StarTree Cloud and StarTree BYOC
Data Processing Addendum

This Data Processing Addendum ("**DPA**"), forms part of the StarTree Master Services Agreement or other applicable written or electronic terms of service or subscription agreement ("**Agreement**") between the StarTree entity which entered into the Agreement ("**StarTree**") and the **Customer** signatory thereto. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. The parties agree that this DPA shall replace any existing DPA or other data protection provisions the parties may have previously entered into in connection with the Services. In consideration of the mutual obligations set forth herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to the Agreement.

1. **Definitions**

(a) "**Agreement**" means the written or electronic agreement between Customer and StarTree for the provision of the Services to Customer.

(b) "**CCPA**" means Title 1.81.5 California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100–1798.199), as amended by the California Privacy Rights Act of 2020 ("**CPRA**") or otherwise, or superseded from time to time.

(c) "**Customer Personal Data**" means any Personal Data that is uploaded into the Cloud Services for storage or hosting that StarTree processes on behalf of Customer in the course of providing Services.

(d) "**Data Protection Laws**" means all data protection and privacy laws applicable to the processing of Customer Personal Data under the Agreement.

(e) "**EEA**" means the European Economic Area.

(f) "**EU GDPR**" means 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).

(g) "**GDPR**" means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.

(h) "**Security Incident**" means an unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

(i) "**Sell" or "Sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing or by electronic or other means, Customer Personal Data to a third party for monetary or valuable consideration.

(j) "**Services**" means any cloud service offering or BYOC offering provided by StarTree to Customer in which StarTree has access to Customer Personal data.

(k) "**Subprocessor**" means any Processor engaged by StarTree or its Affiliates to process Customer Personal Data. Subprocessors may include third parties or StarTree's Affiliates.

(l) **"UK GDPR"** means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

(m) The terms "**Business**", "**collect**", "**Consumer**", "**Controller**", "**Data Subject**", "**Processor**," "**process**,", "**processing**" and "**Personal Data**", and "**Service Provider**" have the meanings given to them in applicable Data Protection Laws.

2. Scope of this DPA

This DPA applies where and only to the extent that StarTree processes Customer Personal Data on behalf of Customer in the course of providing Services to the Customer pursuant to the Agreement.

3. Roles and Scope of Processing

3.1 <u>Role of the Parties</u>. As between the parties, Customer may act as Controller and/or Processor of Customer Personal Data and StarTree may act as Processor and/or subprocessor of Customer Personal Data.

3.2 <u>Customer as Controller of Customer Personal Data</u>. If Customer is Controller of Customer Personal Data, Customer agrees that (i) it will comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Customer Personal Data and any processing instructions it issues to StarTree; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary for StarTree to process Customer Personal Data pursuant to the Agreement and this DPA.

3.3 <u>Customer as Processor of Customer Personal Data</u>. If Customer is Processor of Customer Personal Data, Customer warrants on an ongoing basis that the relevant Controller has authorized: (i) StarTree's processing of Customer Personal Data as outlined in this DPA and in Exhibit A; (ii) Customer's appointment of StarTree as another processor; and (iii) StarTree's engagement of Subprocessors as described in Section 5 below.

3.4 <u>Customer Instructions</u>. StarTree will process Customer Personal Data only (i) for the purpose of providing the Services and in accordance with Customer's documented lawful instructions as set forth in the Agreement and this DPA; (ii) as part of the direct business relationship between Customer and StarTree; or (iii) as permitted by law. StarTree shall inform Customer if, in its opinion, Customer's processing instruction infringes applicable Data Protection Laws. The parties agree that the Customer's complete and final instructions regarding the nature and purposes of the processing are set out in this DPA. StarTree certifies that it understands the restrictions in this Section 3.4 and will comply with such restrictions.

3.5 <u>Details of Data Processing</u>

(a) <u>Subject matter</u>. The subject matter of the data processing under this DPA is Customer Personal Data.

(b) <u>Duration of the processing</u>. As between StarTree and Customer, the duration of the data processing under this DPA is the term of the Agreement.

(c) <u>Purpose of the processing</u>. Performance of the Services.

(d)   Nature of the processing: StarTree will use and otherwise process Customer Personal Data only in accordance with Customer's documented instructions and as described and subject to the terms of the Agreement and this DPA.

(e)   Categories of data subjects: The data subjects of Customer may include Customer's end users, employees, contractors, suppliers, and other third parties.

(f)   Types of Customer Personal Data. Personal data processed under this DPA include Customer Personal Data. Customer acknowledges that it solely chooses the nature and types of Customer Personal Data and that StarTree will be generally unaware of the details of Customer Personal Data processed within the Services.

