Riipen Data Processing Addendum

Effective date: September 5, 2026

Data Addendum

This Data Processing Addendum ("Addendum") supplements the Terms of Service available at https://riipen.com/terms or other written or electronic agreement between Riipen Networks, Inc. ("Riipen") and the individual or entity ("Customer") purchasing access to the services provided by Riipen (the Terms of Service or such other agreement, as applicable, is referred to herein as the "Agreement"; the applicable services are referred to herein as the "Services"). Any capitalized term used but not defined in this Addendum has the meaning provided to it in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control with respect to the parties' data obligations under the Agreement relating to personal data.

I. Introduction

1. Definitions.

As used in this Addendum:

"**Anonymous Data**" means personal data that has been processed in such a manner that it can no longer be attributed to a data subject without additional information unavailable to any third party other than sub-processors.

"**Applicable Data Protection Law**" refers to all laws and regulations applicable to Riipen's processing of personal data under the Agreement.

"**controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**Customer Administrative Information**" means personal data, if any, collected by Riipen from Customer in connection with the vendor-customer relationship between Riipen and Customer (e.g., the names or contact information of individuals authorized by Customer to access Customer's account), including, without limitation, by way of Riipen's website.

"**Customer Application Data**" means personal data, if any, contained in Customer's application(s) and transferred to Riipen in connection with Riipen's provision of its experiential learning solutions, including, without limitation, by way of Riipen's software

development kits (“SDKs”), application programming interfaces (“APIs”), and website and web applications.

“**Customer Data**” means, collectively, Customer Administrative Information and Customer Application Data.

“**Data Privacy Framework**” means (as applicable) the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework self-certification programs operated by the U.S. Department of Commerce, and their respective successors.

“**Data Privacy Framework Principles**” means the Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as amended, superseded or replaced.

“**personal data**” means any information relating to an identified or identifiable natural person (“data subject”), excluding Anonymous Data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Privacy Policy**” means the then-current privacy policy for the Services available at https://www.riipen.com/privacy-policy.

“**processor**” means the entity which processes personal data on behalf of the controller.

“**processing**” (and “process”) means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

“**Security Documentation**” means the documentation set forth at https://www.riipen.com/security-policy.

“**Security Incident**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

“**Sensitive Data**” means (a) social security number, passport number, driver’s license number, or similar identifier); (b) genetic, biometric or health information; (c) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (d) criminal history; or (e) any other information or combinations of information that falls within the definition of

“**special categories of data**” under GDPR or any other applicable law or regulation.

"**Standard Contractual Clauses**" has the meaning set forth in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum.

"**sub-processor**" means processing by (a) Riipen on behalf of Customer where Customer itself acts in its role as a processor or (b) any third party processor engaged by Riipen to process Customer Application Data in order to provide the Services to Customer. For the avoidance of doubt, telecommunication providers are not sub-processors.

"**Third Party Request**" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

II. Controller and Processor

2. Relationship of the Parties.

2.1. Riipen as a Processor of Customer Application Data. The parties acknowledge and agree that with regard to the processing of Customer Application Data, Customer may act either as a controller or processor and Riipen is a processor. Riipen will process Customer Application Data in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions).

2.2. Riipen as a Controller of Customer Administrative Information. The parties acknowledge that, with regard to the processing of Customer Administrative Information, Customer is a controller and Riipen is an independent controller, not a joint controller with Customer. Riipen will process Customer Administrative Information as a controller to provide, optimize, and maintain the Services, including, without limitation, to (a) manage the relationship with Customer; (b) carry out Riipen's business operations, such as accounting, tax, billing, audit, and compliance purposes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; and (d) comply with Riipen's legal or regulatory obligations; or as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Privacy Policy.

3. Purpose Limitation.

Riipen will process Customer Data in order to provide the Services in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

4. Compliance.

Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own processing of personal data, and (b) it has, and will continue to have, the right to transfer, or provide

access to, Customer Data to Riipen for processing in accordance with the terms of the Agreement and this Addendum.

III. Riipen as a Processor – Processing Customer Application Data

5. Customer Instructions.

Customer appoints Riipen as a processor to process Customer Application Data on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the Services to Customer; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between the parties (collectively, "Permitted Purposes").

