DATA PROCESSING ADDENDUM

1. Scope, Order of Precedence and Parties

1.1. This Data Processing Addendum ("**DPA**") applies to the Processing of Personal Information by the Parties in connection with the Customer Agreement and the UGC Agreement (together, "**the Agreements**") as applicable, and is incorporated by reference into each of them.

1.2. In the event of a conflict between the terms of either of the Agreements, the terms of this DPA and / or the EU Standard Contractual Clauses and/or the UK SCC Addendum (if applicable), the following order of precedence shall apply:
- **1.2.1.** the EU Standard Contractual Clauses and/or the UK SCC Addendum (if applicable)
- **1.2.2.** This DPA
- **1.2.3.** The Customer Agreement
- **1.2.4.** The UGC Agreement

2. Definitions and Interpretation

2.1. **Agreements** means the Customer Agreement and the UGC Agreement.

2.2. **Affiliate** means any subsidiary of Shuttlerock that may assist Shuttlerock in the processing of Personal Information under this DPA.

2.3. **Applicable Privacy Laws** means the New Zealand Privacy Act 2020, the Australian Privacy Act 1988, the EU Regulation 2016/679 (EU General Data Protection Regulation), the UK Data Protection Act 2018, the California Consumer Privacy Act as amended by the California Privacy Rights Act, and any other applicable privacy law in force in a relevant jurisdiction.

2.4. **Content Creator** has the same meaning as in the Shuttlerock Creator Program Terms and Conditions (the "**UGC Agreement**");

2.5. **Creator Content** means original digital content created by an independent content creator in their signature style, which features, promotes or markets a Shuttlerock customer's brand, product or services;

2.6. **Creator Profile Data** means all data, including personal information, about a Content Creator that is collected by Shuttlerock and used for the purposes of maintaining a working relationship with them, excluding Creator Content, as detailed in paragraph 4 of this DPA.

2.7. **Customer** has the same meaning as under the Shuttlerock Creative Services Terms and Conditions (the "**Customer Agreement**")

2.8. **Customer Data** means any data provided by the Customer to Shuttlerock for the purposes of Shuttlerock providing Services under the Customer Agreement, including but not limited to the Customer's Intellectual Property, and Initial Copyright Work, and which may include Personal Information about the Customer's employees or contractors, or any other party.

2.9. **Demand** has the meaning set forth in Section 4.

2.10. **Parties** means any of the Creator, the Customer and Shuttlerock.

2.11. **Personal Information** means any data processed in connection with the performance of either of the Agreements that can identify a unique living individual, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of individuals or as such information may be otherwise defined under Applicable Data Protection Laws.

2.12. **Privacy Breach** has the meaning given to it in any applicable jurisdiction, and in particular means the accidental or unauthorised use, deletion, loss, loss of access to, alteration, or disclosure of personal information, collected, transmitted, stored or otherwise processed for the purposes of performing the Agreements.

2.13. **UGC Agreement** means the Shuttlerock Creator Terms and Conditions.

3.   Roles: Data Controller and Data Processor

3.1. The Customer shall be:
   3.1.1. Data Controller of all Personal Information included within Customer Data; and
   3.1.2. Joint Data Controller, with the Content Creator and Shuttlerock, of all Personal Information included within the Creator Content, from the point at which they take possession of that Creator Content.

3.2. The Content Creator shall be:
   3.2.1. Joint Data Controller, with the Customer and Shuttlerock, of all Personal Information included within the Creator Content from the point at which they collect or create that Personal Information.
   3.2.2. Responsible as Joint Data Controller for:
      3.2.2.1.   Collecting Personal Information within the Creator Content,
      3.2.2.2.   Ensuring that all collection and subsequent processing is fair, lawful, and done via reasonable and foreseeable means, and only done with the express written consent of the data subject;

3.2.2.3. Providing all applicable information mandated to be provided under Applicable Privacy Laws at or before that Personal Information is collected. This includes but is not limited to the information stipulated under Article 13 of the EU and UK GDPR.

3.2.2.4. Deletion of all Personal Information after it is no longer necessary for the Content Creator to retain it, after it has been delivered or otherwise transferred to Shuttlerock.

