPA, and, in such case, will abide by Customer's written instructions, including instructions to cease further Processing of the Customer Personal Data, and take any necessary steps to remediate any Processing of such Customer Personal Data not in accordance with Section 4(a) of this DPA. To the extent further costs are involved in abiding by Customer's instructions, the terms of Section 4(g) shall apply.

d. As required by Data Protection Laws, Rosetta Stone shall immediately inform Customer if, in its opinion, an instruction infringes Data Protection Laws.

e. To the extent legally permitted, Rosetta Stone shall promptly notify Customer if it receives a request for any Customer Personal Data from a court, government agency, law enforcement agency, or other authority, and will direct the court, government agency, law enforcement agency, or other authority to request such information directly from Customer. As part of this effort, Rosetta Stone may provide Customer's basic contact information to facilitate this communication. Notwithstanding, if Rosetta Stone is compelled to disclose Customer Personal Data, Rosetta Stone will promptly notify Customer and deliver a copy of the request (except where Rosetta Stone is legally prohibited from doing so) to allow Customer to seek a protective order or any other appropriate remedy.

f. Rosetta Stone maintains security incident management policies and procedures and shall, to the extent permitted by law, promptly notify Customer of any unauthorized disclosure of Customer Personal Data by Rosetta Stone or Rosetta Stone Sub-Processors of which Rosetta Stone becomes aware.

g. With respect to requests for audits or other additional instructions by Customer, unless otherwise expressly provided in the Agreement, the following shall apply:

i. Rosetta Stone shall make available to the Customer all information available to demonstrate compliance with the obligations with respect to Rosetta Stone's processing of Customer Personal Data, and to contribute to audits, including inspections, or as applicable, production of available documentation satisfactory to assess internal controls programs and compliance with Data Protection Laws, if and as required of Rosetta Stone under Data Protection Laws.

ii. If Customer wishes to change its instruction, then Customer has the right to request such a change by sending Rosetta Stone a written notice, and Rosetta Stone shall respond in good faith and provide Customer with information regarding Rosetta Stone's standard processes and an estimate of additional fees and costs for such instruction that would be payable by Customer and obtain Customer's written confirmation of such fees prior to taking such action, to the extent such request or instruction is not part of the standard Services offering. Rosetta Stone shall not be obligated to address Customer's requests or

instructions until written agreement on additional payments, if any, has been executed by the Parties to the Agreement.

iii. If the Parties cannot come to an agreement on such payments, requests or instructions, Customer may terminate the affected Services under any Service Order(s) then in effect under the Agreement upon thirty (30) days written notice to Rosetta Stone, provided, however, that Customer shall pay any outstanding Service fees and costs for the remainder of the term agreed in the applicable Service Order and without affecting the remainder Agreement.

h. Rosetta Stone shall ensure that all persons authorized to Process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

i. Rosetta Stone shall provide assistance to Customer as may be reasonably necessary for Customer to comply with Data Protection Laws, including by assisting Customer in responding to requests for exercising data subject rights under Data Protection Laws, taking into consideration Rosetta Stone's access to Customer Personal Data and the Personal Data available to Customer.

i. If Rosetta Stone receives a request directly from any data subject of Customer's for access to, correction, amendment, deletion of, or any other rights to such data subject's Personal Data received or processed under the Agreement with Customer, Rosetta Stone shall promptly instruct the data subject to direct his/her request to Customer, and, to the extent legally permitted, Rosetta Stone shall not otherwise respond to such data subject request without Customer's prior written instructions.

ii. Where requests are manifestly excessive (e.g., because of their repetitive or non-customary character), Customer acknowledges and agrees that Rosetta Stone may apply additional reasonable fees for Rosetta Stone's costs arising from such assistance.

j. The Parties agree that, as part of the Services, Customer Personal Data may be used by Rosetta Stone to verify, optimize and/or improve the Services and for related internal, business purposes.

k. For the avoidance of doubt, Rosetta Stone acknowledges that it is prohibited from retaining, using, or disclosing Customer Personal Data for any purpose other than providing the Services to Customer and otherwise engaging in a "sale" of Customer Personal Data, as defined by the CCPA.