5.1. Lawfulness of Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer acknowledges that Riipen is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Riipen's provision of the Services meets or will meet the requirements of such laws or regulations. Customer will ensure that Riipen's processing of Customer Application Data, when done in accordance with Customer's instructions, will not cause Riipen to violate any applicable law or regulation, including Applicable Data Protection Law. Riipen will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including Applicable Data Protection Law.

5.2. Additional Instructions. Additional instructions outside the scope of the Agreement or this Addendum, if any, will be agreed to between the parties in writing, including any additional fees that may be payable by Customer to Riipen for carrying out such additional instructions.

6. Confidentiality.

6.1. Responding to Third Party Requests. In the event any Third Party Request is made directly to Riipen in connection with Riipen's processing of Customer Application Data, Riipen will promptly inform Customer and provide details of the same, to the extent legally permitted. Riipen will not respond to any Third Party Request, without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

6.2. Confidentiality Obligations of Riipen Personnel. Riipen will ensure that any person it authorizes to process Customer Application Data has agreed to protect personal data in accordance with Riipen's confidentiality obligations in the Agreement.

7. Sub-processors.

7.1. Authorization for Onward Sub-processing. Customer provides a general authorization for Riipen to engage onward sub-processors that is conditioned on the following requirements:

(a) Riipen will restrict the onward sub-processor's access to Customer Application Data only to what is strictly necessary to provide the Services, and Riipen will prohibit the sub-processor from processing the personal data for any other purpose.

(b) Riipen agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Application Data to the standard required by Applicable Data Protection Law; and

(c) Riipen will be liable to Customer for the acts and omissions of its sub-processors to the same extent that Riipen would itself be liable under this Addendum had it conducted such acts or omissions.

7.2. List of Sub-processor and Changes. Customer consents to Riipen engaging additional third party sub-processors to process Customer Application Data for the Permitted Purposes provided that Riipen maintains an up-to-date list of its sub-processors at https://www.riipen.com/subprocessors, which web page contains a mechanism for Customer to subscribe to notifications of new sub-processors. If Customer so subscribes, Riipen will provide details of any change in sub-processors at least ten (10) days prior to any such change, and Customer may object to any such change, as follows:

(a) In the event of any change in sub-processors, Riipen will notify Customer, and Customer may object to such an engagement in writing within ten (10) days of Customer's receipt of the aforementioned notice.

(b) If Customer reasonably objects to an engagement of a sub-processor in accordance with this Section 7.2, Riipen will provide Customer with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Riipen, in its sole discretion, cannot provide any such alternative(s), or if Customer does not agree to any such alternative(s), if provided, Riipen may terminate this Addendum. Termination will not relieve Customer of any fees owed to Riipen under the Agreement.

(c) If Customer does not object to the engagement of a sub-processor in accordance with Section 7.2 within ten (10) days of notice by Riipen, such sub-processor will be deemed authorized by Customer for the purposes of this Addendum.

8. Data Subject Rights.

Upon Customer's request, Riipen will provide reasonable assistance (at Customer's expense) to assist Customer in complying with its data protection obligations with respect to data subject rights under Applicable Data Protection Law.

9. Deletion and Retention of Customer Application Data.

(a) Riipen will delete Customer Application Data in accordance with the procedures and timeframes specified in Riipen's Security Documentation.

(b) Upon termination of the Agreement, Riipen may retain Customer Application Data in storage for the timeframes specified in Riipen's Security Documentation, provided that Riipen will ensure that Customer Application Data (i) is processed only as necessary for the Permitted Purposes and (ii) remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

(c) Notwithstanding anything to the contrary in this Section 9, Riipen may retain Customer Application Data, or any portion of it, if required by applicable law or regulation, including Applicable Data Protection Law, provided such Customer Application Data remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

IV. Security and Audits

10. Security.

Riipen will maintain appropriate technical and organizational measures to ensure a level of security (including protection against unauthorized or unlawful processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data), confidentiality and integrity of Customer Data, appropriate to the risk of processing Customer Data, and as set forth in Riipen's Security Documentation. Riipen regularly monitors compliance with these measures. Riipen will not materially decrease the overall security of the Service during a subscription term.

