Customer Data Processing Addendum

This Data Processing Addendum ("**DPA**") is entered into between Runway AI, Inc. ("**Vendor**"), and the entity identified below and its Affiliates (**"Customer"**). Customer and Vendor may each be referred to as a "Party" and collectively referred to as the "Parties." This DPA is incorporated by reference into the Enterprise Services Agreement between Vendor and Customer that governs Customer's use of the Services provided by Vendor ("**Agreement**"). All capitalized terms used in this DPA but not defined shall have the meaning set forth in the Agreement. The DPA is effective as of the date of last signature or, if no such date exists, the effective date of the Agreement ("**Effective Date**"). To the extent of any conflict or inconsistency between this DPA and the remaining terms of the Agreement, this DPA will govern. All terms and conditions of the Agreement that do not conflict with this DPA shall remain effective.

1. Definitions

"**Applicable Law(s)**" means all applicable laws, regulations, and other legal or regulatory requirements in any jurisdiction relating to privacy, data protection/security, or the Processing of Personal Data, including without limitation the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and its amendments and implementing regulations ("**CCPA**"), privacy laws passed by other U.S. states (together with the CCPA, "**U.S. State Privacy Laws**"), the United Kingdom Data Protection Act 2018, and the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**").

"**EEA**" means the European Economic Area, which constitutes the member states of the European Union and Norway, Iceland and Liechtenstein, as well as, for the purposes of this DPA, Switzerland and the United Kingdom.

"**EU SCCs**" means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 *on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.

"**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"**Customer Personal Data**" or "**Personal Data**" includes "personal data," "personal information," and "personally identifiable information" processed by Vendor on behalf of Customer to provide the Services, and such terms shall have the same meaning as defined by Applicable Law.

"**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, creating, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making such data available, alignment or combination, restriction, erasure or destruction.

"**Services**" means the enterprise services provided by Vendor to Customer as specified in the Agreement.

"**Standard Contractual Clauses**" means the EU SCCs or the UK SCCs, as applicable.

"**UK SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the effective date at https://ico.org.uk/media2/migrated/4019538/international-data-transfer-agreement.pdf) and completed as described in the "Data Transfers" section below.

2. Relationship of the Parties

2.1. For purposes of this DPA, Vendor acts as a processor of Customer to process Personal Data. Customer acts as either a controller or processor of Personal Data.

3. Scope and Purposes of Processing

3.1 Purpose Limitation.

(a) Vendor shall process Personal Data solely: (i) to fulfill its obligations to Customer under the Agreement, including this DPA; (ii) on Customer's behalf; and (iii) in compliance with Applicable Laws.

(b) Vendor will not (i) sell or share (as such terms are defined in Applicable Laws) Personal Data, (ii) Process Personal Data outside of the direct business relationship between Customer and Vendor, (iii) process Personal Data for any purpose other than for the specific purposes set forth in the Agreement, or (iv) otherwise engage in any Processing of the Personal Data outside of what a processor or Service Provider may engage in under Applicable Law, unless obligated or permitted to do otherwise by Applicable Law.

(c) Vendor shall comply with any applicable restrictions under Applicable Laws on combining the Personal Data with personal data that Vendor receives from, or on behalf of, another person or persons, or that Vendor collects from any interaction between it and any individual.

(d) Vendor will immediately inform Customer if Vendor is legally required to Process Personal Data in a manner that is inconsistent with Customer's instructions (unless legally prohibited from providing such notice) or if an instruction from Customer infringes Applicable Law.

(e) Further details regarding Vendor's Processing operations, including the purposes for Processing Personal Data, are set forth in Exhibit A.

3.2 Notification of Inability to Comply. Vendor will notify Customer after Vendor determines that it can no longer meet its obligations under Applicable Laws.

3.3 Remediation. Customer shall have the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data by Vendor.

4. Subcontracting

4.1 Subprocessors. Vendor's current third-party subprocessors are listed at https://runwayml.com/customer-subprocessors/ (the

"Subprocessor List"). Prior to a subprocessor's Processing of Personal Data, Vendor will impose contractual obligations on the subprocessor substantially the same as those imposed on Vendor under this DPA. Vendor remains liable for its subprocessors' performance under this DPA to the same extent Vendor is liable for its own performance.