5. SUB-PROCESSING

a. In accordance with the structure of the Services as described in Section 2 of this DPA, Customer consents to Rosetta Stone's use of Sub-Processors (which shall be understood as potentially any Rosetta Stone affiliates or subsidiaries, as defined in this DPA) in the performance of Rosetta Stone's obligations under the Agreement in accordance with the terms of the this DPA.

b. In addition to the possible use of Rosetta Stone's affiliates or subsidiaries as Sub-Processors, Customer authorizes Rosetta Stone to engage, as third parties Sub-Processors, the entities listed at https://support.rosettastone.com/s/article/Enterprise-and-Education-Subprocessors?language=en_US (as may be updated by Rosetta Stone from time to time).

i. If Customer subscribes to such webpage, Rosetta Stone shall inform Customer of any Sub-Processor additions or replacements by updating such webpage at least ten (10) days prior to the addition or replacement.

c. Customer may object to a Sub-Processor addition or replacement solely on reasonable grounds by notifying Rosetta Stone of its objection and the grounds within ten (10) days after receipt of Rosetta Stone's notice. In the event of such an objection, Rosetta Stone may elect to not engage such Sub-Processor. If Rosetta Stone continues use of such Sub-Processor after Customer's reasonable objection, then Customer may elect to immediately (without prejudice to accrued fees or other rights under the Agreement) suspend or terminate the Agreement upon notice to Rosetta Stone.

d. Notwithstanding the foregoing, Rosetta Stone may replace a Sub-Processor if the need for the change is urgent and necessary to provide the Services and continuity thereof. In such instance, Rosetta Stone shall notify Customer of the replacement as soon as reasonably practicable, and Customer shall retain the right to object to the replacement Sub-Processor pursuant to this paragraph.

e. Rosetta Stone shall remain at all times responsible for and fully liable to Customer for the Sub-Processors' performance of its obligations. Rosetta Stone shall also enter into a binding written agreement with each authorized Sub-Processor that imposes, for the concerned processing, the same or greater obligations as Rosetta Stone's obligations as set forth under this DPA.

i. When Rosetta Stone LLC acts as a Sub-Processor, where applicable, Rosetta Stone LLC shall comply with the obligations imposed on "data importers" under Module THREE of the EU Model Clauses ("**P2P Model Clauses**").

ii. For purposes of the P2P Model Clauses, Sections 6 and 7 below shall apply.

6. CROSS-BORDER TRANSFER OF PERSONAL DATA

a. To the extent that Rosetta Stone as a Processor, Processes Customer Personal Data where the relevant Customer entity is established in the European Union ("**EU**")/European Economic Area ("**EEA**") or otherwise subject to the EU General Data Protection Regulation ("**GDPR**"), and such Processing by Rosetta Stone occurs in whole or in part in a jurisdiction outside the European Economic Area that has not been deemed to provide an adequate level of protection by the European Commission ("**EC**") under GDPR Art. 45 ("**Third Country**"), Rosetta Stone shall Process all such Customer Personal Data in accordance with Module TWO of the EU Model Clauses ("**C2P Model Clauses**"), which is hereby incorporated into this DPA by reference. For purposes of the C2P Model Clauses:

i. Signature to the Agreement constitutes signature to the C2P Model Clauses, including the appendices thereto (where applicable).

ii. Appendix A to this DPA shall serve as Annex I.

iii. Appendix B to this DPA shall serve as Annex II.

iv. The list of Sub-Processors linked in Section 5 shall serve as Annex III.

b. To the extent that Rosetta Stone Processes Customer Personal Data in a particular jurisdiction, and such Processing would be prohibited by non-EU/EEA Data Protection Laws in the absence of the implementation of terms comparable to the C2P Model Clauses, Rosetta Stone shall Process all such Customer Personal Data in accordance with the C2P Model Clauses, and for such purposes, references to EU/EEA jurisdictions shall be deemed to be references to the relevant non-EU/EEA jurisdictions as applicable.

