DeepFabric

DEEPFABRIC DATA PROCESSING ADDENDUM

Version: [YYYY-MM-DD]

This Data Processing Addendum ("DPA") forms part of the DeepFabric Master Service Agreement (the "MSA") between UNPLATFORMS, INC. d/b/a DeepFabric ("Provider") and the customer identified in the applicable Order Form ("Customer").

This DPA is incorporated pursuant to Section 6.4 of the MSA and applies where Provider Processes Customer Personal Data on behalf of Customer in connection with the Services.

Capitalized terms not defined in this DPA have the meanings given in the MSA.

1. Scope and Applicability

1.1 Applicability. This DPA applies where Provider Processes Customer Personal Data on behalf of Customer as a Processor or Subprocessor under applicable Data Protection Laws. It does not govern Processing for which Provider acts as an independent Controller, including its own business administration and account management, to the extent permitted by law.

1.2 Duration. This DPA becomes effective when incorporated into the Agreement and remains applicable for as long as Provider Processes Customer Personal Data on Customer's behalf, including any authorized implementation activities and lawful retention following expiration or termination of the Services.

1.3 Relationship to the Agreement. This DPA supplements the MSA and does not expand the Services or processing activities authorized under the applicable Order Form. In the event of a conflict concerning the Processing or protection of Customer Personal Data, this DPA controls for its specified data-protection subject matter, subject to applicable law and mandatory international-transfer instruments. The MSA otherwise governs.

2. Definitions and Roles

2.1 Definitions. For purposes of this DPA:

- **"Customer Personal Data"** means Personal Data Processed by Provider on Customer's behalf in connection with the Services, including Personal Data contained in Customer Data, AI Outputs, or related technical records. Information remains subject to this DPA for as long as it constitutes Personal Data under applicable law, regardless of its designation under the MSA.
- **"Data Protection Laws"** means privacy and data-protection laws applicable to the Processing of Customer Personal Data under the Agreement, including, where applicable, the EU General Data Protection Regulation ("EU GDPR"), UK GDPR, California Consumer Privacy Act as amended ("CCPA"), and other applicable U.S. state privacy laws.
- **"Personal Data"** means information relating to an identified or identifiable individual, or otherwise constituting personal data or personal information under applicable Data Protection Laws.
- **"Controller," "Processor," "Processing," and "Data Subject"** have the meanings assigned under applicable Data Protection Laws, including equivalent roles such as business and service provider where relevant.

- **"Subprocessor"** means a third party, including a Provider Affiliate, engaged by Provider to Process Customer Personal Data on Customer's behalf.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.
- **"Restricted Transfer"** means a transfer of Personal Data requiring an international-transfer safeguard under applicable Data Protection Laws.

2.2 Roles. Customer acts as Controller or, where Customer processes Personal Data on behalf of another Controller, as Processor. Provider acts as Processor or Subprocessor, as applicable, when Processing Customer Personal Data on Customer's behalf.

2.3 Compliance. Each Party will comply with Data Protection Laws applicable to its role. Customer is responsible for determining the lawful purposes of Processing, providing required notices, establishing appropriate legal bases, and ensuring that its instructions to Provider are lawful. Where Customer acts as a Processor, Customer represents that it has the authority necessary to instruct and authorize Provider's Processing.

3. Processing Instructions

3.1 Documented Instructions. Provider will Process Customer Personal Data only on Customer's documented instructions, including those reflected in the Agreement, applicable Order Forms, authorized workflows and configurations, and other written instructions consistent with the Agreement. Such Processing may include hosting, storing, organizing, analyzing, transforming, transmitting, securing, supporting, and otherwise Processing Customer Personal Data as necessary to provide the Services described in Schedule A.

3.2 Legal Requirements. Provider may Process Customer Personal Data as required by applicable law. Where legally permitted, Provider will notify Customer before undertaking Processing required by law that is outside Customer's instructions.

3.3 Unlawful Instructions. Provider will inform Customer if it reasonably determines that an instruction infringes applicable Data Protection Laws, to the extent required by law. Provider may suspend the affected Processing while the Parties work to resolve the concern.

3.4 Customer Responsibilities. Customer is responsible for the legality, accuracy, and appropriateness of Customer Personal Data submitted to the Services and for ensuring that such Processing is permitted under the Agreement. Protected health information, payment-card data, or other specially regulated data requiring additional contractual safeguards may be Processed only as authorized under MSA Section 3.3 and any applicable additional agreement.