3.3. Shuttlerock shall be:

3.3.1. Data Controller of all Personal Information within Creator Profile Data;

3.3.2. Joint Data Controller of all Personal Information within the Creator Content from the time at which they take possession of that Creator Content; and

3.3.3. Data Processor of all Personal Information within the Customer Data.

Data type	Data Controller	Joint Data Controllers	Processor
Customer Data	Customer	N/A	Shuttlerock
Creator Content	N/A	Content Creator Shuttlerock Customer	N/A
Creator Profile	Shuttlerock	N/A	Customer

3.4. In all circumstances where any party is a Data Processor it will only process Personal Information in line with the instructions of the Data Controller, and it will not process that Personal Information for any other purposes unless expressly agreed with the applicable Data Controller as identified at paragraph 3.1 to 3.3 above.

3.5. In circumstances where the Parties are Joint Data Controllers, each shall be jointly responsible for its obligations to any applicable data subject, starting from the time that it collects or receives the relevant Personal Information from the data subject, or any other Joint Data Controller. Notwithstanding the foregoing provision:

3.5.1. In relation to Creator Content, the Content Creator shall be responsible for providing the data subject with Shuttlerock and the Customer shall be responsible for providing the data subject with the information stipulated under Article 14 of the EU and UK GDPR.

3.6. In circumstances where a party is a sole Data Controller it will only process Personal Information in line with its obligations under Applicable Privacy Laws, and in a manner that is consistent with its public facing Privacy Policy or other privacy collection notice.

4. **Purposes of Processing**

4.1. Shuttlerock will only process the Customer Data for the specific purpose of performing the Services in line with the Customer Agreement, and any other ancillary document such as a Statement of Work, that contains the Customer's written instructions.

4.2. Shuttlerock will only process the Creator Content for the purpose of facilitating the effective completion of any SOW under a UGC Agreement, and further, for the purposes set out in its Privacy Policy, which can be found at *https://www.shuttlerock.com/privacy*.

4.3. Shuttlerock will only process the Creator Profile Data for the purposes of:

4.3.1. Finding and identifying Content Creators suitable to joint its UGC Program;

4.3.2. Onboarding Content Creators and administering the UGC program to provide Creator Program Services to Customers, as described and set out in the UGC Agreement. The Creator Profile Data is collected by Shuttlerock with the fully informed and freely given consent of the Content Creator, and on the basis that the collection and processing of each of the categories of Personal Information within the Creator Profile Data is necessary for the performance of the UGC Agreement.

4.4. The parties will not disclose any Personal Information for which they are a Data Controller in response to a subpoena, judicial or administrative order, or other binding instrument (a "Demand") unless required by law. Each party will promptly notify the any Joint Data Controller or applicable Processor of any Demand unless prohibited by law and provide the Data Contoller with reasonable assistance to facilitate that Data Controller's timely response to the Demand.

4.5. Shuttlerock may also aggregate Personal Information as part of the Services in order to provide, secure, and enhance Shuttlerock products and Services.

4.6. Shuttlerock may provide Personal Information to Affiliates in connection with any anticipated or actual merger, acquisition, sale, bankruptcy, or other reorganization of some or all of its business, subject to the obligation to protect

Personal Information consistent with the terms of this DPA.

4.7. Shuttlerock will not sell or share Personal Information within the meaning of those terms as set out in the California Consumer Privacy Act, as amended by the California Privacy Rights Act.

5. Categories of Personal Information to be Processed

5.1. In relation to Customer Data, the Customer shall determine the Personal Inforamtion that it provides to Shuttlerock, and where applicable the Content Creator, in order to perform the Services. This may involve the processing of Personal Information of the Customer's employees, contractors, suppliers, agents, customers, end users, as well as actors, models, or voice artists. The Customer has obtained the consent of the applicable data subject for the processing of any such personal information within the Customer Data for the purposes of engaging Shuttlerock under the Customer Agreement.

5.2. The Processing of Personal Information within Customer Data may include the following categories of Personal Information:
   5.2.1. Direct identifiers such as name, date of birth,
   5.2.2. Contact information such as home telephone number, cell telephone number, email address, home or postal mail address,
   5.2.3. Family and other personal circumstance information, such as age, date of birth, marital status, spouse or partner, and number of children,
   5.2.4. Employment information such as employer, work address, work email and phone, job title and function, manager,
   5.2.5. Other data such as services purchased, device identifiers, online profiles and behavior, and IP address;
   5.2.6. Other Personal Information to which the Customer provides Shuttlerock access in connection with the provision of the Services.

