ROSETTA STONE LTD.
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 Ltd. ("Rosetta Stone"), 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 Personal Data of employees or other Authorized End Users of Customer (as defined in the Agreement), by Rosetta Stone as data processor on behalf of Customer and in accordance with Customer's instructions as data controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions. For the purposes of this DPA, the following terms shall have the following meanings:

"Personal Data" means any information received by Rosetta Stone from Customer relating to Customer's users authorized by Customer to use the Services that is sufficient to cause such person to be identified, directly or indirectly, specifically by reference to any of the Categories of Personal Data specified in Annex 1, to the extent applicable.

"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.

"Privacy Shield Framework" means the EU-U.S. or Swiss-U.S. Privacy Shield Framework.

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 the categories of data subjects and Personal Data to be Processed are as described in Annex 1 of this DPA and the Processing shall be as required to provide the Services.

3. Customer's Obligations.

a. Customer remains the responsible data controller (or similar term under applicable law) for the Processing of the Personal Data subject to this DPA as instructed to Rosetta Stone. Subject to the provisions contained in Section 4g below, 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 applicable laws, including data protection laws, in particular with any notice and/or consent requirements, and, notwithstanding anything to the contrary in the Agreement, Customer shall remain responsible for and protect 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.

b. 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 will Process the Personal Data in compliance with applicable law 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 document agreed to by the parties, in accordance with the terms of this DPA. For the avoidance of doubt, Rosetta Stone acknowledges that it is prohibited from retaining, using or disclosing Personal Data for any purpose other than providing the Services to Customer.

b. Rosetta Stone will 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 Personal Data, and take any necessary steps to remediate any Processing of such 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(f) shall apply.

c. With respect to the Personal Data transferred to or received by Rosetta Stone under the Agreement, Rosetta Stone has implemented, and will 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.

d. 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 Personal Data by Rosetta Stone or its subprocessors of which Rosetta Stone becomes aware.

e. To the extent legally permitted, Rosetta Stone shall promptly notify Customer if it receives a request for any 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 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. With respect to requests for audits or other additional instructions by Customer, unless otherwise expressly provided in the Agreement, the following shall apply: 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 applicable law, if and as required of Rosetta Stone under applicable law. 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. 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.

g. As required by applicable law, Rosetta Stone shall immediately inform Customer if, in its opinion, an instruction infringes applicable data privacy regulations.

h. Rosetta Stone will ensure that persons authorized to process the 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 applicable data protection laws, including by assisting Customer in responding to requests for exercising data subject rights under applicable law, taking into consideration Rosetta Stone's access to Customer Personal Data and the Personal Data available to Customer. If Rosetta Stone receives a request 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 Services 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, and Rosetta Stone shall provide Customer with commercially reasonable cooperation and assistance in relation to handling such data subject's request to exercise rights to such data subject's Personal Data if and as directed by Customer. 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, Personal Data may be used by Rosetta Stone to verify, optimize and/or improve the Services and for related internal, business purposes.

5. Cross-Border Transfers

a. As required or acceptable to satisfy cross-border transfer obligations under applicable law, to the extent that Rosetta Stone stores or otherwise processes Personal Data in the U.S., including but not limited to Personal Data about individuals who reside in the European Economic Area ("EEA"), the United Kingdom and/or Switzerland, the parties agree that the Standard Contractual Clauses for the Transfer of Personal Data to Data Processors Established In Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 (link) ("**Model Processor Clauses**"), including the appendices attached thereto, are incorporated into this DPA by reference, and shall apply to such transfers. For purposes of any transfers, Rosetta Stone shall be the "data importer," and Customer established in the relevant jurisdiction shall be the "data exporter." The data processing activities in Appendix 1 to the Model Processor Clauses shall be as described in Annex 1 of this DPA, and the technical and organizational security measures in Appendix 2 to the Model Processor Clauses shall be those measures described in Annex 2 of this DPA. The parties agree that acceptance of the Agreement, constitutes all necessary signatures to the Model Processor Clauses with respect to transfers to Rosetta Stone.

b. In event that a successor to the Privacy Shield Framework or Model Processor Clauses are established, Rosetta Stone agrees it shall, as appropriate and required by applicable law, coordinate in good faith with Customer to establish supplemental data transfer terms with Customer.