4. Confidentiality and Security

4.1 Confidentiality. Provider will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate contractual or statutory confidentiality obligations and access such information only as reasonably necessary for their authorized responsibilities.

4.2 Security Measures. Provider will maintain appropriate technical and organizational safeguards designed to protect Customer Personal Data in accordance with the DeepFabric Security Measures incorporated under Section 6.1 of the MSA. The Security Measures establish the contractual security

baseline and may be updated as permitted by the MSA, provided that such updates do not materially diminish the overall level of protection.

4.3 Security Responsibilities. Provider is responsible for safeguards within its possession or control. Customer remains responsible for security relating to Customer-controlled systems, credentials, user permissions, configurations, integrations, and other Customer-controlled environments, as provided in the Agreement.

5. Data Use and AI Processing

5.1 Authorized AI Processing. Provider may Process Customer Personal Data through AI models and associated technical systems as reasonably necessary to perform Customer-authorized workflows, including document extraction, retrieval, indexing, embeddings, contextualization, inference, classification, summarization, and generation of AI Outputs.

5.2 Model Training. Provider will not use Customer Personal Data to train or fine-tune models, or permit third-party AI model providers to use such data to train or improve publicly available general-purpose models, unless expressly authorized by Customer through a mechanism permitted under MSA Section 5.3 and applicable Data Protection Laws. MSA Section 5.3 governs the distinction between ordinary AI Processing and model training.

5.3 Other Uses. Provider will not sell Customer Personal Data, disclose it to other customers, or use it for unrelated advertising or other purposes inconsistent with the Agreement or applicable Data Protection Laws.

Provider's rights relating to Usage Data and Aggregated Statistics remain governed by the MSA. Such information remains subject to this DPA to the extent it constitutes Personal Data under applicable law. Information that is properly anonymized and no longer constitutes Personal Data falls outside this DPA.

6. Subprocessors

6.1 Authorization. Customer grants Provider general authorization to engage Subprocessors as reasonably necessary to provide the Services. Provider will maintain a list of authorized Subprocessors that Process Customer Personal Data, available to Customer upon request or through Provider's access-controlled trust portal.

6.2 Subprocessor Obligations. Provider will use commercially reasonable measures in selecting and overseeing Subprocessors. Subprocessors that Process Customer Personal Data will be bound by written data-protection obligations appropriate to their processing activities and providing the protections required under applicable Data Protection Laws. Provider remains responsible for the performance of Subprocessor obligations to the extent required by applicable law and the Agreement.

6.3 Subprocessor Changes. Where required by applicable Data Protection Laws or international-transfer terms, Provider will give Customer reasonable advance notice of intended additions or replacements of Subprocessors that Process Customer Personal Data, ordinarily at least thirty (30) days before the change takes effect. Notices may be provided electronically through Provider's designated customer communication channels, including an access-controlled portal accompanied by an electronic change notification.

Changes to vendors that do not Process Customer Personal Data are excluded. Urgent changes necessary for security, continuity, or legal compliance may be implemented on shorter notice to the extent permitted by law, with notice as soon as practicable.

6.4 Objections. Where required by applicable Data Protection Laws, Customer may object to a proposed Subprocessor within ten (10) business days after notice, based on reasonable, documented data-protection concerns. The Parties will work in good faith toward a commercially reasonable resolution. If an objection cannot be resolved, Provider may offer an alternative arrangement or discontinue the affected Processing or Services, subject to the Agreement and applicable law. This Section does not independently create a refund right or additional termination remedy except as required by law.

6.5 Customer-Selected Services. Third-party services selected or controlled directly by Customer are governed by the applicable responsibilities in the MSA and are not automatically Provider Subprocessors merely because they integrate with the Services.

7. Personal Data Breaches

7.1 Notification. Provider will notify Customer without undue delay and, in any event, within seventy-two (72) hours after becoming aware of a Personal Data Breach involving Customer Personal Data Processed on Customer's behalf, unless prohibited by law. Provider will not delay the initial notification solely because an investigation is incomplete.

