
DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) is incorporated by reference into the [Terms and Conditions](#) (“**Agreement**”) governing the use of the Platform (as defined under the Agreement). This DPA is entered into by and between you, either individually, or on behalf of your employer or any other entity which you represent (collectively, “**you**”, “**your**”, “**Customer**”), and RiversideFM, Inc. (“**Riverside**”, “**us**”, “**we**”, “**our**”) to reflect the parties’ agreement with regard to the Processing of Personal Data by Riverside solely on behalf of the Customer. Both parties shall be referred to as the “**Parties**” and each, a “**Party**”.

By using the Platform, you accept this DPA and, if you intend to use the Platform on behalf of or in the course of your employment by an organizational Customer, you represent and warrant that you have full authority to bind the Customer to this DPA. If you cannot, or do not agree to, comply with and be bound by this DPA, or do not have authority to bind the Customer or any other entity, please do not provide Personal Data to us.

In the event of any conflict between certain provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail over the conflicting provisions of the Agreement solely with respect to the Processing of Personal Data.

1. DEFINITIONS

- (a) “**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control”, for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.
- (b) “**Authorized Affiliate**” means any of Customer's Affiliate(s) which is explicitly permitted to use the Platform pursuant to the Agreement between Customer and Riverside but has not signed its own agreement with Riverside and is not a “Customer” as defined under the Agreement.
- (c) “**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et. Seq, and its implementing regulations, as amended by the California Privacy Rights Act and as may be amended from time to time.
- (d) The terms, “**Controller**”, “**Member State**”, “**Processor**”, “**Processing**” and “**Supervisory Authority**” shall have the same meaning as in the GDPR. The terms “**Business**”, “**Business Purpose**”, “**Consumer**” and “**Service Provider**” shall have the same meaning as in the CCPA.
- (e) For the purpose of clarity, within this DPA “**Controller**” shall also mean “**Business**”, and “**Processor**” shall also mean “**Service Provider**”, to the extent that the CCPA applies. In the same manner, Processor’s Sub-processor shall also refer to the concept of Service Provider.
- (f) “**Data Protection Laws**” means all applicable and binding privacy and data protection laws and regulations, including (without limitation) such laws and regulations of the European Union, the European Economic Area and their Member States, Switzerland, the United Kingdom, Canada, Israel and the United States of America, as applicable to the Processing of Personal Data under the Agreement including (without limitation) the GDPR, the UK GDPR, the FADP and the CCPA, as applicable to the Processing of Personal Data hereunder and in effect at the time of Riverside’s performance hereunder.
- (g) “**Data Subject**” means the identified or identifiable person to whom the Personal Data relates.
- (h) “**FADP**” means the Swiss Federal Act on Data Protection of 25 September 2020.
- (i) “**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

- (j) **“Personal Data” or “Personal Information”** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to or with an identified or identifiable natural person or Consumer, to the extent such information is processed by Riverside solely on behalf of Customer, under this DPA and the Agreement between Customer and Riverside. For the avoidance of doubt, Personal Data does not include “Content Data” as defined in Riverside’s [Privacy Policy](#).
- (k) **“Platform”** means the services provided to Customer by Riverside in accordance with the Agreement.
- (l) **“Security Documentation”** means the security measures applicable to the Platform, as made reasonably available by Riverside upon Customer’s request.
- (m) **“Sensitive Data”** means Personal Data that is protected under a special legislation and requires unique treatment, such as “special categories of data”, “sensitive data” or other materially similar terms under applicable Data Protection Laws, which may include any of the following: (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number; (c) financial, credit, genetic, biometric or health information; (d) information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences; and/or (e) account passwords in unhashed form.
- (n) **“Standard Contractual Clauses”** means the standard contractual clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (“**EU SCCs**”), or (b) where the UK GDPR applies, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses as issued by the Information Commissioner’s Office under S119A(1) of the Data Protection Act 2018 and in force as of 21 March 2022 (“**UK Addendum**”).
- (o) **“Sub-processor”** means any third party that Processes Personal Data under the instruction or supervision of Riverside.
- (p) **“UK GDPR”** means the Data Protection Act 2018, as well as the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419).

2. PROCESSING OF PERSONAL DATA

- 2.1 **Roles of the Parties.** The Parties acknowledge and agree that with regard to the Processing of Personal Data solely on behalf of Customer as part of Riverside’s provision of the Platform, (i) Customer is the Controller of Personal Data, (ii) Riverside is the Processor of such Personal Data.