4.   Data Transfers

4.1   Data Storage and Processing Facilities. Customer Personal Data will only be deployed in the geographic location(s) that Customer specifies via the Service (the "**Deployment Region**"). Customer is solely responsible for any transfer of Customer Personal Data caused by Customer's subsequent designation of other Deployment Regions. As part of providing the Services, including Support Services, StarTree may access Customer Personal Data anywhere in the world where StarTree, its Affiliates or its Subprocessors maintain data processing operations, however, StarTree will not access any Customer Personal Data within any OFAC sanctioned territories. StarTree will at all times provide an adequate level of protection for the Customer Personal Data processed, in accordance with the requirements of applicable Data Protection Laws.

4.2   Cross-Border Transfers. Where the transfer of Customer Personal Data is from the EEA, Switzerland or the United Kingdom to a territory which has not been recognized by the European Commission as providing an adequate level of protection for Customer Personal Data on the basis of Article 45 GDPR (or in the case of transfers from the United Kingdom, by the United Kingdom Government), StarTree agrees to process that Customer Personal Data in compliance with the provisions outlined in Exhibit A hereto, which forms an integral part of this DPA.

5.   Subprocessing

5.1   Authorized Subprocessors. Customer agrees that in order to provide the Services, StarTree may engage Subprocessors to process Customer Personal Data. StarTree maintains a list of its authorized Subprocessors on its website at https://startree.ai/legal/subprocessors.

5.2   Subprocessor Obligations. Where StarTree authorizes any Subprocessor as described in Section 5.1 above:

(a)   Access to Customer Personal Data will be limited only to what is necessary to assist StarTree in providing or maintaining the Services, and Subprocessor will be prohibited from accessing Customer Personal Data for any other purpose;

(b)   StarTree will enter or has already entered into a written agreement with the Subprocessor imposing data protection terms that require the Subprocessor to protect the Customer Personal Data to the standard required by applicable Data Protection Laws; and

(c) StarTree will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Subprocessor that cause StarTree to breach any of its obligations under this DPA.

Upon request and subject to any pre-existing confidentiality obligations, StarTree will provide Customer with all the relevant information it reasonably can in connection with its applicable Subprocessor agreements when required to satisfy Customer's obligations under applicable Data Protection Laws.

5.3 Subprocessor Updates. StarTree will provide Customer with a 30-day prior notice on its website if it intends to make any changes to its Subprocessors. Customer may, within 90 days of notification, object in writing to StarTree's appointment of a new Subprocessor, provided that such objection is based on reasonable grounds relating to the processing of Customer Personal Data by the new Subprocessor. In such event, the parties will discuss such objection in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred by Customer prior to suspension or termination).

6. Security Measures and Security Incident Response

6.1 Security Measures. StarTree has implemented and will maintain appropriate technical and organizational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of the Customer Personal Data ("**Security Measures**"). The Security Measures applicable to the Services are set forth in the StarTree Cloud Security Addendum available at https://startree.ai/legal/security, as updated or replaced from time to time in accordance with Section 6.2 below.

6.2 Updates to Security Measures. Customer has carried out its own review of the information made available by StarTree relating to data security and has made an independent determination that the Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that StarTree may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

6.3 Personnel. StarTree restricts its personnel from processing Customer Personal Data without authorization by StarTree as set forth in the Security Measures and shall ensure that any person who is authorized by StarTree to process Customer Personal Data is under an appropriate obligation of confidentiality and agrees to comply with applicable Data Protection Laws.

6.4 Customer Responsibilities. Without prejudice to StarTree's obligations under this DPA, and elsewhere in the Agreement, Customer is responsible for its secure use of the Services, including: (i) protecting account authentication credentials; (ii) protecting the security of Customer Personal Data when in transit to and from the Services; (iii) implementing measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (iv) taking any appropriate steps to securely encrypt or pseudonymise any Customer Personal Data uploaded to the Services.

6.5 Security Incident. In the event of a Security Incident, StarTree will notify Customer without undue delay, and in any case, where feasible, within seventy-two (72) hours of a confirmed Security Incident

and will provide updates to Customer. StarTree will reasonably cooperate with Customer as required to fulfil Customer's obligations under Data Protection Laws.

7. Audits

7.1 <u>Customer Audit Rights</u>. To the extent Customer's audit requirements under applicable Data Protection Laws cannot reasonably be satisfied through StarTree's relevant audit reports and certifications ("**Audit Reports**"), documentation or compliance information StarTree makes generally available to its customers or through reasonably written audit questions, which Customer may request no more than once per calendar year, StarTree will promptly respond to Customer's additional audit requests. Before the commencement of an audit, Customer and StarTree will mutually agree upon the scope, timing, duration, and control and evidence requirements, provided that this requirement to agree will not permit StarTree to unreasonably delay performance of the audit. To the extent needed to perform the audit, StarTree will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Personal Data by StarTree available. Neither Customer nor the third-party auditors, if any, shall have access to any data from StarTree's other customers or to StarTree systems or facilities not involved in the processing of Customer Personal Data. Customer is responsible for all costs and expenses related to such audit, including all reasonable costs and expenses for any time StarTree expends for any such audit.