7.2 Investigation and Cooperation. Provider will take commercially reasonable measures to investigate, contain, mitigate, and remediate a Personal Data Breach to the extent within its reasonable control. Taking into account the nature of the incident and the information reasonably available, Provider will provide information reasonably necessary to support Customer's compliance with applicable Data Protection Laws. Information may be provided in stages as it becomes available.

7.3 External Notifications. Customer is responsible for determining and making notifications to affected individuals and regulatory authorities, except where applicable law imposes a direct obligation on Provider. Provider will provide reasonable assistance consistent with this DPA.

7.4 No Admission. Notification of a Personal Data Breach does not constitute an admission of fault or liability.

8. Individual Rights and Regulatory Assistance

8.1 Data Subject Requests. Taking into account the nature of the Processing and information available to Provider, Provider will provide reasonable assistance to Customer in responding to requests from individuals exercising rights under applicable Data Protection Laws, including access, correction, deletion, and portability.

8.2 Direct Requests. If Provider receives a request directly from an individual concerning Customer Personal Data, Provider will, where legally permitted, direct the individual to Customer or notify Customer and will not independently respond except as required by law or instructed by Customer.

8.3 Compliance Assistance. Provider will provide reasonable information and assistance concerning data protection assessments, regulatory inquiries, consultations with supervisory authorities, and other compliance obligations applicable to Customer's use of the Services, taking into account the nature of the Processing and information reasonably available to Provider.

For assistance requiring substantial additional work beyond the ordinary operation of the Services, Provider may charge commercially reasonable fees, subject to advance notice and Customer approval, to the extent permitted by applicable law.

8.4 Legally Compelled Disclosure. Provider will notify Customer of legally binding demands for Customer Personal Data where legally permitted and will disclose only the information required by law. Provider will reasonably cooperate with Customer in seeking confidential or protective treatment where appropriate.

9. Return and Deletion

9.1 Customer Instructions. Upon expiration or termination of the applicable Services, Provider will, at Customer's election, return or delete Customer Personal Data, subject to applicable legal requirements and permitted retention exceptions. Customer may use available standard export functionality before access expires. Additional export assistance may be provided as reasonably agreed by the Parties.

9.2 Deletion Process. Following a valid deletion request or expiration of the applicable Services, Provider will delete or de-identify Customer Personal Data from active systems within thirty (30) days, or such longer period as reasonably necessary due to technical limitations or agreed by the Parties, subject to applicable Data Protection Laws.

Customer Personal Data retained in backups or archives will remain protected under the Agreement, will not be used for ordinary operational purposes, and will be deleted through Provider's documented retention and backup processes unless continued retention is required by law.

9.3 Retained Information. Provider may retain Customer Personal Data only to the extent permitted by MSA Section 5.4, this DPA, and applicable law. Retained identifiable Customer Personal Data remains subject to applicable confidentiality and security obligations.

9.4 Confirmation. Upon reasonable written request, Provider will confirm completion of applicable deletion procedures, subject to lawful retention exceptions.

10. Compliance Reviews

10.1 Compliance Information. Upon reasonable request, Provider will make available information reasonably necessary to demonstrate compliance with this DPA, including applicable security documentation, available independent assessment reports, certifications, and written responses, subject to appropriate confidentiality and security restrictions.

10.2 Review and Verification. Customer will ordinarily rely on the information provided under Section 10.1 to assess compliance. Where such information is insufficient or additional review is required by applicable Data Protection Laws, Provider will reasonably cooperate with a proportionate review of its Processing of Customer Personal Data, including audits and inspections where legally required.

10.3 Review Conditions. Reviews will be limited to matters relevant to this DPA and ordinarily conducted no more than once in any twelve (12) month period, with reasonable advance written notice, during regular business hours, and without unreasonable disruption. Additional reviews may occur where required by law or a competent regulator, or where reasonably necessary following a material Personal Data Breach or credible evidence of material noncompliance.

Reviews are subject to appropriate confidentiality, security, and operational restrictions. Customer bears its own review costs unless otherwise required by law or agreed in writing.

10.4 Technical Testing. Review rights do not independently authorize penetration testing, vulnerability scanning, automated system testing, or access to Provider source code, other customers' information, or sensitive security configurations without Provider's prior written approval, except to the extent such access is required by applicable law.