Riverside acts as a Controller over certain types of personal data, including “Content Data” (as defined in Riverside’s Privacy Policy), which may be used to help train and improve Riverside’s artificial intelligence and machine learning models. Please read Riverside’s [Privacy Policy](#) for further information.

- 2.2 **Customer’s Processing of Personal Data.** Customer, in its use of the Platform, and Customer’s instructions to the Riverside, shall comply with Data Protection Laws. Customer shall establish and have any and all required legal bases in order to collect, Process and transfer to Riverside the Personal Data, and to authorize the Processing by Riverside, and for Riverside’s Processing activities on Customer’s behalf, including the pursuit of ‘business purposes’ as defined under the CCPA.

2.3 Riverside’s Processing of Personal Data.

- 2.3.1 When Processing on Customer’s behalf under the Agreement, Riverside shall Process Personal Data for the following purposes: (i) In accordance with the Agreement and this DPA; (ii) To comply with Customer’s reasonable and documented instructions, where such instructions are consistent with the terms of the Agreement, regarding the manner in which the Processing

shall be performed; (iii) Rendering Personal Data fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognized by Data Protection Laws and guidance issued thereunder; (iv) Disclosing Personal Data to, or receiving Personal Data from, third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Platform (e.g., integrations between the Platform and any services provided by third parties, as configured by or on behalf of Customer; and (v) Processing as required under the laws applicable to Riverside, and/or as required by a court of competent jurisdiction or other competent governmental or semi-governmental authority, provided that Riverside shall inform Customer of the legal requirement before Processing, unless such law or order prohibit such information on important grounds of public interest.

2.3.2 In the event that Customer discloses or otherwise makes available to Riverside De-identified Data (as defined by applicable Data Protection Laws), Riverside shall (i) take reasonable measures to ensure such data cannot be associated with a natural person, and (ii) maintain and use such data without attempting to re-identify it.

2.3.3 Riverside shall inform Customer without undue delay if, in Riverside's opinion, an instruction for the Processing of Personal Data given by Customer infringes applicable Data Protection Laws. To the extent that Riverside cannot comply with an instruction from Customer, Riverside (i) shall inform Customer, providing relevant details of the issue, (ii) Riverside may, without liability to Customer, temporarily cease all Processing of the affected Personal Data (other than securely storing such data) and/or suspend Customer's access to the Platform, and (iii) if the Parties do not agree on a resolution to the issue in question and the costs thereof, Customer may, as its sole remedy, terminate the Agreement and this DPA with respect to the affected Processing, and Customer shall pay to Riverside all the amounts owed to Riverside or due before the date of termination, if any. Customer will have no further claims against Riverside (including, without limitation, requesting refunds) pursuant to the termination of the Agreement and the DPA as described in this paragraph.

2.4 **Details of the Processing.** The subject matter of Processing of Personal Data by Riverside is the provision and operating of the Platform pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of Processing) to this DPA.

2.5 **Sensitive Data.** The Platform is not intended for the processing of Sensitive Data, except to the extent that a specific Platform feature or tool is expressly designed by Riverside to collect or process such data in order to provide that feature or tool. If Customer wishes to use the Platform to process Sensitive Data, it must first obtain Riverside's explicit prior written consent.

2.6 **CCPA Standard of Care; No Sale or Sharing of Personal Information.** Riverside acknowledges and confirms that it does not receive or process any Personal Information as consideration for any services or other items that Riverside provides to Customer under the Agreement or this DPA. Riverside certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling or sharing (as such terms are defined in the CCPA) any Personal Information Processed hereunder, without Customer's prior written consent or instruction, nor take any action that would cause any transfer of Personal Information to or from Riverside under the Agreement or this DPA to qualify as "selling" and/or "sharing" such Personal Information under the CCPA. Riverside acknowledges that Customer discloses Personal Information to Riverside only for limited and specified purposes set out in this DPA and the Agreement. Riverside shall process all Personal Information only (i) for such limited and specific purpose(s), and (ii) in compliance with applicable sections of the CCPA. Riverside shall not (i) retain, use, or disclose Personal Information outside the direct business relationship of the Parties, as described in the Agreement, or for any business or commercial purpose other than for the specific business purpose of providing the Platform or as otherwise permitted by the CCPA, the Agreement and/or this DPA, nor (ii) combine Personal Information with Personal Information Riverside Processes on behalf of other parties unless expressly permitted under the CCPA, its implementing regulations and the Agreement between the Parties. Riverside further acknowledges that Customer has the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Riverside. Riverside shall notify Customer if Riverside makes a determination

that it can no longer meet its obligations under the CCPA.

