DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the agreement, order form, or online terms governing Customer's use of the Services (the "**Agreement**") and is entered into between the [ ] ("**Customer**") and [GMI Cloud US Inc.] ("**GMI**").

GMI and Customer shall be collectively referred to herein as "**Parties**" and individually as a "**Party**". Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

1. DEFINITIONS

"Applicable Data Protection Laws" means all data protection and privacy laws applicable and binding to a Party's Processing of Personal Data under the Agreement, including, as applicable, the EU GDPR, UK GDPR; and the Swiss FADP.

"Account and Usage Data" means (a) Personal Data relating to Customer's representatives, administrators, and billing and support contacts, and (b) technical, telemetry, usage, billing, fraud-prevention, and security data generated through use of the Services to administer accounts, provide billing and support, secure and improve the Services, prevent fraud and abuse, and comply with law, in accordance with GMI's privacy notice, excluding the substantive content of prompts and outputs.

"Covered Data" means Personal Data contained in Customer Content that GMI Processes on Customer's behalf to provide the Services. Covered Data excludes Account and Usage Data.

"Customer Content" means, if not defined in the Agreement, data provided to GMI by Customer through the Services, and data that Customer generated from such data through its use of the Services.

"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 regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

"SCCs" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission on June 4, 2021, as may be amended, updated or replaced from time to time.

"Security Incident" means a confirmed breach of security resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Covered Data, excluding unsuccessful attempts that do not compromise Covered Data, and excluding any breach caused by Customer or by hardware or infrastructure that is managed, hosted or operated outside of GMI's control.

"Swiss FADP" means, as applicable, the Federal Act on Data Protection of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 14 June 1993) or the revised Federal Act on Data Protection of 25 September 2020 (Switzerland) (with the Ordinance to the Federal Act on Data Protection of 31 August 2022).

"Sub-processor" means any Processor engaged by GMI to assist in Processing Covered Data on GMI's behalf in providing Services, including any third-party model provider whose AI model or inference service is made available through the Services and that may receive Customer Content to provide the selected functionality ("**Third-Party Model Provider**").

"UK Addendum" means the UK International Data Transfer Addendum issued by the UK Information Commissioner, as may be amended or replaced from time to time.

"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.

"**U.S. Privacy Laws**" means the subset of Available Data Protection Laws applicable to residents of the United States, including without limitation the California Consumer Privacy Act of 2018, as amended, by the California Privacy Rights Act of 2020, together with all implementing regulations ("**CCPA**").

"Zero Data Retention" or **"ZDR"** means the optional configuration described in Section 5.2.

The terms **"Personal Data," "Process", "Processing," "Controller," "Processor,"** and **"Data Subject"** have the meanings given under Applicable Data Protection Laws, or, if not defined there, under the EU GDPR. The terms "data subject", "controller" and "processor" include "consumer", "business", and "service provider", respectively, as required by Applicable Data Protection Law.

2. APPLICABILITY

2.1 This DPA applies only to the extent that GMI Processes Covered Data on behalf of Customer in the course of providing Services, where such Processing is subject to Applicable Data Protection Laws. GMI will not use Covered Data for its own purposes except to provide the Services and as otherwise expressly permitted under this DPA.

2.2 The subject matter and details of the Processing of Customer Personal Data are described in Schedule 1.

3. SCOPE AND ROLES

3.1 **Roles.** The Parties agree that, where Applicable Data Protection Laws define the relationship between Parties as one between a Controller and a Processor, Customer is the Controller of Covered Data and GMI is a Processor of Covered Data. GMI is an independent Controller only for Account and Usage Data. When Customer selects a MaaS model route served by a Third-Party Model Provider, such provider act as a Sub-processor unless the Sub-processor register expressly identifies such provider as an independent Controller. GMI makes no representation regarding Third Party Model Provider's retention, location, or data-use practices; Customer is responsible for selecting routes appropriate to its requirements.

3.2 **Customer Instructions.** GMI will process Covered Data only in accordance with Customer's documented instructions, to the extent lawful, though this DPA, the Agreement and any instructions provided by Customer through its use and configuration of the Services, unless applicable law requires otherwise ("**Instructions**"). GMI will only Process Covered Data for the

purposes of delivering the Services to Customer pursuant to the Agreement and this DPA. Customer's instructions provided to GMI with respect to the Processing of Personal Data must at all times comply with Applicable Data Protection Laws. Customer is solely responsible for the accuracy, quality and legality of Personal Data and for the means by which it acquired such Personal Data, including, without limitation, receiving all necessary consents of each Data Subject providing all required notices.