11. International Data Transfers

11.1 Transfers. Provider may Process Customer Personal Data in locations permitted under the Agreement and Security Measures, subject to applicable Data Protection Laws. Where Processing constitutes a Restricted Transfer, the Parties will rely on an appropriate lawful transfer mechanism.
11.2 European Transfers. Where required, the Parties will apply the relevant modules of the European Commission's Standard Contractual Clauses adopted under Decision (EU) 2021/914, together with the applicable completed annexes and supplementary measures described in Schedule C.
11.3 UK and Swiss Transfers. Where applicable, Restricted Transfers from the United Kingdom or Switzerland will be governed by the relevant approved transfer instruments and jurisdiction-specific modifications identified in Schedule C.
11.4 Mandatory Transfer Terms. Mandatory provisions of an applicable international-transfer instrument control over conflicting provisions of this DPA and the MSA to the extent required by law.

12. General Terms

12.1 Relationship to the MSA. Except as expressly provided in this DPA for its specified data-protection subject matter, the MSA remains in full force and effect. This DPA does not independently expand the purchased Services, establish additional service levels, or create obligations concerning data or activities outside its scope.
12.2 Liability. The liability limitations, exclusions, and caps in MSA Section 11 apply to claims arising under this DPA, except to the extent liability cannot lawfully be limited or a mandatory international-transfer instrument expressly requires otherwise. **This DPA does not create a separate or additional contractual liability cap.**
12.3 Changes in Law. If changes in Data Protection Laws require modifications to this DPA, the Parties will cooperate in good faith to implement legally necessary amendments.
12.4 Versioning. The version of this DPA incorporated into an accepted MSA governs the relevant Services and renewals unless the Parties agree otherwise. Publication of an updated DPA does not, by itself, modify an existing agreement.

SCHEDULE A — DETAILS OF PROCESSING

A.1 Parties and Roles

Customer acts as Controller or instructing Processor, as applicable. Provider acts as Processor or Subprocessor.

A.2 Subject Matter

Provision, configuration, support, security, and operation of the DeepFabric SaaS platform and the AI agents and workflows purchased under the applicable Order Form.

A.3 Duration

The applicable authorized implementation period and Subscription Term, together with any permitted post-termination Processing or retention under the Agreement and this DPA.

A.4 Nature of Processing

Receipt, collection, extraction, storage, organization, retrieval, indexing, transformation, analysis, inference, summarization, classification, generation, transmission, access, support, backup, and deletion, as applicable to the Services.

A.5 Purposes and Business Activities

Processing is limited to the business purposes established by the applicable Order Form, which may include:

- Processing supplier invoices, purchase orders, contracts, receipts, and procurement documents.
- Processing freight, shipment, carrier, logistics, inventory, claims, and operational records.
- Reconciling transactions, applying Customer-defined rules, identifying exceptions, and preparing outputs for review.
- Generating reports, recommendations, and other AI Outputs for authorized workflows.
- Providing integrations, user administration, support, troubleshooting, security monitoring, and related service operations.

Only activities covered by the applicable Order Form are authorized for a particular Customer.

A.6 Categories of Data Subjects

As applicable to the subscribed workflows:

- Customer employees, contractors, and Authorized Users.
- Suppliers, vendors, carriers, logistics providers, and their personnel.
- Business customers and business contacts.
- Other individuals whose information is included in Customer-authorized operational records.

A.7 Categories of Personal Data

As applicable to Customer's submitted records and purchased workflows:

- Names, business email addresses, telephone numbers, and job titles.
- User identifiers, account identifiers, and role or access information.
- Business addresses, shipment or delivery information, and operational references.
- Information in purchase orders, invoices, contracts, freight documents, claims, correspondence, and other authorized records.
- Related service logs and AI Outputs to the extent they constitute Personal Data.

A.8 Sensitive or Specially Regulated Data

Customer is not authorized to submit protected health information, payment-card data, or other specially regulated data requiring additional contractual safeguards unless expressly approved under MSA Section 3.3 and any necessary additional agreement.

A.9 Processing Locations

Provider's applicable production hosting and authorized access locations are governed by the Security Measures and applicable Subprocessor arrangements.

A.10 Frequency

Continuous, periodic, or Customer-initiated Processing, depending on the subscribed workflows and Customer's use of the Services.