11. Security Incident Notification.

11.1. In the event of a Security Incident, Riipen will, to the extent permitted and required by applicable law:

(a) notify Customer without undue delay, but in no event later than seventy-two (72) hours after Riipen's discovery of the Security Incident impacting Customer Data of which Riipen is a processor (e.g., Customer Application Data);

(b) notify Customer without undue delay of any Security Incident involving Customer Data of which Riipen is a controller (e.g., Customer Administrative Information).

11.2. To the extent a Security Incident is caused by Riipen's violation of this Addendum, Riipen will make reasonable efforts to remediate the cause of such Security Incident and provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects impacted by a Security Incident.

12. Audits.

The parties acknowledge that Customer must be able to assess Riipen's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Riipen is acting as a processor on behalf of Customer.

12.1. Riipen's Audit Program. Riipen uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Application Data. Such audits are performed at least once annually at Riipen's expense by independent third party security professionals at Riipen's selection, and result in the generation of a confidential audit report ("Audit Report"). A description of Riipen's certifications and standards for audit can be found within Riipen's Security Documentation.

12.2. Customer Audit. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Riipen will make available to Customer a copy of Riipen's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Law will be satisfied by these Audit Reports. To the extent that Riipen's provision of an Audit Report does not provide sufficient information or Customer is required to respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Riipen that: (a) ensures the use of an independent third party; (b) provides notice to Riipen in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Riipen's then-current rates; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Customer; and (g) obligates Customer, to the extent permittedby law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

V. Unnecessary Personal Data

13. Unnecessary Personal Data.

The Services are comprised of Riipen's experiential learning solutions. In providing the Services, it is not necessary for Riipen to receive personal data from Customer, except for Customer Administrative Information for the vendor-customer relationship between Riipen and Customer (all personal data outside of Customer Administrative Information are referred to herein as "Unnecessary Personal Data"). Riipen hereby instructs Customer, and Customer agrees, not to transfer or otherwise make accessible to Riipen any Unnecessary Personal Data. Notwithstanding any other provisions, Riipen shall not be liable for any Unnecessary Personal Data.

Without limiting the above paragraph, Riipen's SDKs include scrubbing filters that allow Customer to block or limit the amount of personal data, including Sensitive Data, to be transferred from Customer's application(s) to Riipen in connection with the Services. However, Riipen does not guarantee that all personal data or Sensitive Data will be

scrubbed by such filters, and Customer acknowledges and agrees that it is ultimately Customer's responsibilities to ensure that no Unnecessary Personal Data will be transferred or made accessible to Riipen.

VI. International Provisions

14. Processing in Canada.

Customer acknowledges that, as of the Effective Date, Riipen's primary processing facilities are in Canada.

15. Jurisdiction Specific Terms. To the extent Riipen processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms) of this Addendum, the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) apply in addition to the terms of this Addendum.

16. Cross Border Data Transfer Mechanisms for Data Transfers.To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area ("EEA"), the United Kingdom, Switzerland, or any other jurisdiction listed in Schedule 4 (Jurisdiction Specific Terms)) to Riipen located outside of that jurisdiction ("Transfer Mechanism"), the terms set forth in Schedule 3 (Cross Border Transfer Mechanisms) will apply.

VII. Miscellaneous

17. Limitation of Liabilities. The liabilities of Riipen and all of its affiliates (collectively, "Riipen Parties"), taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the limitation of liabilities provisions in the Agreement. For the avoidance of doubt, Riipen Parties' total liabilities for all claims from Customer and Customer's affiliates arising out of or related to the Agreement and this Addendum shall apply in the aggregate for all claims under both the Agreement and this Addendum and, in particular, shall not apply individually and severally to Customer and/or to any of its affiliates.

18. Cooperation and Data Subject Rights. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third Party Request relating to the processing of Customer Administrative Information conducted by the other party, such party will promptly inform such other party in writing. The parties agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law.