c. The Parties may, without amending the Agreement append additional document(s) to this DPA as the Parties deem necessary to facilitate the processing of Customer Personal Data by Rosetta Stone in a particular jurisdiction in compliance with Data Protection Laws.

d. When GDPR applies, if there is any conflict between the terms of this DPA, any C2P Model Clauses in force under the Agreement and any other provisions in the Agreement (or other terms and conditions as may be imposed from time to time, including but not limited to any unilateral terms imposed by either Party), the terms of the C2P Model Clauses shall prevail.

7. **SUPPLEMENTAL OBLIGATIONS FOR THE EU MODEL CLAUSES**

a. Clause 7 (Optional Docking Clause) and the optional language under Clause 11(a) (Optional Redress with Independent Resolution Body) shall not apply.

b. Clause 9(a) shall apply, as detailed in Section 5 above.

c. The Parties re-affirm their commitment to ensuring appropriate data protection safeguards for international data transfers. The Parties agree that as a supplement to, and not in contradiction of the EU Model Clauses nothing in this DPA or the attachments hereto will modify the limitations and disclaimers of liability set forth in the Agreement and such limitations and disclaimers shall continue to apply in full force and effect except to the extent prohibited by law. For the avoidance of doubt, this Section 6(f) applies only as between Customer on the one hand and Rosetta Stone on the other and shall not affect the rights of any relevant data subjects or regulators.

d. Clause 17, Option 1 (Governing Law) shall apply. The Parties agree that the EU Model Clauses shall be governed by the laws of Germany.

e. The Parties further agree that for purposes of the EU Model Clauses, Clause 18 (Choice of Forum and Jurisdiction), any disputes arising from the EU Model Clauses shall be resolved by the courts of Germany.

f. It is expressly agreed that sections 7 d) and e) are only applicable when EU Model Clauses are used according to section 6 a). For other jurisdictions, the law of the Primary Agreement will govern, and disputes shall be resolved by the courts designated by such Primary Agreement.

8. **ADDITIONAL TERMS**

a. The Parties agree to amend this DPA from time to time as may be necessary to permit the Parties to remain in compliance with Data Protection Laws and/or ensuring appropriate safeguards for Customer Personal Data.

b. This DPA supersedes any inconsistent provision in the Agreement between Rosetta Stone and Customer with respect to the Parties' obligations to comply with Data Protection Laws with respect

to Customer Personal Data. When GDPR applies, if there is any conflict between the EU Model Clauses, this DPA and the Related Agreement(s), the terms of the EU Model Clauses shall prevail.

c. This DPA is subject to the terms of, and fully incorporated and made part of, the Agreement. Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement and the terms of this DPA, the relevant terms of this DPA shall take precedence. This DPA shall amend and supplement any provisions relating to Processing of Personal Data previously negotiated between the Parties in the Agreement (including any existing Data Processing Exhibit or any other data processing terms within the Agreement).

Appendix A

A. Parties

Data exporter:
Name: Customer, as defined in this DPA
Address and contact person's name, position, and contact details: As specified in the Agreement.
Activities relevant to the data transferred under the SCCs: Provision of Services consisting in publicly available offerings of Rosetta Stone US's SaaS-based subscription language learning services.
Role: Controller

Data importer:
Name: Rosetta Stone, as defined in this DPA
Address and contact person's name, position, and contact details: As specified in the Agreement.
Activities relevant to the data transferred under the SCCs: Provision of Services consisting in publicly available offerings of Rosetta Stone US's SaaS-based subscription language learning services.
Role (controller / processor): Processor

B. Description of transfer:

Categories of data subjects whose personal data is transferred:

Any data subject whose personal data is transferred to Rosetta Stone in the course of Rosetta Stone's Services under the Agreements, which may include the following categories:

- Employees, agents, advisors, contractors, or other personnel of Customer or any of its subsidiaries or affiliates (who are natural persons), and any other end users authorized by Customer to use the Services under the Services Agreement.