SCHEDULE B — AUTHORIZED SUBPROCESSORS

Provider maintains a current list of Subprocessors authorized to Process Customer Personal Data in connection with the Services.

The list identifies the applicable Subprocessors, their relevant processing functions, and other information required by applicable Data Protection Laws. It is maintained as confidential security and compliance documentation and made available to Customer upon reasonable request or through Provider's access-controlled trust portal, including before covered Processing begins where required by applicable law.

Provider may update the list in the ordinary course of its operations, subject to any notification and objection requirements under Section 6 of this DPA.

Where additional Subprocessor information or specific authorizations are required under applicable international-transfer instruments, such information will be provided in accordance with Schedule C and the relevant legal requirements.

SCHEDULE C — INTERNATIONAL DATA TRANSFERS

This Schedule requires completion by privacy counsel before use in transactions involving Restricted Transfers.

C.1 EU Standard Contractual Clauses

Where applicable, the Parties incorporate the European Commission Standard Contractual Clauses adopted under Decision (EU) 2021/914, using the relevant module:

- Module Two — Controller to Processor.
- Module Three — Processor to Processor.

The Parties will identify the applicable module, data exporter, data importer, supervisory authority, governing law, and competent courts, and complete the required annexes.

C.2 Transfer Details

Required field	Value
Data exporter	[Customer / relevant Controller or Processor]
Data importer	UnPlatforms, Inc. d/b/a DeepFabric
Applicable SCC module	[Module Two / Module Three]
Categories and purposes	Schedule A, supplemented as required
Technical and organizational measures	Incorporated DeepFabric Security Measures, supplemented as required
Onward recipients	Applicable Schedule B Subprocessors
Competent supervisory authority	[To be determined]
SCC governing law and jurisdiction	[To be determined]
Supplementary transfer safeguards	[To be determined]

C.3 United Kingdom

Where required, the Parties will use the applicable UK International Data Transfer Addendum to the EU SCCs or another approved UK transfer mechanism, including the necessary completed mandatory tables and terms.

C.4 Switzerland

Where required, the applicable EU SCCs will be supplemented with the modifications necessary to comply with Swiss data-protection law.

C.5 Mandatory Instruments

This Schedule does not modify the mandatory provisions of any applicable transfer instrument. Required instruments, modules, annexes, and supplementary protections must be completed before they are relied upon for a Restricted Transfer.

SCHEDULE D — U.S. STATE PRIVACY TERMS

D.1 Applicability. This Schedule applies where Provider Processes Customer Personal Data as a service provider, contractor, or equivalent Processor under the CCPA or other applicable U.S. state privacy laws.

D.2 Limited Business Purposes. Customer discloses Personal Data to Provider solely for the specified business purposes described in Schedule A and the applicable Order Form. Provider will retain, use, and disclose such Personal Data only for those purposes or as otherwise permitted by applicable law.

D.3 Restrictions. Provider will not:

1. Sell or share Customer Personal Data as those terms are defined under applicable law.
2. Retain, use, or disclose Customer Personal Data for purposes outside the specified business purposes, except as permitted by law.
3. Use Customer Personal Data outside the direct business relationship between Customer and Provider except as permitted by law.
4. Combine Customer Personal Data with information received from other customers or collected through other relationships except as permitted by applicable law.

D.4 Compliance. Provider will comply with requirements applicable to service providers or contractors under the CCPA and other applicable state privacy laws and will provide the level of privacy protection required by those laws.

D.5 Compliance Review. Customer may take reasonable and appropriate steps to verify that Provider Processes Customer Personal Data in accordance with applicable U.S. state privacy laws. Such verification will ordinarily be conducted through the confidential documentation and review procedures in Section 10, without limiting any oversight rights required by applicable law.

D.6 Notice and Remediation. Provider will notify Customer if it determines it can no longer meet its applicable obligations under this Schedule. The Parties will cooperate to address unauthorized use or disclosure and take reasonable steps to remediate noncompliance, including reasonable and appropriate steps Customer is entitled to take under applicable law.

D.7 Subprocessors. Provider will impose applicable service-provider, contractor, or equivalent restrictions on Subprocessors as required by Data Protection Laws.

D.8 Other State Laws. To the extent other applicable U.S. state privacy laws impose additional mandatory Processor obligations, the Parties will comply with those requirements and implement any necessary supplementary contractual provisions.