19. Conflict.

In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in Schedule 4 (Jurisdiction Specific Terms); (2) the terms of this Addendum outside of Schedule 4; (3) the Agreement; and (4) the Privacy Policy. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

20. Failure to Perform.

In the event that changes in law or regulation render performance of this Addendum impossible or commercially unreasonable, the parties may renegotiate this Addendum in good faith. If renegotiation would not cure the impossibility or the parties cannot reach an agreement, the parties may mutually agree to terminate the Agreement for convenience.

21. Updates.

Riipen may update the terms of this Addendum from time to time; provided, however, Riipen will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this Addendum are available at https://www.riipen.com/subprocessors.

SCHEDULE 1 - DETAILS OF PROCESSING

1. Nature and Purpose of the Processing.

Riipen will process personal data as necessary to provide the Services under the Agreement, and as further instructed by Customer in its use of the Services. Riipen does not sell Customer's personal data or Customer end users' personal data and does not share such personal data with third parties for compensation or for those third parties' own business interests.

Customer Application Data: Riipen will process Customer Application Data as a processor in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions) of this Addendum.

Customer Administrative Information: Riipen will process Customer Administrative Information as a controller for the purposes set forth in Section 2.2 (Riipen as a Controller of Customer Administrative Information) of this Addendum.

2. Processing Activities.

Customer Data will be subject to the following basic processing activities:

(a) use of the data to set up, operate, monitor, and provide the Services (including operational and technical support);

(b) continuous improvement of service features and functionalities provided as part of the Services;

(c) communication to authorized users;

(d) computer processing of the data, including data transmission, data retrieval, data access;

(e) network access to allow data transfer;

(f) monitoring, troubleshooting and administering the underlying Service infrastructure and database;

(g) security monitoring, network-based intrusion detection support, penetration testing; and

(h) execution of instructions of Customer in accordance with the Agreement.

3. Duration of the Processing.

Customer Application Data: Customer Application Data will be retained for the duration of the Agreement and subject to Section 9 of the Addendum.

Customer Administrative Information: Riipen will process Customer Administrative Information as long as required (a) to provide the Services to Customer; (b) for Riipen's legitimate business needs; or (c) by applicable law or regulation. Customer Administrative Information will be stored in accordance with the Privacy Policy.

4. Categories of Data Subjects.

Customer Application Data: Customer and Customer's end users, if applicable.

Customer Administrative Information: Customer (i.e., individuals authorized by Customer to access Customer's account with Riipen).

5. Categories of Personal Data.

Riipen processes the personal data, if any, that constitute Customer Application Data or Customer Administrative Information.

See Section 13 (Unnecessary Personal Data) of this Addendum.

6. Sensitive Data or Special Categories of Data.

Customer Application Data: See Section 13 (Unnecessary Personal Data) of this Addendum.

Customer Administrative Information: Riipen does not ask for, and does not desire to receive, any Sensitive Data. Riipen hereby instructs Customer, and Customer agrees, not to transfer or otherwise make accessible to Riipen any Sensitive Data.

SCHEDULE 2 - TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Riipen will apply and maintain the technical and organizational security measures set forth in Riipen's Security Documentation.

Where applicable, this Schedule 2 will serve as Annex II to the Standard Contractual Clauses.

SCHEDULE 3 - CROSS BORDER DATA TRANSFER MECHANISMS

1. Definitions

As used herein:

"**EC**" means the European Commission.

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

"**EU Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

"**Standard Contractual Clauses**" means, depending on the circumstances unique to Customer, any of the following:

(a) UK International Data Transfer Agreement, and

(b) EU Standard Contractual Clauses.

"**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1. Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the applicable Standard Contractual Clauses as set forth in Section 2.2 (EU Standard Contractual Clauses) or Section 2.3 (UK International Data Transfer Agreement) of this Schedule 3; and, if (a) is applicable, then (b) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2. EU Standard Contractual Clauses. The parties agree that the EU Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the European Economic Area 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 European Economic Area that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses 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 Standard Contractual Clauses will apply where Riipen is processing Customer Administrative Information.

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Customer Application Data and Riipen is processing Customer Application Data.

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Application Data and Riipen is processing Customer Application Data.