5.3. In relation to Creator Profile Data, the Personal Information will be about the Creator, and will include the following categories of Personal Information:
   5.3.1. Direct identifiers such as name, profile photo
   5.3.2. Contact information such as home telephone number, cell telephone number, email address, home or postal mail address,
   5.3.3. Banking information limited to that which is necessary to enable Shuttlerock or the Customer to pay the Content Creator for their services.
   5.3.4. Demographic information that will enable the Shuttlerock and the Customer to identify whether the Content Creator is suitable for engagement under the UGC Agreement for any particular SOW, including but not limited to hobbies and interests, speciality vertices, profile biog, social media links, age, gender and ethnicity.

5.4. In relation to the Creator Content, the Personal Information will be about either the Creator or any actor, model or voice artist featured in the Creator Content, and which the Content Creator has obtained explicit written consent to use for the purposes set out under the UGC Agreement. The Personal Information may include the following categories:

5.4.1. Direct identifiers including but not limited to their name;

5.4.2. Visual or audio information including but not limited to their still or moving image or their voice.

5.5. The Content Creator will only collect and process Personal Information for which it has the express written consent from the data subject. Evidence of that consent must be provided by the Content Creator to Shuttlerock before or at the same time that Creator Content is shared with or disclosed to Shuttlerock.

5.6. Shuttlerock will retain all consent evidence provided by Content Creators for the purpose of demonstrating compliance with its consent obligations under Applicable Privacy Laws. The ongoing retention of that consent evidence amounts to a legitimate business interest and as such it will not be deleted in response to any request for deletion by a data subject under Applicable Privacy Laws unless the data subject has sufficiently significant countervailing interests.

6. Sub-processing

6.1. Subject to the terms of this DPA, each Data Controller authorises the applicable Processor or Joint Data Controller to engage Sub-Processors and Affiliates for the Processing of Personal Information. These Sub-Processors and Affiliates are bound by written agreements that require them to provide at least the level of data protection required of Shuttlerock by the Agreement and this DPA.

6.2. Each Data Controller may ask the applicable Processor or Joint Data Controller to perform an audit on a Sub-Processor or to obtain an existing third-party audit report related to the Sub-Processor's operations to verify compliance with these requirements. Each Data Controller remains responsible at all times for such Sub-Processors' and Affiliates' compliance with the requirements of the Agreement, this DPA and Applicable Data Protection Laws.

6.3. A list of Shuttlerock's Sub-Processors and Affiliates, as well as a mechanism to obtain notice of any updates to the list, are available at https://www.shuttlerock.com/sub-processor-list. At least fourteen (14) calendar days before authorizing any new Sub-Processor to access Personal Information, Shuttlerock will update the list of Sub-Processors and Affiliates. Where Shuttlerock is a Processor (and not a Sub-Processor), the following terms apply:

6.3.1. If, based on reasonable grounds related to the inability of such Sub-Processor or Affiliate to protect Personal Information, the applicable Data Controller does not approve of a new Sub-Processor or Affiliate, then that Data Controller may terminate any subscription for the affected Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval.

6.3.2. If the affected Service is part of a suite (or similar single purchase of Services), then any such termination will apply to the entire suite.

6.3.3. After such termination, You shall remain obligated to make all payments required under any purchase order or other contractual obligation with Shuttlerock and shall not be entitled to any refund or return of payment from Shuttlerock.

7. International Transfer of Personal Information

7.1. All Personal Information of individuals in the UK or European Economic Area processed by Shuttlerock will be stored by default in the EU.

7.2. Notwithstanding the foregoing, in relation to the Customer Agreement:

7.2.1. the Customer and Shuttlerock may agree upon the location for storage of Personal Information, or

7.2.2. Shuttlerock may transfer Personal Information to other third countries as necessary to perform the Services, and the Customer appoints Shuttlerock to perform any such transfer in order to process Personal Information as necessary to provide the Services. Shuttlerock will follow the requirements of this DPA regardless of where such Personal Information is stored or Processed.