6. Subprocessing.

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 subprocessors in the performance of Rosetta Stone's obligations under the Agreement in accordance with the terms of this DPA.

b. Rosetta Stone may, by giving prior notice to Customer, add or make changes to the subprocessors. Customer may object to the appointment of any such additional subprocessor within fourteen (14) calendar days of such notice on reasonable and specific grounds relating to the protection of Customer's Personal Data, in which case Rosetta Stone shall have the right to cure the objection through one of the following options (to be selected at Rosetta Stone's sole discretion): (a) Rosetta Stone will cancel its plans to use the subprocessor with regard to Personal Data or will offer an alternative to provide the Services to Customer without such subprocessor; or (b) Rosetta Stone will take such corrective steps identified by Customer in its objection (which remove Customer's objection) and proceed to use the subprocessor with regard to Personal Data; or (c) Rosetta Stone may cease to provide or Customer may agree not to use (temporarily or permanently) the particular aspect of the Services that would involve the use of such subprocessor with regard to Personal Data, subject to a mutual agreement of the parties to adjust the remuneration for the impacted Subscription Services, considering the reduced scope of the Subscription Services. Objections to a subprocessor shall be submitted to Rosetta Stone by following the directions set forth in the subprocessor notice or subprocessor list provided by Rosetta Stone to Customer. If none of the above options are reasonably available and the objection

has not been resolved to the mutual satisfaction of the parties within thirty (30) days after Rosetta Stone's receipt of Customer's objection, either party may terminate the affected Services and Customer will be entitled to a pro-rata refund for prepaid fees based on the portion of the Services not performed as of the date of termination. Notwithstanding the foregoing, Rosetta Stone may replace a subprocessor 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 subprocessor pursuant to this paragraph. Rosetta Stone agrees that its agreements with subprocessors will include contractual commitments to protect and maintain the confidentiality and security of Personal Data consistent with Rosetta Stone's obligations as processor under this Agreement, the requirements of applicable law, and taking into account the Personal Data processed and services provided by subprocessors

c. Rosetta Stone shall be liable for the acts and omissions of its subprocessors to the same extent it would be liable if performing the services of each such subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. Governing Law.
This DPA is governed by and construed in accordance with the laws of the jurisdiction provided for in the Agreement without regard for its choice of law rules.

8. Termination.
a. This DPA shall remain in full force and effect for so long as the Agreement remains in effect, and shall immediately terminate if the Agreement is terminated for any reason.

b. The Services include self-service reporting tools enabling Customer's designated Enterprise Administrator User(s) to access and export reports with the Personal Data of its Authorized End Users at any time during the service period. Upon expiration or termination of the Agreement, Rosetta Stone shall continue to make such Personal Data available for export by Customer (i.e., allow Customer to download reports) upon request made within thirty (30) days of termination or expiration of the Agreement. After such thirty (30) day period, Rosetta Stone shall have no obligation to maintain or provide any Personal Data and may, unless legally prohibited, securely remove and delete or otherwise render unreadable or undecipherable Personal Data in its possession or control in accordance with Rosetta Stone's then-current data removal protocols, with no liability to Licensee, unless otherwise agreed to by Licensor and Licensee in writing in the Service Order for the applicable service. When Personal Data removal has been completed, Rosetta Stone will provide written confirmation of same upon written request.

9. Miscellaneous
a. 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 or inconsistency 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).
b. The Agreement shall apply only between Rosetta Stone and Customer and shall not confer any rights to any third parties.

c. All other terms and conditions of the Agreement remain unchanged.

ANNEX 1
DETAILS OF THE PROCESSING

Purpose of the Processing:

Provision of Services consisting in publicly available offerings of Rosetta Stone's SaaS-based subscription language learning services.

Categories of Data Subjects

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 data subjects:

- 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

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
- Title/position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data for the purpose of language learning
- Personal life data for the purpose of language learning
- Month and year of birth (for speech recognition software functionality)
- Gender (for speech recognition software functionality)
- Connection data
- General geographic location (e.g., country/city)
- 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)
- Localization data
- Other personal data as may be provided by Customer or the data subject related to the use of the Services

Special Categories of Data or Sensitive Personal Data

None

ANNEX 2
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

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.