(d) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 7.2 (List of Sub-processor and Changes) of this Addendum;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter: Customer.

Contact details: The email address(es) designated by Customer in Customer's account via its notification preferences.

Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

Data Importer: Riipen Networks Inc.

Contact details: Riipen's data protection officer - security@riipen.com

Data Importer Role: The Data Importer's role is set forth in Section 2 (Relationship of the Parties) of this Addendum.

Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these Standard Contractual Clauses, incorporated herein, including their Annexes, as of the Effective Date of the Agreement.

(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

The categories of data subjects are described in Section 4 of Schedule 1 (Details of Processing) of this Addendum.

The Sensitive Data transferred is described in Section 6 of Schedule 1 (Details of Processing) of this Addendum.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is described in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The purpose of the processing is described in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The period for which the personal data will be retained is described in Section 3 of Schedule 1 (Details of Processing) of this Addendum.

For transfers to sub-processors, the purpose of the processing is set forth at https://riipen.com/subprocessors.

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

(ix) Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the Standard Contractual Clauses.

2.3 UK International Data Transfer Agreement. The parties agree that the UK International Data Transfer Agreement 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 International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in Section 2.2(d)(vi) of this Schedule 3.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.2 (EU Standard Contractual Clauses) of this Schedule 3.

(c) In Table 3 of the UK International Data Transfer Agreement:

1. The list of Parties is located in Section 2.2(d)(vi) of this Schedule 3.

2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 1 (Details of the Processing).

3. Annex II is located in Schedule 2 (Technical and Organizational Security Measures)

4. The list of sub-processors is located at https://riipen.com/subprocessors.

(d) In Table 4 of the UK International Data Transfer Agreement, both the importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.4. Conflict. To the extent there is any conflict between the Standard Contractual Clauses, and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms) of this Addendum, the Agreement, or the Privacy Policy, the provisions of the Standard Contractual Clauses will prevail.

SCHEDULE 4 - JURISDICTION SPECIFIC TERMS

United States of America

1. “US State Privacy Laws” means all applicable state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“CCPA”), the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

2. The definition of “Applicable Data Protection Law” includes US State Privacy Laws.

3. The following Sections 3(a) to 3(j) apply where Riipen processes personal data subject to the CCPA:

(a) The term “personal information”, as used in this Section 3, will have the meaning provided in the CCPA.

(b) Riipen is a service provider when processing Customer Data. Riipen will process any personal information contained in Customer Data only for Permitted Purposes (as defined in Section 5 of the Addendum). As a service provider, Riipen will not sell or share Customer Data or retain, use, or disclose Customer Data (i) for any purpose other than Permitted Purposes, including retaining, using, or disclosing Customer Data for a commercial purpose other than Permitted Purposes, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Riipen.

(c) Riipen will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own processing of personal information.

(d) Customer will have the right to take reasonable and appropriate steps to help ensure that Riipen uses personal information in a manner consistent with Customer’s obligations under the CCPA.

(e) Riipen will notify Customer if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA.

(f) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information.

(g) Riipen will provide reasonable additional and timely assistance to assist Customer in complying with its obligations with respect to consumer requests as set forth in the Agreement.

(h) For any sub-processor used by Riipen to process personal information subject to the CCPA, Riipen will ensure that Riipen's agreement with such sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors.

(i) Riipen will not combine or update personal information that it collected pursuant to the Agreement with Customer with personal information that it received from another source or collected from its own interaction with Consumer, unless such combination or update is required to perform any Permitted Purposes as permitted by the CCPA or regulations adopted by the California Privacy Protection Agency.

(j) Riipen certifies that it understands and will comply with its obligations under the CCPA.

4. Riipen acknowledges and confirms that it does not receive Customer Data as consideration for any Services provided to Customer.

European Economic Area (EEA)

1. The definition of "Applicable Data Protection Law" includes the General Data Protection Regulation (EU 2016/679) ("GDPR").

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

(a) require any appointed sub-processor to protect the Customer Application Data 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

(b) 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.

3. 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.

United Kingdom (UK)

1. 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).

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

(a) require any appointed sub-processor to protect the Customer Application Data 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

(b) 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 UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

3. 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.