7.3. Where the Processing involves the international transfer of Personal Information under Applicable Data Protection Laws in the European Economic Area or the UK to Shuttlerock, Affiliates or Sub-Processors in a jurisdiction (i) that has not been deemed by the European Commission or the UK Information Commissioner's Office to provide an adequate level of data protection, and (ii) there is not another legitimate basis for the international transfer of such

Personal Information, such transfers are subject to either the 2021 EU Standard Contractual Clauses and/or the UK SCC Addendum (as applicable) or other valid transfer mechanisms available under Applicable Data Protection Laws. For international transfers subject to:

7.3.1. the 2021 EU SCCs, the parties hereby incorporate by reference the 2021 EU SCCs in unmodified form (Module Two where the Customer is a Data Controller and Shuttlerock is a Processor or Module One where the parties are Joint Data Controllers, as applicable).

7.3.2. the UK SCC Addendum, the parties hereby incorporate by reference the UK SCC Addendum in unmodified form.

7.4. The 2021 EU SCCs are available at source https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; and

7.5. The UK SCC Addendum are available at source https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf

7.6. The SCCs shall be between the applicable Data Controller and Processor or Joint Data Controllers, irrespective of location. For such purposes, the Data Controller will act as the Data Exporter on its own behalf and on behalf of any of if its own entities. For purposes of Clause 7 of the 2021 EU SCCs, any acceding entity shall enforce its rights through the applicable Data Controller.

7.7. Where the Processing involves the international transfer of Personal Information under other Applicable Privacy Laws to Shuttlerock, Affiliates or Sub-Processors, such transfers are subject to the data protection terms specified in in this DPA and Applicable Data Protection Laws.

8. Requests from Data Subjects

8.1. Shuttlerock will cooperate with any reasonable request by the Customer or Content Creator to give effect to a request by a data subject to exercise their rights in relation to their Personal Information for which Shuttlerock is Processor or Joint Controller in relation to the Customer Agreement or UGC Agreement, under any Applicable Privacy Laws.

8.2. Where necessary, Shuttlerock will notify its sub-processors and Affiliates of any such request to ensure that they take the appropriate action to give full effect to the Data Subject's request.

8.3. If Shuttlerock receives a request from a data subject to exercise one or more of their rights under Applicable Privacy Laws, Shuttlerock will direct the data subject to the Party who originally provided that Personal Information to Shuttlerock, and will not provide any substantive response to any such request unless so

requested by the applicable Party.

9. Security

9.1. The Parties shall implement and maintain appropriate administrative, technical, and organizational practices designed to protect Personal Information against any misuse or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information.

9.2. Shuttlerock's security practices are set forth at Appendix 1.

9.3. Shuttlerock seeks to continually strengthen and improve its security practices, and so reserves the right to modify the controls described herein. Any modifications will not diminish the level of security during the relevant term of Services.

9.4. Shuttlerock employees are bound by appropriate confidentiality agreements and required to take regular data protection training as well as comply with Shuttlerock corporate privacy and security policies and procedures.

10. Privacy Breach

10.1. In relation to Personal Information contained within Customer Data, Shuttlerock shall notify the Customer without undue delay after becoming aware of a Privacy Breach involving such Personal Information in Shuttlerock's possession, custody or control.

10.2. Such notification shall at least:
    10.2.1. describe the nature of the Privacy Breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Information records concerned;
    10.2.2. provide the name and contact details of the data protection officer or other contact where more information can be obtained; and
    10.2.3. describe the measures taken or proposed to be taken to address the Privacy Breach including, where appropriate, measures to mitigate its possible adverse effects. You will coordinate with Shuttlerock on the content of any public statements or required notices to individuals and/or Supervisory Authorities.

10.3. In relation to Personal Information contained in Creator Profile Data, Shuttlerock shall notify the Content Creator without undue delay after becoming aware of a Privacy Breach involving such Personal Information in Shuttlerock's possession, custody or control. Such notification shall at least include the types of information listed at 10.2 above.

10.4. In relation to Personal Information contained within Creator Content, each Joint Data Controller shall notify the other Joint Data Controllers without undue delay

after becoming aware of a Privacy Breach involving such Personal Information in their possession, custody or control.

11. Instructions and Providing Information and Assistance

11.1. The Customer may provide additional reasonable instructions to Shuttlerock related to the Processing of Personal Information that are necessary for the Customer and Shuttlerock to comply with their respective obligations under Applicable Privacy Laws as a Data Controller and Data Processor. Shuttlerock will comply with the Customer's reasonable instructions at no additional charge, provided that in the event that the Customer's instructions impose costs on Shuttlerock beyond those included in the scope of Services under the Agreement, the parties agree to negotiate in good faith to determine the additional costs. Shuttlerock will promptly inform the Customer if it believes that the instructions are not consistent with Applicable Privacy Laws, provided that Shuttlerock shall not be obligated to independently inspect or verify the Customer's Processing of Personal Information.