3. **DATA SUBJECT REQUESTS**

Riverside shall, to the extent legally permitted, notify Customer or refer Data Subject or Consumer to Customer, if Riverside receives a request from a Data Subject or Consumer to exercise their rights (to the extent available to them under applicable Data Protection Laws) of access, right to rectification, restriction of Processing, erasure, data portability, objection to the Processing, their right not to be subject to automated individual decision making, to opt-out of the sale of Personal Information, or the right not to be discriminated against ("**Data Subject Request**"). Taking into account the nature of the Processing, Riverside shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible and reasonable, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. Riverside may advise Data Subjects on available features for self-exercising their Data Subject Requests through the Platform (where appropriate), or refer Data Subject Requests received, and the Data Subjects making them, directly to the Customer for its treatment of such requests.

4. **CONFIDENTIALITY**

Riverside shall ensure that its personnel and advisors engaged in the Processing of Personal Data (i) have committed themselves to confidentiality and (ii) are informed of the confidential nature of Personal Data and required to keep it confidential.

5. **SUB-PROCESSORS**

- 5.1 **Appointment of Sub-processors.** Customer provides Riverside a general authorization to engage with Sub-processors to perform the Processing described herein. Customer acknowledges and agrees that (a) Riverside's Affiliates may be engaged as Sub-processors; and (b) Riverside and Riverside's Affiliates on behalf of Riverside may each engage third-party Sub-processors in connection with the provision of the Platform.

5.2 **List of Current Sub-processors and Notification of New Sub-processors.**

- 5.2.1 Riverside makes available to Customer the current list of Sub-processors used by Riverside to process Personal Data, accessible [here](#). Such Sub-processor list includes the identities of those Sub-processors used by Riverside to Process the Personal Data solely on Customer's behalf, the entity's country and type of service ("**Sub-Processor List**"). The Sub-Processor List as of the data of first use of the Platform by Customer is hereby deemed authorized upon first use of the Platform.
- 5.2.2 Riverside shall provide notification of any new Sub-processor(s) before authorizing such new Sub-processor(s) to Process Personal Data in connection with the provision of the Platform (the "**Sub-processor Notice**").

- 5.3 **Objection to New Sub-processors.** Pursuant to the publication of a new Sub-processor Notice, Customer may reasonably object to Riverside's use of a new Sub-processor, for reasons relating to the protection of Personal Data intended to be Processed by such Sub-processor, by notifying Riverside promptly in writing to DPO@riverside.com within seven (7) days after receipt of notice by Riverside of such new appointment. Such written objection shall include the reasons for objecting to Riverside's use of such new Sub-processor. Failure to object to such new Sub-processor in writing within seven (7) days following Riverside's notice shall be deemed as acceptance of the new Sub-Processor. In the event Customer reasonably objects to a new Sub-processor, as permitted in the preceding sentences, Riverside will use reasonable efforts to make available to Customer a change in the Platform or recommend a commercially reasonable change to Customer's configuration or use of the Platform to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Riverside is unable to make available such change within thirty (30) days, Customer may, as a sole remedy, terminate the applicable Agreement and this DPA with respect only to those services or features of the Platform which cannot be provided by Riverside without the use of

the objected-to new Sub-processor, by providing written notice to Riverside. All amounts due under the Agreement before the termination date with respect to the Processing at issue shall be duly paid to Riverside and Customer shall not be entitled to any refunds. Until a decision is made regarding the new Sub-processor, Riverside may temporarily suspend the Processing of the affected Personal Data and/or suspend access to the Platform.

- 5.4 **Agreements with Sub-processors.** Riverside, or a Riverside Affiliate on behalf of Riverside, has entered into a written agreement with each Sub-processor containing appropriate safeguards for the protection of Personal Data. Where Riverside engages a Sub-processor for carrying out specific Processing activities on behalf of the Customer, the same or materially similar data protection obligations as set out in this DPA shall be imposed on such new Sub-processor by way of a contract, in particular obligations to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws. Where a Sub-processor fails to fulfil its data protection obligations concerning its Processing of Personal Data, Riverside shall remain responsible for the performance of the Sub-processor's obligations.