3.3 **Notice to Customers.** GMI will promptly inform Customer if GMI reasonably believes that an Instruction violates Applicable Data Protection Laws, and may suspend the affected Processing until the issue is resolved. GMI will, to the extent legally permitted, inform Customer if GMI receives a legally binding request for disclosure of Covered Data by a law enforcement authority. If applicable law requires GMI to process Covered Data other than on Customers' instructions, GMI will inform Customers unless legally prohibited from doing so.

3.4 **Customer Obligations.** Where Customer acts on behalf of another Controller, Customer may act either as a "controller" or "processor", with respect to Processed Covered Data. Customer warrants on an ongoing basis that the relevant third-party controller has authorized: (a) the Instructions; (b) Customer's engagement of GMI as a processor; and (c) GMI's engagement of Sub-processors. Customer will, comply with all applicable laws, including, Applicable Data Protection Laws. Nothing in this DPA or the Agreement will be construed to state or imply that GMI has a direct relationship with the individual customers or users of Customer or its affiliates or that GMI is acting as a Controller under Applicable Data Protection Laws.

4. CUSTOMER OBLIGATIONS

4.1 **Notices and authorizations.** Customer represents, warrants and covenants that it has and shall maintain throughout the Term all necessary rights, consents and authorizations, to the extent required under Applicable Data Protection Laws to provide the Covered Data to GMI and to authorize GMI to Process Covered Data in connection with the Agreement, including this DPA. Customer will reasonably cooperate with GMI to assist GMI in performing any of its obligations under Applicable Data Protection Laws.

4.2 **Sensitive Personal Data.** Unless expressly permitted in the Agreement, Customer will not submit Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences, including but not limited to (a) protected health information subject to HIPAA absent a Business Associate Agreement; (b) payment card numbers or authentication data; (c) government-issued identification numbers.

4.3 **Configurations.** Customer acknowledges that it is responsible for securely configuring its account, credentials, endpoints, model routes, retention settings, optional features, and other design decisions for the Services as well as for the security of its own applications. Customer

will implement such configurations and design decisions, including retention periods, deletion setting, in a manner that complies with Applicable Data Protection Laws.

5. DATA RETENTION AND OPTIONAL ZERO DATA RETENTION

5.1 **Standard Retention.** ZDR is only available upon Customer's written request through its GMI account representative and will not apply until GMI confirms its application to Customer's Services in writing. Unless ZDR has been confirmed in writing, Covered Data may be retained as reasonably necessary to provide the Services and features, address security and support needs, and satisfy legal obligations. Retention may vary by endpoint type, model route, feature, and configuration.

5.2 **Deletion on Termination.** Following termination or expiration of the Agreement, all Processed Covered Data will be deleted pursuant to GMI's retention and deletion policies. If Customer requests return of Covered Data within thirty (30) days upon the end of the term, GMI will return Covered Data within a reasonable period, subject to any legal retention obligation and any technically necessary backup retention. GMI reserves the right to retain relevant data and information when required by applicable law; when under court order, subpoena, or other legal order; or when preserving evidence following or in anticipation of a civil or criminal lawsuit. Covered Data in backups will be isolated from ordinary access and deleted in the normal backup life cycle unless earlier deletion is legally required or technically infeasible. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will use relevant functionality to rectify or delete that data if required by Applicable Data Protection Laws.

6. CONFIDENTIALITY AND SECURITY

6.1 **Confidentiality.** GMI shall ensure that any person authorized by GMI to Process Covered Data is bound by appropriate confidentiality obligations or subject to appropriate statutory obligation of confidentiality.

6.2 **Security Measures**. GMI will implement and maintain appropriate technical and organizational measures to protect Covered Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or authorized access to Covered Data, as described in Schedule 2. GMI may update the measures from time to time, provided that such updates do not result in a material reduction in the overall level of security. Security is a shared responsibility: Customer is responsible for account access, API key security, permissions, and endpoint and network configuration.

7. SECURITY INCIDENTS

7.1 **Incident Notification.** GMI will notify Customer after becoming aware of a Security Incident, and in any event, will use commercially reasonable efforts to notify Customer within forty-eight (48) hours and, to enable Customer to meet any seventy two (72) hour regulator-notification obligation under the EU GDPR or UK GDPR. Notices may be provided in phases and will describe, to the extent known, the nature of the incident, affected data and Data Subjects,

likely consequences, remediation measures, and a contact point for further information. If it is not possible to provide all such information at the same time, the initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2 **No Acknowledgement of Fault.** GMI's notification of or response to a Security Incident will not be construed as an acknowledgement by GMI of any fault or liability with respect to the Security Incident. GMI will take reasonable steps to contain, investigate, and remediate the Security Incident and will reasonably assist Customer with its notification obligations. However, GMI is not obligated to assess Covered Data to identify information subject to any specific legal requirements.