11.2. The Parties will provide each other with information reasonably necessary to assist the other Parties' compliance with their obligations under Applicable Privacy Laws, including without limitation Shuttlerock's obligations under the EU General Data Protection Regulation to implement appropriate data security measures, carry out a data protection impact assessment and consult the competent Supervisory Authority (taking into account the nature of Processing and the information available to Shuttlerock), and as further specified in this DPA.

12. Return and Deletion of Personal Information

12.1. Shuttlerock will return or provide an opportunity for the Customer to retrieve all Personal Information after the end of the provision of Services and delete existing copies. With respect to cloud services, the Customer shall have thirty (30) calendar days to download its Personal Information after termination of the Agreement and must contact Shuttlerock technical support for download access and instructions.

12.2. In the event the Customer does not contact Shuttlerock technical support for this purpose within 30 calendar days after the end of the provision of Services, Shuttlerock shall delete the Personal Information promptly, except for:
12.2.1. back-ups deleted in the ordinary course, and
12.2.2. retention as required by applicable law.

12.3. In the event of either (i) or (ii), Shuttlerock will continue to comply with the relevant provisions of this DPA until such data has been deleted.

13. Audit

13.1. In the event the information requested of Shuttlerock under Section 11 above does not satisfy the Customer's obligations under Applicable Data Protection Laws, the Customer may carry out an audit of Shuttlerock's Processing of Customer Personal Information up to one time per year or as otherwise required by Applicable Data Protection Laws. To request an audit, the Customer must provide Shuttlerock with a proposed detailed audit plan four weeks in advance, and Shuttlerock will work with the Customer in good faith to agree on a final written plan.

13.2. Any such audit shall be conducted at the Customers own expense, during normal business hours, without disruption to Shuttlerock's business, and in accordance with Shuttlerock's security rules and requirements. Prior to any audit, Shuttlerock undertakes to provide the Customer reasonably requested information and associated evidence to satisfy the Customer's audit obligations, and the Customer undertakes to review this information prior to undertaking any independent audit. If any of the requested scope of the audit is covered by an audit report issued to Shuttlerock by a qualified third-party auditor within the prior twelve months, then the parties agree that the scope of the Customer's audit will be reduced accordingly.

13.3. The Customer may use a third-party auditor with Shuttlerock's agreement, which will not be unreasonably withheld. Prior to any third-party audit, such auditor shall be required to execute an appropriate confidentiality agreement with Shuttlerock. If the third party is the Customer's Supervisory Authority and applicable law enables it to audit Shuttlerock directly, Shuttlerock will cooperate with and provide reasonable assistance to the Supervisory Authority in accordance with Applicable Data Protection Laws.

13.4. The Customer will provide Shuttlerock with a copy of any final report unless prohibited by Applicable Data Protection Laws, will treat the findings as Confidential Information in accordance with the terms of the Customer Agreement (or confidentiality agreement entered into between You and Shuttlerock), and use it solely for the purpose of assessing Shuttlerock's compliance with the terms of the Customer Agreement, this DPA, and Applicable Data Protection Laws.

14. Data Protection Officer

14.1. Shuttlerock's global Data Protection Officer can be contacted c/o Shuttlerock, Level 1, 47 Bridge Street, Nelson 7010, Nelson, New Zealand. The Customer may include the contact information for any appointed Data Protection Officer in their order for Services.

15. Term

15.1. This Agreement becomes effective upon engagement by the Customer or Content Creator with Shuttlerock under either the Customer Agreement or UGC Agreement as applicable.