6. SECURITY & AUDITS

- 6.1 **Controls for the Protection of Personal Data.** Riverside shall maintain industry-standard technical and organizational measures for the protection of Personal Data Processed hereunder (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data, confidentiality and integrity of Personal Data, including those measures set forth in the Security Documentation), as may be amended from time to time. Upon the Customer's reasonable request, Riverside will reasonably assist Customer, at Customer's cost and subject to the provisions of Section 11.1 below, in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the Processing and the information available to Riverside.
- 6.2 **Audits and Inspections.** Upon Customer's 30 days' prior written request at reasonable intervals (no more than once every 12 months), and subject to strict confidentiality undertakings by Customer, and at Customer's expense, Riverside shall make available to Customer that is not a competitor of Riverside (or Customer's independent, reputable, third-party auditor that is not a competitor of Riverside and not in conflict with Riverside, subject to their confidentiality and non-compete undertakings) information necessary to demonstrate compliance with this DPA, and allow for and contribute to audits, including inspections, conducted by them, provided, however, that such auditor will not have access to non-Customer data. Riverside may satisfy the audit obligation under this section by providing Customer with attestations, certifications and summaries of audit reports conducted by accredited third party auditors. Any information, audits, inspections and the results therefrom, including the documents reflecting the outcome of the audit and/or the inspections, will only be used by Customer to assess compliance with this DPA, and shall not be used for any other purpose or disclosed to any third party without Riverside's prior written approval. Upon Riverside's first request, Customer shall return all records or documentation in Customer's possession or control provided by Riverside in the context of the audit and/or the inspection).
- 6.3 In the event of an audit or inspections as set forth above, Customer shall ensure that it (and each of its mandated auditors) will not cause (or, if it cannot avoid, minimize) any damage, injury or disruption to Riverside's premises, equipment, personnel and business while conducting such audit or inspection.
- 6.4 The audit rights set forth in 6.2 above, shall only apply to the extent that the Agreement does not otherwise provide Customer with audit rights that meet the relevant requirements of Data Protection Laws (including, where applicable, article 28(3)(h) of the GDPR or the UK GDPR).

7. DATA INCIDENT MANAGEMENT AND NOTIFICATION

Riverside maintains security incident management policies and procedures and, to the extent required under applicable Data Protection Laws, shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data Processed by Riverside on behalf of the Customer (a "**Data Incident**"). Riverside shall

make reasonable efforts to identify and take those steps as Riverside deems necessary and reasonable in order to remediate and/or mitigate the cause of such Data Incident to the extent the remediation and/or mitigation is within Riverside's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or anyone who uses the Platform on Customer's behalf. Customer will not make, disclose, release or publish any finding, admission of liability, communication, notice, press release or report concerning any Data Incident which directly or indirectly identifies Riverside (including in any legal proceeding or in any notification to regulatory or supervisory authorities or affected individuals) without Riverside's prior written approval, unless, and solely to the extent that, Customer is compelled to do so pursuant to applicable Data Protection Laws. In the latter case, unless prohibited by such laws, Customer shall provide Riverside with reasonable prior written notice to provide Riverside with the opportunity to object to such disclosure and in any case, Customer will limit the disclosure to the minimum scope required.

8. **RETURN AND DELETION OF PERSONAL DATA**

Following termination of the Agreement and subject thereto, Riverside shall, at the choice of Customer (indicated through the Services or by written notification to Riverside) delete or return to Customer all the Personal Data it Processes solely on behalf of the Customer in the manner described in the Agreement, and Riverside shall delete existing copies of such Personal Data unless Data Protection Laws require otherwise. To the extent authorized or required by applicable law, Riverside may also retain one copy of the Personal Data solely for evidence purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