4.2 Notification & Right to Object. Vendor shall notify Customer of new subprocessors by email or by update of the website available at https://runwayml.com/customer-subprocessors/, where Customer may subscribe to email notifications. Customer may object to Vendor's use of a new subprocessor by notifying Vendor at legal@runwayml.com within fifteen (15) days after receipt of Vendor's notice. In the event Customer offers legitimate objections to a new subprocessor, Vendor will use reasonable efforts to make available to Customer a change in the services or recommend a commercially reasonable change to Customer's use of the services to avoid Processing of Personal Data by the objected-to subprocessor without unreasonably burdening the Customer. In the event that the Parties fail to agree within five days, Customer may in the following thirty days terminate the affected part of the Service.

5. Assistance & Cooperation

5.1 Security. Vendor shall maintain (and require its subprocessors to maintain) reasonable and appropriate technical and organizational measures to protect Personal Data, as set forth in Annex II of Exhibit A. Vendor shall ensure that persons authorized to carry out processing have committed themselves to confidentiality or are under the appropriate statutory obligation of confidentiality.

5.2 Personal Data Breach Notification & Response. Vendor shall inform Customer of a Personal Data Breach without undue delay or within the time period required under Applicable Law, and in any event no later than forty-eight (48) hours following such confirmation. To the extent available, this notification will include Vendor's then-current assessment of the following, which may be based on incomplete information:

(a) the nature of the Personal Data Breach, including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

(b) the likely consequences of the Personal Data Breach; and

(c) measures taken or proposed to be taken by Vendor to address the Personal Data Breach, including, where applicable, measures to mitigate its possible adverse effects.

At Vendor's own expense, Vendor will investigate the Personal Data Breach and take all necessary steps to mitigate the effects of the Personal Data Breach and reduce the risk to data subjects whose Personal Data was involved.

6. Responding to Requests & Complaints

Vendor shall promptly, and in any event without undue delay, notify Customer of (i) any third-party or data subject requests or complaints regarding the Processing of Personal Data; or (ii) any government or data subject requests for access to or information about Vendor's Processing of Personal Data on Customer's behalf and await written instructions from Customer on how, if at all, to assist in responding to the request, unless prohibited by Applicable Law. Vendor will provide Customer with reasonable cooperation and assistance in relation to any such request.

7. DPIAs and Consultation with Supervisory Authorities or other Regulatory Authorities

Upon Customer's written request, Vendor shall provide Customer with reasonable cooperation and assistance as needed and appropriate to fulfill Customer's obligations under Applicable Law to carry out a data protection impact assessment related to Customer's use of the Services. Vendor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority (as defined under the GDPR) in the performance of its tasks relating the data protection impact assessment, and to the extent required under Applicable Law.

8. Data Transfers

8.1 With respect to Personal Data transferred from the EEA, the EU SCCs shall apply and form part of this DPA. For purposes of the EU SCCs, they shall be deemed completed as follows:

(a) Where Customer acts as a controller with respect to Personal Data subject to the EU SCCs, its Module 2 applies. Where Customer acts as a processor with respect to Personal Data subject to the EU SCCs, its Module 3 applies.

(b) Clause 7 (the optional docking clause) is included.

(c) Under Clause 9 (Use of sub-processors), the parties select Option 2 (General written authorization), and the time period for notice of subprocessor changes is specified in Section 4.2 (Notification & Right to Object).

(d) Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

(e) Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of Ireland.

(f) Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of Ireland.

(g) Annexes I and II of the EU SCCs are set forth in Exhibit A below.

(h) Annex III of the EU SCCs (List of subprocessors) is inapplicable.

8.2 With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the UK SCCs shall apply and form part of this DPA. For purposes of the UK SCCs, they shall be deemed completed as follows:

(a) Table 1 of the UK SCCs: The Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer,

including those set forth in Exhibit A. The Key Contact shall be the contacts set forth in Exhibit A.