8. DATA SUBJECT REQUESTS AND ASSISTANCE

8.1 **Requests**. During the term, if GMI receives a request from a Data Subject that relates to Covered Data and identifies Customer, GMI will advise the Data Subject to submit their request to Customer. GMI will notify Customer, unless legally prohibited, and will not respond to that Data Subject's request without Customer's prior authorization, unless legally compelled to do so. Customer is responsible for responding to any such request. GMI will, at the cost of the Customer, provide reasonable cooperation to assist Customer in responding to Data Subject requests and fulfilling its obligations under Applicable Data Protection Laws relating to the Processing of Covered Data.

8.2 **Assistance.** To the extent required under Applicable Data Protection Laws, GMI will, at Customer's expense, provide reasonably requested information regarding GMI's Processing of Covered Data to enable Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. AUDITS

9.1 **Audits**. Upon Customer's reasonable written request, GMI will make available to Customer with its privacy and security policies and other reasonably necessary information to demonstrate GMI's compliance with this DPA, no more than once per year. If that information is insufficient, GMI may allow third party audits or inspections by Customer, at Customer's expense, provided that they are (i) minimally disruptive to GMI's business; (ii) reasonably necessary to confirm that GMI is processing Covered Data in a manner consistent with this DPA. and (iii) conducted no more than once in any 12-month period (except after a Security Incident or where required by a regulator). Any such requests should be made in writing at least thirty (30) days in advance, and Parties must have entered into a confidentiality agreement, and such request must not be made by a competitor of GMI. Audits must be limited in scope, confidential, non-disruptive, and not extend to unrelated systems or other Customers' data. Nothing in this Section limits rights under the SCCs where they apply.

10. INTERNATIONAL DATA TRANSFERS

10.1 **International Data Transfer**. Parties acknowledge that no transfer mechanism is required for the Processing of Covered Data in, or transfers of Covered Data to, an Adequate Country. If Covered Data is transferred to a country that is not an Adequate Country and EU GDPR applies to the transfer, the parties will ensure that the transfer is made using an Alternative Transfer Solution or, if no Alternative Transfer Solution applies, the SCCs. When Customer acts as a Controller, the Controller-to-Processor Modules under the SCCs will apply. When Customer is acting as a Processor, the Processor-to-Processor Modules under the SCCs will apply. If Customer acts as a Processor, Customer will promptly forward to the relevant third-party controller any notice received from GMI relating to the SCCs. Nothing in this DPA is intended to modify or contradict the SCCs, and the SCCs will prevail in the event of any conflict

"Adequate Country" means, as applicable, (a) for data processed subject to the EU GDPR, the European Economic Area or a country or territory recognized as ensuring adequate protection under the EU GDPR; (b) for data processed subject to the UK GDPR, the United Kingdom or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data Protection Act 2018; and (c) for data processed subject to the Swiss FADP, Switzerland or a country or territory recognized as ensuring adequate protection under the Swiss FADP.

"Alternative Transfer Solution" means a transfer mechanism, other than the SCCs, that permits the lawful transfer of personal data to a third country under EU GDPR.

11. U.S. PRIVACY PROVISIONS

11.1 **Prohibitions.** Where Covered Data is subject to the CCPA or other U.S. Privacy Laws, GMI acts as a "service provider" or "contractor" and will comply with the applicable restrictions. The terms "business", "business purpose", "consumer", "personal information", "processing", "sale", "sell", "service provider", and "share" have the meanings given in the CCPA. GMI will not, unless otherwise permitted by law:

(i) sell or share Covered Data;
(ii) retain, use, or disclose or otherwise process Covered Data for purposes other than providing the Services specified in the Agreement;
(iii) combine Covered Data with Personal Data from other sources except as directed by Customer or permitted by law;
(iv) provide Customer with monetary or other valuable consideration in exchange for Covered Data from Customer;
(v) [use Customer Content to train or improve AI models, except to the extent expressly enabled or instructed by Customer].

11.2 **Compliance**. To the extent that Customer permits or instructs GMI to Process Covered Data subject to U.S. Privacy Laws in a de-identified form as part of the Services, GMI shall:

(i) adopt reasonable measures to prevent such de-identified data from being used to infer information about, or otherwise being linked to, a particular natural person or household;

(ii) maintain and use such de-identified data in that form and not attempt to re-identify the information, except as may be permitted by U.S. Privacy Laws; and

(iii) before sharing de-identified data with any other party, including Sub-processors, contractually obligate any such recipients to comply with the requirements of the above.