Categories of personal data transferred:

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, subject to the terms of the Agreement, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Employer
- Email
- ID data
- Professional life data for the purpose of language learning
- Voice type (for speech recognition software functionality)
- Country
- Username and password
- Connection data (*e.g.*, IP, OS, device ID, MAC address - to the extent such information qualifies as personal data under applicable law)
- Product usage, progress and/or user interaction data (to the extent such information qualifies as personal data under applicable law)
- Product interface language
- Other personal data as may be provided by Customer or the data subject related to the use of the Services

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

- None

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

- Continuous basis: Customer Personal Data is transferred when an Authorized End User or a Customer Administrator uses the Services;

Nature of the processing

- The data is processed as part of the data exporter's and the data importer's regular business operations as well as on an *ad hoc* basis where a specific business need arises. The nature of the processing may include, but is not limited to, collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing

- To provide the Services set forth in the Agreement.

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

- Customer Personal Data will be retained until 366 days after contract expiration and then be removed according to Rosetta Stone's protocols. Designated Customer point of contact may request an earlier date by submitting the request through Rosetta Stone's data privacy management portal.

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

- The data importer may use various processors to process the data for the purposes set out above. Such processors are typically engaged on the basis of a contract with an unlimited term.

C. Competent supervisory authority

Unless otherwise stated in the DPA, for Controllers established in the EU/EEA, the competent supervisory authority is the supervisory authority of the EU/EEA Member State where the data exporter is established.

Appendix B
Technical and organizational measures

Taking into account:

- the state of the art,
- the costs of implementation and
- the nature, scope, context and
- the purpose of processing as well as
- the risk of varying likelihood and severity for the rights and freedoms of natural persons,

Rosetta Stone shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as follows:

i. **Access Controls** – policies, procedures, and physical and technical controls designed: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt and decrypt Personal Data where appropriate.

ii. **Security Awareness and Training** – a security awareness and training program for all members of the workforce (including management), which includes training on how to implement and comply with its Information Security Program.

iii. **Security Incident Procedures** – a Security Incident Response Plan, and policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

iv. **Contingency Planning** – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Personal Data or systems that contain Personal Data, including a data backup plan and a disaster recovery plan.

v. **Device and Media Controls** – policies and procedures that govern the receipt and removal of hardware and electronic media that contain Personal Data into and out of processing facilities, and the movement of these items within processing facilities, including policies and procedures to address the final disposition of Personal Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of Personal Data from electronic media before the media are made available for re-use.

vi. **Audit Controls** – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

vii. **Security Audits** - annual third party security audits, such as SSAE 16 SOC2, of hosting and data center providers, who also maintain current ISO 27001 certifications.

viii. **Data Integrity** – policies and procedures to ensure the confidentiality, integrity, and availability of Personal Data and protect it from disclosure, improper alteration, or destruction.

ix. **Storage and Transmission Security** – technical security measures to guard against unauthorized access to Personal Data that is being transmitted over an electronic communications network, including a mechanism to ensure Personal Data in electronic form is encrypted while in transit and in storage on networks or systems to which unauthorized individuals may have access.

x. **Assigned Security Responsibility** – designate a security official responsible for the development, implementation, and maintenance of its Information Security Program, and inform Company upon request as to the person responsible for security.

xi. **Storage Media** - policies and procedures to ensure that prior to any storage media containing Personal Data being assigned, allocated or reallocated to another user, or prior to such storage media being permanently removed from a facility, irreversibly delete such Personal Data from both a physical and logical perspective, such that the media contains no residual data, or if necessary physically destroy such storage media such that it is impossible to recover any portion of data on the media that was destroyed. Also maintain an auditable program implementing the disposal and destruction requirements set forth in this Section for all storage media containing Personal Data.

xii. **Testing** – regularly test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified.

xiii. **Adjust the Program** – monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the Personal Data, internal or external threats to the Personal Data, and changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.