(b) Table 2 of the UK SCCs: The Approved EU SCCs referenced in Table 2 shall be the EU SCCs as executed by the Parties pursuant to this Addendum.

(c) Table 3 of the UK SCCs: Annex 1A, 1B, and II shall be set forth in Exhibit A.

(d) Table 4 of the UK SCCs: Customer may end this Addendum as set out in Section 19 of the UK SCCs.

(e) By entering into this DPA, the Parties are deemed to be signing the UK SCCs and their applicable Tables and Appendix Information.

8.3 With respect to Personal Data transferred from Switzerland for which Swiss law (and not the law in any European Economic Area jurisdiction) governs the international nature of the transfer, the EU SCCs shall apply and shall be deemed to have the following differences to the extent required by the Swiss Federal Act on Data Protection ("FADP"):

(a) References to the GDPR in the EU SCCs are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR.

(b) The term "member state" in the EU SCCs shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs.

(c) References to personal data in the EU SCCs also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope.

(d) Under Annex I(C) of the EU SCCs (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the EU SCCs insofar as the transfer is governed by the GDPR.

9. Audits

Vendor obtains annual third-party certifications and audits, which Vendor may make available to Customer as Vendor's Confidential Information to be used by Customer strictly for Customer's determination of Vendor's compliance with this DPA. If Customer has a reasonable basis to conclude that such information provided by Vendor is not satisfactory to confirm such compliance, Customer may, upon reasonable prior notice, carry out an audit of Vendor's policies, procedures, and records relevant to the Processing of Customer Personal Data when required by Applicable Law or Customer's supervisory authority. All such audits will be conducted: (i) upon the reasonable notice to Vendor; (ii) no more than once per twelve-month period, unless directed otherwise by a regulator or supervisory authority; (iii) during Vendor's normal business hours; and (iv) subject to reasonable confidentiality measures.

10. Return or Destruction of Personal Data

Except to the extent required otherwise by Applicable Laws, Vendor will, at the choice of Customer, return to Customer and/or securely destroy all Personal Data upon written request of Customer after the termination of the Agreement. Except to the extent prohibited by Applicable Laws, Vendor will inform Customer if it is not able to return or delete the Personal Data.

Exhibit A

Annexes I and II of the EU SCCs

A. LIST OF PARTIES

Data exporter(s):

The data exporter is the Customer operating in the countries which belong to the European Economic Area, UK and/or Switzerland and/or, to the extent agreed by the Parties, Customer in any other country to the extent the GDPR applies.

Customer will provide Customer's contact person's name, position and contact details as well as (if appointed) the data protection officer's name and contact details and (if relevant) the representative's contact details.

Activities relevant to the data transferred under these Clauses: Obtaining the Services from Data Importer

Role (controller/processor): Controller (for Module 2) or Processor (for Module 3)

Data importer(s):

Name: Runway AI, Inc.

Address: 18 West 18th Street, 11th Floor, New York, NY 10011, USA

Contact person's name, position and contact details: Runway Legal, legal@runwayml.com

Activities relevant to the data transferred under these Clauses: Providing the Service to Data Exporter

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Individuals depicted in images, videos, or audio or voice samples/clones uploaded or generated by Customer

Categories of personal data transferred

Images and videos; audio and voice samples/clones

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

In the event that data exporter provides sensitive data (e.g., certain voice data or facial image data), data importer will follow the safeguards set forth in Annex II, including access restrictions, encryption, logging, and transport security to protect it.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuously, for the length of the Agreement between the parties.

Nature of the processing

Personal data will be processed for purposes of fulfilling Vendor's obligations to Customer under the Agreement and the DPA.

Purpose(s) of the data transfer and further processing

Personal data will be processed for purposes of fulfilling Vendor's obligations to Customer under the Agreement and the DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data shall be retained for the length of time necessary to provide the services under the Agreement, or as otherwise required by applicable law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Vendor's subprocessors will process personal data to assist Vendor in providing the services pursuant to the Agreement, for as long as needed for Vendor to provide the services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13.

The parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Physical Security
Runway AI, Inc.'s production servers are maintained by third-party cloud service providers, such as AWS and GCP. The physical and environmental security protections are the responsibility of such cloud service providers. Runway AI, Inc. reviews the attestation reports and performs a risk analysis of such cloud service providers on at least an annual basis.

Logical Access
Runway AI, Inc. provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes. Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are regularly reviewed to ensure least privilege access. Runway maintains password management and lockout policies designed to ensure strong passwords consistent with industry standard practices and requires use of multi-factor authentication to access Runway production systems containing Customer Personal Data. Management & Leadership is responsible for provisioning access to the system based on the employee's role and performing a background check upon hire. Runway AI, Inc. conducts mandatory security awareness training for all employees at the time of hire.When an employee is terminated, Management & Leadership is responsible for deprovisioning access to all in scope systems within 1 day of that employee's termination.

Change Management
Runway AI, Inc. maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures. A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Patch Management
Runway AI, Inc. takes a proactive approach to patch management. Runway maintains up-to-date anti-malware software, has implemented a vulnerability management program with regular scanning for vulnerabilities, subscribes to a vulnerability notification service, has a method for prioritizing vulnerability remediation based on risk, and has established remediation timeframes based on risk rating. Once a patch is released, and the associated security vulnerability has been reviewed and assessed for its applicability and importance, the patch is applied and verified in a timeframe which is commensurate with the risk posed to its systems. The CTO and engineers regularly monitor various websites, message boards, and mailing lists where notifications of bug- related patches are often disclosed through public announcement by the vendor. The backend team reviews the availability of patches and independently determines if it is necessary to deploy within the production environment. Approved patches applied in a test environment, validated, and then applied to the production environment.

Problem Management
Runway AI, Inc. maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents. Runway AI, Inc. internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements. Runway AI, Inc. utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

System Monitoring
A variety of tools are used for threat detection purposes and will surface diagnostic logs to a Log Analytics Workspace for further review and analysis. Network flow logs will be captured by network security groups where they can be analyzed using the AWS Network Watcher. The vulnerability assessment process involves - threat modeling, implementation of antivirus software or hardened OS, and system patching. Alerts are sent immediately when a potential virus threat is detected, and logs are generated and retained for at least one year with at least three months readily available. AWS services are used to identify newly emerging vulnerabilities and will also periodically scan your deployed resources for insecure configurations as well as known vulnerabilities and will provide the appropriate remedy (such as applying a patch, hardening your resource configuration in a specific manner, etc.). The organization also monitors vendors for patch updates to remediate 0-day vulnerabilities.

Backup and Disaster Recovery

Runway maintains processes, procedures, and controls to ensure the required level of continuity for information security during an adverse situation. Runway maintains contingency plans to address emergencies that could damage or destroy Customer Content, including a data backup plan and a disaster recovery plan.

Data Protection
Runway implements encryption key management procedures and encrypts Customer Content in transit (TLS 1.2+) and at rest using a minimum of AES-128 bit cipher. Runway assigns roles and responsibilities for information security to respective owners to develop, implement, and manage Runway's administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of Customer Content. Runway maintains policies establishing data retention and secure destruction requirements.

Audit and Testing
Runway engages an independent external auditor to conduct annual reviews of its security practices against recognized audit standards, such as SOC 2 Type II audits. Runway creates, protects, and retains information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. Runway reviews and analyzes audit records on a regular basis to detect significant unauthorized activity. Runway ensures that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Runway performs periodic network and application vulnerability testing, manual or automated, at least once every year. Runway regularly undergoes security assessment activities (including dynamic and static scans). Runway contracts with independent third parties to perform penetration testing and vulnerability scanning on the Services at least annually. Runway implements procedures to document and address vulnerabilities discovered during vulnerability and penetration tests. Any remediation items identified as a result of the assessment are resolved as soon as possible on a timetable commensurate with the risk. Upon request, Runway will provide summary details of the tests performed, findings, and whether the identified issues have been resolved.