8. Return or Deletion of Data

Upon termination or expiration of the Agreement, StarTree shall (at Customer's election) delete or return (in the same format sent to StarTree) all Customer Personal Data in its possession or control in accordance with the terms of the Agreement.

9. Cooperation

9.1 <u>Data Subject Request</u>. The Services provide Customer with the ability to retrieve and delete Customer Personal Data. Customer may use these controls to comply with Customer's obligations under applicable Data Protection Laws, including Customer's obligations related to any requests from data subjects involving Customer Personal Data ("**Data Subject Requests**"). To the extent that Customer is unable to independently access the relevant Customer Personal Data using such controls or otherwise, StarTree shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to such Data Subject Requests. If any such Data Subject Request is made directly to StarTree, StarTree shall, to the extent legally permitted: (i) advise the data subject to submit their Data Subject Request to Customer; (ii) promptly notify Customer; and (iii) not otherwise respond to that Data Subject Request without authorization from Customer unless legally compelled to do so. Customer will be responsible for responding to any such Data Subject Requests.

9.2 <u>Requests for Customer Personal Data</u>. If StarTree receives a subpoena, court order, warrant or other legal demand from law enforcement or public or judicial authorities seeking the disclosure of Customer Personal Data, StarTree shall, to the extent permitted by applicable laws, promptly notify Customer in writing of such request and reasonably cooperate with Customer to limit, challenge or protect against such disclosure.

9.3 <u>Legal Compliance</u>. To the extent StarTree is required under applicable Data Protection Laws, StarTree will (at Customer's expense) provide reasonably requested information regarding the Services to

enable the Customer to carry out data protection impact assessments and prior consultations with data protection authorities as required by law.

10.   CCPA Compliance

10.1   <u>Applicability</u>. This section 10 applies to the extent Customer is a Business that is subject to the CCPA and submits Personal Information (as that term is defined under CCPA) as part of Customer Personal Data in connection with StarTree's performance of the Agreement. Customer appoints StarTree as its Service Provider to collect and process the Customer Personal Data for the purposes outlined in section 3.4.

10.2   <u>Service Provider Commitments</u>. StarTree will not (a) Sell Customer Personal Data; (b) retain, use, or disclose the Customer Personal Data for any purpose other than for the Business Purpose, including to retain, use, or disclose the Customer Personal Data for a commercial purpose other than providing its Services under the Agreement; (c) retain, use, or disclose the Customer Personal Data outside of the direct business relationship between StarTree and the Customer; (d) process the Customer Personal Data for targeted and/or cross context behavioural advertising; (e) combine Customer Personal Data that it receives from, or on behalf of, Customer, with Personal Information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Consumer, if and to the extent such combination would be inconsistent with the limitations on Service Providers under the CCPA or other laws.

11.   General

11.1   For the avoidance of doubt, any claim or remedies the Customer and/or its Affiliates may have against StarTree, any of its Affiliates and their respective employees, agents and Subprocessors (hereinafter "**StarTree Group**") arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) for breach of cross-border data transfers and related provisions outlined in the Standard Contractual Clauses (to the extent applicable and as defined in Exhibit A hereto); (iii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer; and (iv) under applicable Data Protection Laws, including any claims relating to damages paid to a data subject, will be subject to any limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Such limitation of liability does not apply to any direct claim or remedies a data subject may have against Customer or StarTree. Customer further agrees that any regulatory penalties incurred by StarTree Group in relation to the Customer Personal Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce StarTree's liability under the Agreement as if it were liability to the Customer under the Agreement.

11.2   Any claims against StarTree or its Affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

11.3   To the extent reasonably necessary to comply with changes to applicable Data Protection Laws or in response to guidance or mandates issued by any court, regulatory body, or supervisory authority with jurisdiction over StarTree, StarTree may modify, amend, or supplement the terms of this DPA. StarTree will endeavour to provide prior written notice of any such changes to Customer by posting a notice on StarTree's website and/or in Customer's StarTree Cloud web portal, where applicable.