9. **CROSS-BORDER DATA TRANSFERS**

- 9.1 **Transfers from the EEA, the United Kingdom and Switzerland to countries that offer adequate level of data protection.** Personal Data may be transferred from EU Member States, the three other EEA member countries (Norway, Liechtenstein and Iceland) (collectively, "**EEA**"), the United Kingdom ("**UK**") and Switzerland to countries that offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, the Member States or the European Commission, the UK, and/or Switzerland, including similarly approved mechanisms and frameworks ("**Adequacy Decisions**"), as applicable, without any further safeguard being necessary. For the avoidance of doubt, "**Adequacy Decisions**" include the European Commission's adequacy decision of 10 July 2023, establishing the EU-US Data Privacy Framework.
- 9.2 Riverside participates in and certifies compliance with the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and Swiss-U.S. Data Privacy Framework (together, the "**Data Privacy Framework**"). Riverside will (i) provide at least the same level of privacy protection as required by the Data Privacy Framework Principles; (ii) notify Customer if Riverside makes a determination it can no longer meet its obligation to provide the same level of protection as is required by the Data Privacy Framework Principles, and (iii) upon notice, including under the preceding subsection (ii), take reasonable and appropriate steps to remediate unauthorized processing.
- 9.3 If Riverside transfers Personal Data protected under this DPA to a jurisdiction for which the European Commission has not issued an adequacy decision, Riverside will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws and Regulations.
- 9.4 As applicable, if: (i) the Data Privacy Framework is invalidated; (ii) Riverside is no longer able to continue complying with the principles of the Data Privacy Framework; (iii) an adequacy recognition is invalidated or otherwise terminated, then a transfer of Personal Data outside of the EEA, the UK or Switzerland to Riverside shall be subject to Section 9.5.
- 9.5 **Transfers from the EEA, the United Kingdom and Switzerland to other countries.** If the Processing of Personal Data by Riverside includes a transfer (either directly or via onward transfer) from the EEA ("**EEA Transfer**"), the UK ("**UK Transfer**"), and/or Switzerland ("**Swiss Transfer**") to other countries which have not been subject to a relevant Adequacy Decision, and such transfers are not performed through an alternative recognized compliance mechanism as may be adopted by Riverside for the lawful transfer

of personal data (as defined in the GDPR, the UK GDPR, or the FADP, as relevant) outside the EEA, the UK or Switzerland, as applicable, then (i) the terms set forth in Part 1 of **Schedule 2** (EEA Cross Border Transfers) shall apply to any such EEA Transfer; (ii) the terms set forth in Part 2 of **Schedule 2** (UK Cross Border Transfers) shall apply to any such UK Transfer; (iii) the terms set forth in Part 3 of **Schedule 2** (Swiss Cross Border Transfers) shall apply to any such Swiss Transfer; and (iv) the terms set forth in Part 4 of **Schedule 2** (Additional Safeguards) shall apply to any such transfers.

10. **AUTHORIZED AFFILIATES**

- 10.1 **Contractual Relationship.** The Parties acknowledge and agree that, by executing the DPA, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, in which case each Authorized Affiliate agrees to be bound by the Customer's obligations under this DPA, if and to the extent that Riverside Processes Personal Data on the behalf of such Authorized Affiliates, thus qualifying them as the "**Controller**". All access to and use of the Platform by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Customer.
- 10.2 **Communication.** Customer shall remain responsible for coordinating all communication with Riverside under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

11. **OTHER PROVISIONS**

- 11.1 **Data Protection Impact Assessment and Prior Consultation.** Upon Customer's reasonable request, Riverside shall provide Customer, at Customer's cost, with reasonable cooperation and assistance needed to fulfil Customer's obligation under applicable Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Platform, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Riverside. Riverside shall provide, at Customer's cost, reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 11.1, to the extent required under applicable Data Protection Laws.
- 11.2 **Modifications.** Each Party may request in writing any variations to this DPA if they are required as a result of any change in, or decision of a competent authority under, any Data Protection Laws, to allow Processing of Customer Personal Data to be made (or continue to be made) without breach of those Data Protection Laws. Pursuant to such notice: (a) The Parties shall use commercially reasonable efforts to accommodate such modification requested by Customer or that Riverside believes is necessary; and (b) Customer shall not unreasonably withhold or delay agreement to any consequential variations to this DPA proposed by Riverside to protect Riverside against additional risks, or to indemnify and compensate Riverside for any further steps taken or costs incurred in connection with variations made at Customer's request. The Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the relevant Party's notice as soon as reasonably practicable.