Appendix 1 - Services Security

Description of the Technical and Organisational Security Measures implemented by Shuttlerock

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal information	Shuttlerock has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest. Shuttlerock uses only recommended secure cipher suites and protocols to encrypt all traffic in transit and Customer Data is securely encrypted with strong ciphers and configurations when at rest.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Shuttlerock's customer agreements contain strict confidentiality obligations. Additionally, Shuttlerock requires every downstream Sub-processor to sign confidentiality provisions that are substantially similar to those contained in Shuttlerock's customer agreements. Shuttlerock has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for ensuring the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident	Daily, weekly and monthly backups of production datastores are taken. Backups are periodically tested in accordance with information security and data management policies.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Shuttlerock has undergone a SOC 2 Type 2 audit that includes the Security and Processing Integrity Trust Service Criteria.
Measures for user identification and authorization	Shuttlerock uses secure access protocols and processes and follows industry best-practices for authentication, including Multi Factor Authentication (MFA) and Single Sign On (SSO). Shuttlerock deploys two-factor authentication across many of its systems, and network infrastructure is securely configured to vendor and industry best practices to block all unnecessary ports, services, and unauthorized network traffic.
Measures for the protection of data during transmission	Shuttlerock has deployed secure methods and protocols for transmission of confidential or sensitive information over public

	networks. Shuttlerock uses only recommended secure cipher suites and protocols to encrypt all traffic in transit (i.e. TLS 1.2)
Measures for the protection of data during storage	Encryption-at-rest is automated using AWS's transparent disk encryption, which uses industry standard AES-256 encryption to secure all volume (disk) data. All keys are fully managed by AWS.
Measures for ensuring physical security of locations at which personal information are processed	All Shuttlerock processing occurs in physical data centers that are managed by sub-processors. The list of the sub-processors Shuttlerock engages with can be found here https://www.shuttlerock.com/sub-processor-list.
Measures for ensuring events logging	Shuttlerock monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is managed by the security and engineering teams. Log activities are investigated when necessary and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Shuttlerock adheres to a change management process to administer changes to the production environment for the Services, including changes to its underlying software, applications, and systems. All production changes are automated through CI/CD tools to ensure consistent configurations.
Measures for internal IT and IT security governance and management	Shuttlerock maintains a SOC 2 Type II compliant risk-based information security governance program. The framework for Shuttlerock's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Services and confidentiality, integrity, and availability of Customer Data.
Measures for certification/assur ance of processes and products	Shuttlerock undergoes annual SOC 2 Type II audits.
Measures for ensuring data minimisation	Shuttlerock's customers unilaterally determine what customer personal information they route through the Services. As such, Shuttlerock operates on a shared responsibility model. Shuttlerock gives Customers control over exactly what personal information enters the platform. All Customer Data is deleted from the Services following Shuttlerock's Data Retention Plan and Data Deletion Policy.
Measures for ensuring data quality	Shuttlerock has a multi-tiered approach for ensuring data quality. These measures include: (i) unit testing to ensure quality of logic used to process API calls, (ii) database schema validation rules which execute against data before it is saved to our database, (iii) a schema-first API design using GraphQL and strong typing to enforce a strict contract between official clients and API resolvers. Shuttlerock applies these measures across the board, both to ensure the quality of any usage data that Shuttlerock collects and to ensure that the Shuttlerock

	platform is operating within expected parameters. Shuttlerock ensures that data quality is maintained from the time a Customer sends Customer Data into the Services and until that Customer Data is presented or exported.
Measures for ensuring limited data retention	Shuttlerock Customers unilaterally determine what Customer Data they route through the Services. As such, Shuttlerock operates on a shared responsibility model. If a Customer is unable to delete Customer personal information via the self-services functionality of the Services, then Shuttlerock deletes Customer Data upon the Customer's written request, within the timeframe specified in this DPA and in accordance with Applicable Data Protection Laws. All Customer Data is deleted from the Services following Shuttlerock's Data Retention Plan and Data Deletion Policy.
Measures for ensuring accountability	Shuttlerock has adopted measures for ensuring accountability, such as implementing data protection and information security policies across the business, recording and reporting Security Incidents involving personal information, and formally assigning roles and responsibilities for information security and data privacy functions. Additionally, Shuttlerock conducts regular third-party audits to ensure compliance with our privacy and security standards.
Measures for allowing data portability and ensuring erasure	All personal information in the Services may be deleted by the Customer or at the Customer's request. personal information is incidental to Shuttlerock's Services. Based on Privacy by Design and Data Minimization principles, Shuttlerock severely limits the instances of personal information collection and processing within the Services. Most use cases for porting personal information from Shuttlerock are not applicable. However, Shuttlerock will respond to all requests for data porting in order to address Customer needs.
Technical and organizational measures of sub-processors	Shuttlerock enters into Data Processing Agreements with its authorized Sub-Processors with data protection obligations substantially similar to those contained in this Addendum.