11.4   This DPA will be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by applicable Data Protection Laws.

11.5   Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in Exhibit A (Cross-Border Data Transfers); (2) the terms of this DPA outside of Exhibit A; and (3) the Agreement. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

11.6   If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, then the invalidity or unenforceability of such provision does not affect any other provision of this DPA and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

EXHIBIT A

CROSS-BORDER DATA TRANSFERS

1. **Definitions**

   (a) "**EU Standard Contractual Clauses (Controller-to-Processor)**" or **"EU SCCs (Controller-to-Processor)"** means Module 2 of the SCCs

   (b) "**EU Standard Contractual Clauses (Processor-to-Processor)**" or **"EU SCCs (Processor-to-Processor)"** means Module 3 of the SCCs

2. **EU Standard Contractual Clauses**

2.1 For transfers of Customer Personal Data from the EEA and/or Switzerland that are subject to Section 4.2 of the DPA:

   (a) Where Customer is a controller of Customer Personal Data, the EU SCCs (Controller-to-Processor) will apply and are incorporated into the DPA by reference; and

   (b) Where Customer is a processor of Customer Personal Data, the EU SCCs (Processor-to-Processor) will apply and are incorporated into the DPA by reference.

2.2 In relation to transfers of Customer Personal Data protected by the EU GDPR, the SCCs shall apply as follows:

   (a) Module Two terms shall apply (where Customer is the controller of Customer Personal Data) and the Module Three terms shall apply (where Customer is the processor of Customer Personal Data);

   (b) in Clause 7, the optional docking clause shall apply and Authorized Affiliates may accede the SCCs under the same terms and conditions as Customer, subject to mutual agreement of the parties;

   (c) in Clause 9, option 2 ("**general authorization**") is selected, and the process and time period for prior notice of Sub-processor changes shall be as set out in Section 4.3 of the DPA;

   (d) in Clause 11, the optional language shall not apply;

   (e) in Clause 17, option 1 shall apply and the SCCs shall be governed by Irish law;

   (f) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

   (g) Annex I shall be deemed completed with the information set out in Annex A to the DPA; and

   (h) Annex II shall be deemed completed with the information set out in the Security Addendum, subject to Section 6.1 (Security Measures) of the DPA.

2.3 In relation to transfers of Customer Personal Data protected by the UK GDPR, the SCCs as implemented under Section 1(a) above shall apply with the following modifications:

(i) "UK Addendum" means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioners Office under S.119 (a) of the UK Data Protection Act 2018, as updated or amended from time to time

(j) the SCCs shall be modified and interpreted in accordance with Part 2 of the UK Addendum, which shall be deemed incorporated into and form an integral part of the DPA;

(k) Tables 1, 2 and 3 in Part 1 of the UK Addendum shall be deemed completed with the information set out in the DPA and the Security Addendum respectively, and Table 4 in Part 1 of the UK Addendum shall be deemed completed by selecting "neither party"; and

(l) Any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

2.4 In relation to transfers of Customer Personal Data protected by the Swiss Data Protection Act, the SCCs as implemented under Section 1(a) above will apply with the following modifications:

(a) references to "Regulation (EU) 2016/679" and specific articles therein shall be interpreted as references to the Swiss Data Protection Act and the equivalent articles or sections therein;

(b) references to "EU", "Union", "Member State" and "Member State law" shall be replaced with references to "Switzerland" and/or "Swiss law" (as applicable);

(c) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland");

(d) the SCCs shall be governed by the laws of Switzerland ; and

(e) disputes shall be resolved before the competent Swiss courts.

2.5 Where the Standard Contractual Clauses apply pursuant to Section 8.1 of this DPA, this section sets out the parties' interpretations of their respective obligations under specific provisions of the Clauses, as identified below. Where a party complies with the interpretations set out below, that party shall be deemed by the other party to have complied with its commitments under the Standard Contractual Clauses:

(a) where Customer is itself a processor of Customer Personal Data acting on behalf of a third party controller and StarTree would otherwise be required to interact directly with such third party controller (including notifying or obtaining authorizations from such third party controller), StarTree may interact solely with Customer and Customer shall be responsible for forwarding any necessary notifications to and obtaining any necessary authorizations from such third party controller;

(b) the certification of deletion described in Clause 16(d) of the SCCs shall be provided by StarTree to Customer upon Customer's written request;

(c)   for the purposes of Clause 15(1)(a) the SCCs, StarTree shall notify Customer and not the relevant data subject(s) in case of government access requests, and Customer shall be solely responsible for notifying the relevant data subjects as necessary; and

(d)   Taking into account the nature of the processing, Customer agrees that it is unlikely that StarTree would become aware of Customer Personal Data processed by StarTree is inaccurate or outdated. To the extent StarTree becomes aware of such inaccurate or outdated data, StarTree will inform the Customer in accordance with Clause

3.   Alternative Data Export Solutions

3.1   Notwithstanding the foregoing, the parties agree that in the event StarTree adopts another alternative data export solution (as recognized under applicable Data Protection Laws), then the alternative data export solution shall apply instead of the Standard Contractual Clauses. In the event that the alternative data export solution is later determined to not constitute an adequate level of data protection under applicable Data Protection Laws, the Standard Contractual Clauses shall apply as the data export solution.