SCHEDULE 1 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

1. Providing the Platform to Customer;
2. Performing the Agreement, this DPA and/or other contracts executed by the Parties;
3. Acting upon Customer's instructions, where such instructions are consistent with the terms of the Agreement;
4. Sharing Personal Data with third parties in accordance with Customer's instructions and/or pursuant to Customer's use of the Platform (e.g., integrations between the Platform and any services provided by third parties, as configured by or on behalf of Customer to facilitate the sharing of Personal Data between the Platform and such third-party services);
5. Complying with applicable laws and regulations;
6. All tasks related with any of the above.

Duration of Processing

Subject to any section of the DPA and/or the Agreement dealing with the duration of the Processing and the consequences of the expiration or termination thereof, Riverside will Process Personal Data pursuant to the DPA and Agreement for the duration of the Agreement, unless otherwise agreed upon in writing.

Type of Personal Data

Personal Data uploaded and/or generated by Customer in its use of the Platform, including through video and audio recordings. This may include:

- Audio and video recordings of participants in customer-organized sessions, including any third parties featured in those recordings.
- Transcripts, captions and AI-generated derivatives of those recordings (for example, summaries, chapters and clip suggestions).

Categories of Data Subjects

Customer may submit Personal Data to the Platform which may include, but is not limited to, Personal Data relating to the following categories of Data Subjects:

- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Any other third-party individual whose Personal Data Customer decides to have Processed through the Platform.

SCHEDULE 2 – CROSS BORDER TRANSFERS

STANDARD CONTRACTUAL CLAUSES

PART 1 – EEA-TRANS BORDER TRANSFERS

1. The parties agree that the terms of the EU SCCs are hereby incorporated by reference and shall apply to an EEA Transfer.
2. **Module One** (Controller to Controller) of the EU SCCs shall apply where the EEA Transfer is effectuated by both Customer and Riverside as the data controller of the Personal Data.
3. **Module Two** (Controller to Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data controller of the Personal Data and Riverside is the data processor of the Personal Data.
4. **Module Three** (Processor to Processor) of the EU SCCs shall apply where the EEA Transfer is effectuated by Customer as the data processor of the Personal Data and Riverside is a Sub-processor of the Personal Data.
5. Clause 7 of the EU SCCs (Docking Clause) shall not apply.
6. Option 2: GENERAL WRITTEN AUTHORISATION in Clause 9 of the EU SCCs shall apply, and the method for appointing and time period for prior notice of Sub-processor changes shall be as set forth in Section 5 of the DPA.
7. In Clause 11 of the EU SCCs, the optional language will not apply.
8. In Clause 17 of the EU SCCs, Option 1 shall apply, and the Parties agree that the EU SCCs shall be governed by the laws of the Republic of Ireland.
9. In Clause 18(b) of the EU SCCs, disputes will be resolved before the courts of the Republic of Ireland.
10. Annex I.A of the EU SCCs shall be completed as follows:

Data Exporter: Customer.

Contact details: As detailed in the Agreement.

Data Exporter Role:

Module One: The Data Exporter is a data controller.

Module Two: The Data Exporter is a data controller.

Module Three: The Data Exporter is a data processor.

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

Data Importer: Riverside

Contact details: As detailed in the Agreement.

Data Importer Role:

Module One: The Data Importer is a data controller.

Module Two: The Data Importer is a data processor.

Module Three: The Data Importer is a sub-processor.

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

11. Annex I.B of the EU SCCs shall be completed as follows:

The categories of data subjects are described in **Schedule 1** (Details of Processing) of this DPA.

The categories of personal data are described in **Schedule 1** (Details of Processing) of this DPA.

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

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

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

The period for which the personal data will be retained is for the duration of the Agreement, unless agreed otherwise in the Agreement and/or the DPA.

In relation to transfers to Sub-processors, the subject matter, nature, and duration of the processing is set forth at the link detailed in Section 5 of the DPA.

12. Annex I.C of the EU SCCs shall be completed as follows:

The competent supervisory authority in accordance with Clause 13 is the supervisory authority in the Member State stipulated in Section 9 above.

13. The Security Documentation referred to in the DPA serves as Annex II of the EU SCCs.

14. To the extent there is any conflict between the EU SCCs and any other terms in this DPA or the Agreement, the provisions of the EU SCCs will prevail.

PART 2 – UK TRANS-BORDER TRANSFERS

The Parties agree that the UK Addendum is hereby incorporated by reference and shall apply to UK Transfers as set forth in this Part 2.