11.3 **Applicability.** This DPA is intended to satisfy the processor-contract requirements of applicable state laws, including those of California, Colorado, Connecticut, Utah, Virginia, Texas, Oregon, and Montana. Customer will not take any action that would (a) render the provision of Covered Data to GMI a "sale" under U.S. Privacy Laws or a "share" under the CCPA; or (b) render GMI not a "service provider" under the CCPA or "processor" under U.S. Privacy Laws.

11.4 **Customer Notice.** GMI will notify Customer without undue delay if GMI determines that it can no longer meet its obligations under the CCPA. If Customer reasonably believes that GMI's Processing of Covered Data is not consistent with the requirements of the CCPA and notifies GMI accordingly, Parties will work together in good faith to remedy the issue, or, if after doing so, Customer reasonably determines that the issue cannot be remedied, GMI will stop Processing the affected Covered Data upon written instruction from Customer.

12. TERM, LIABILITY, AND GENERAL

12.1 This DPA applies only to GMI's Processing of Covered Data. If there is a conflict between (a) the Applicable Data Protection Laws and the remainder of this DPA, the Applicable Data Protection Laws shall prevail; and (b) this DPA and the remainder of the Agreement, this DPA will prevail.

12.2 This DPA will remain in effect for as long as GMI Processes Covered Data under the Agreement. This DPA will automatically expire when, GMI deletes all Covered Data as described in this DPA. Provisions that by their nature survive, including confidentiality, security, deletion, transfers, liability, will remain in effect until the applicable obligations have been satisfied.

12.3 The limitations of liability in the Agreement apply to this DPA as permitted by law, except for liability to Data Subjects under the third-party beneficiary provisions of the SCCs. Each Party is responsible for regulatory fines imposed on it for its own violations.

12.4 Without prejudice to the SCCs and UK Addendum, this DPA is governed by the law and forum of the Agreement, or, if unspecified, the laws of the State of New York and the courts of New York. GMI may update this DPA as reasonably necessary to comply with Applicable Data Protection Laws. If any provision is unenforceable, the remainder remains in effect. Notices will

be given in accordance with the Agreement; Security Incident notices will be sent to Customer's designated security or privacy contact.

SIGNATURES

The Parties may execute this DPA in counterparts and by electronic signature.

GMI CLOUD US INC.	CUSTOMER
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

SCHEDULE 1 — DETAILS OF PROCESSING (ANNEX I TO THE SCCs)

Element	Description
Data exporter	Customer, as identified in the Agreement (Controller, or Processor on behalf of another Controller).
Data importer	GMI Cloud US Inc. (Processor).
Subject matter	GMI's provision of Services in accordance with the Agreement.
Duration	The term of the Agreement, plus the period from the end of the term until the return or deletion of all Covered Data by GMI in accordance with this DPA.
Nature and purposes	GMI will Process Covered Data for the purpose of providing Services to Customer in accordance with this DPA.
Categories of Data Subjects	Data Subjects may include Customer's employees, customers, suppliers and end users.
Categories of Personal Data	Customer may submit Personal Data to the Services, the categories of which will depend on Customer's use of the Services as determined and controlled by Customer.
Sensitive data (if applicable)	No sensitive data is intended to be transferred unless Customer includes it in the Services.
Frequency	Continuous, depending on Customer's use of the Services.

SCHEDULE 2 — TECHNICAL AND ORGANIZATIONAL MEASURES (ANNEX II TO THE SCCs)

Control Area	Baseline Measures
Governance	Documented security policies, assigned responsibilities, risk assessments, and personnel security awareness.
Access control	Role-based access on least-privilege principles, unique accounts, multi-factor authentication for privileged access, and periodic access reviews.
Encryption	Industry-standard encryption of Covered Data in transit (TLS) and at rest for persistent production data stores.
Network and infrastructure	Segmentation or equivalent logical controls, firewalls, secrets management, secure configuration, and monitoring of production systems.
Development and vulnerability management	Code review, controlled deployment, vulnerability scanning, patch management, and penetration testing or independent assessment as appropriate.
Logging and monitoring	Security and operational logging to detect and investigate suspicious activity, subject to minimization and retention controls.
Incident response	Documented procedures to identify, contain, investigate, remediate, and communicate Security Incidents, with post-incident review.
Availability and recovery	Backup, redundancy, and business-continuity measures appropriate to the Services and service tier.
Vendors and physical security	Risk-based Sub-processor review with contractual flow-down; physical access controls and reliance on audited controls of cloud and colocation providers.
Data life cycle and testing	Retention, deletion, and disposal controls consistent with the relevant provisions under the DPA; periodic testing of control effectiveness.