Table 1: Parties: As stipulated in Section 10 of Part 1 of this **Schedule 2**.

Table 2: Selected SCCs, Modules and Selected Clauses: As stipulated in Part 1 of this **Schedule 2**.

Table 3: Appendix Information: Annex 1A: As stipulated in Section 10 of Part 1 of this **Schedule 2**; Annex 1B: As stipulated in Section 11 of Part 1 of this **Schedule 2**; Annex II: As stipulated in Section 13 of Part 1 of this **Schedule 2**; Annex III: As set forth at the link detailed in Section 5.2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes: Neither Party may end this UK Addendum in the manner set out in Section 19 of the Mandatory Clauses of the UK Addendum.

Mandatory Clauses: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

PART 3 – SWISS CROSS BORDER TRANSFERS

The Parties agree that the EU SCCs as detailed in Part 1 of this **Schedule 2**, shall be adjusted as set out below where the FADP applies to Swiss Transfers:

1. References to the Standard Contractual Clauses mean the EU SCCs as amended by this Part 3;
2. The Swiss Federal Data Protection and Information Commissioner shall be the sole Supervisory Authority for Swiss Transfers exclusively subject to the FADP;

3. The terms “General Data Protection Regulation” or “Regulation (EU) 2016/679” as utilized in the EU SCCs shall be interpreted to include the FADP with respect to Swiss Transfers;
4. References to Regulation (EU) 2018/1725 are removed;
5. Swiss Transfers subject to both the FADP and the GDPR shall be dealt with by the Swiss Federal Data Protection and Information Commissioner insofar as the Swiss Transfer is governed by the FADP, and by the EU Supervisory Authority named in Part 1 of this **Schedule 2**, insofar as the Swiss Transfer is governed by the GDPR;
6. References to the “Union”, “EU” and “EU Member State” shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of exercising their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;
7. Where Swiss Transfers are exclusively subject to the FADP, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP;
8. Where Swiss Transfers are subject to both the FADP and the GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FADP insofar as the Swiss Transfers are subject to the FADP.

PART 4 – ADDITIONAL SAFEGUARDS

1. In the event of an EEA Transfer, a UK Transfer, or a Swiss Transfer, the Parties agree to supplement these with the following safeguards and representations, where appropriate:
 - a. The data importer as defined in Part 1 of this **Schedule 2** shall have in place and maintain in accordance with good industry practice measures to protect the Personal Data from interception (including in transit from the data exporter as defined in Part 1 of this **Schedule 2** to the data importer and between different systems and services). This includes having in place and maintaining network protection intended to deny attackers the ability to intercept data and encryption of Personal Data whilst in transit and at rest intended to deny attackers the ability to read data.
 - a. The data importer will make commercially reasonable efforts to resist, subject to applicable laws, any request for bulk surveillance relating to the Personal Data protected under GDPR or the UK GDPR, or the FADP, including under section 702 of the United States Foreign Intelligence Surveillance Act (“FISA”);
 - b. If the data importer becomes aware that any government authority (including law enforcement) wishes to obtain access to or a copy of some or all of the Personal Data, whether on a voluntary or a mandatory basis, then unless legally prohibited or under a mandatory legal compulsion that requires otherwise:
 - I. The data importer shall inform the relevant government authority that Riverside is a processor of the Personal Data and that the data exporter, as the controller, has not authorized Riverside to disclose the Personal Data to the government authority, and inform the relevant government authority that any and all requests or demands for access to the Personal Data should therefore be notified to or served upon the Controller in writing;
 - II. The data importer will use commercially reasonable legal mechanisms to challenge any such demand for access to Personal Data which is under the data importer's control. Notwithstanding the above, (a) the data exporter acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access, and (b) if, taking into account the nature, scope, context and purposes of the intended government authority access to Personal Data, the data importer has a reasonable and good-faith belief that urgent access is necessary to prevent an imminent risk of serious harm to any individual or entity, this subsection (e)(II) shall not apply. In such event, the data

importer shall notify the data exporter, as soon as possible, following the access by the government authority, and provide the data exporter with relevant details of the same, unless and to the extent legally prohibited to do so.

2. Once in every 12-month period, the data importer will inform the data exporter, at the data exporter's written request, of the types of binding legal demands for Personal Data it has received and solely to the extent such demands have been received, including national security orders and directives, which shall encompass any process issued under section 702 of FISA.