HOSTED AI INC.

DATA PROCESSING AGREEMENT

Between hosted·ai and its Service Provider / Customer under the Master Licence Agreement

Last Updated Date: 29/10/2026

1. Introduction and Incorporation

This Data Processing Agreement ("DPA") is entered into between Hosted AI Inc., a Delaware corporation ("hosted·ai," "we," "us" or "our") and the entity identified as "Customer" in the Master Licence Agreement between hosted·ai and Customer (the "MLA"). This DPA is the "DPA" referenced in, and incorporated by reference into, Section 2 (Structure of the Agreement) and Section 10 (Data Protection) of the MLA General Terms and Conditions, and is available on an ongoing basis at https://hosted.ai/legal/dpa.

This DPA applies whenever hosted·ai Processes Personal Data on behalf of Customer in connection with the Services, including Personal Data relating to Customer's own personnel and, where applicable, Customer's end users of the Services ("End Users"). Where hosted·ai's Software is used to provide a GPU-as-a-Service offering to Customer's End Users, the additional End User-facing disclosures at the hosted·ai End User Data Processing & Sub-Processor Disclosure Addendum (the "End User DPA Addendum") describe the specific, limited data that flows from that Software to hosted·ai; this DPA governs hosted·ai's obligations as a Processor or Sub-processor with respect to any Personal Data within that data flow.

Consistent with Clause 3 of the MLA (Order of Precedence), this DPA prevails over the MLA, its Schedules, and any Order in respect of the Processing of Personal Data. Capitalized terms not defined in this DPA have the meanings given in the MLA.

2. Definitions

"Applicable Data Protection Laws" means all data protection and privacy laws applicable to the Processing of Personal Data under this DPA, including, as applicable, the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the UK GDPR and Data Protection Act 2018 ("UK GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), the Swiss Federal Act on Data Protection ("FADP"), India's Digital Personal Data Protection Act 2023 ("DPDP Act"), and other U.S. state consumer privacy laws.

"Controller" means the entity that determines the purposes and means of the Processing of Personal Data (or, under CCPA/CPRA, a "Business").

"Customer Personal Data" means any Personal Data Processed by hosted·ai on behalf of Customer in connection with the Services, including: (a) account, authentication and usage data of Customer's Authorised Users in their use of the Services, and Personal Data contained in support requests, diagnostic data, and Customer workloads, datasets or storage that hosted·ai hosts or accesses to provide the Services; and (b) to the extent applicable per the End User DPA Addendum, Personal Data relating to Customer's End Users that hosted·ai Processes as a Sub-processor. Customer Personal Data does not include Personal Data that hosted·ai Processes as an independent Controller under Section 3.

"Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

"Personal Data" means any information relating to an identified or identifiable natural person, as defined under Applicable Data Protection Laws.

"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.

"Processing" (and "Process") means any operation performed on Personal Data, whether or not by automated means, as defined under Applicable Data Protection Laws.

"Processor" means the entity that Processes Personal Data on behalf of a Controller (or, under CCPA/CPRA, a "Service Provider" or "Contractor").

"Standard Contractual Clauses" or "SCCs" means the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission (Commission Implementing Decision (EU) 2021/914), and, for transfers subject to UK GDPR, the UK's International Data Transfer Addendum to those clauses (the "UK Addendum").

"Sub-processor" means any third party (including a hosted·ai Affiliate) engaged by hosted·ai to Process Customer Personal Data on hosted·ai's behalf.

3. Roles of the Parties

As between hosted·ai and Customer, Customer is the Controller (or, where Customer itself Processes Personal Data on behalf of its own End Users, the Processor) of Customer Personal Data, and hosted·ai is the Processor (or Sub-processor, as applicable) that Processes Customer Personal Data solely on behalf of, and under the documented instructions of, Customer, as described in this DPA. Where Customer acts as a Processor with respect to its End Users' Personal Data, hosted·ai acts as a Sub-processor, and Customer represents that it is authorized to give hosted·ai instructions with respect to such Personal Data, including entering into this DPA on behalf of any applicable Controller.

For purposes of the CCPA/CPRA, hosted·ai is a Service Provider (or, where applicable, a Contractor) with respect to Customer Personal Data that constitutes personal information under that law, and the terms of Section 10 of this DPA apply.

Notwithstanding the foregoing, hosted·ai acts as an independent Controller, and not under this DPA, when it Processes Personal Data for its own purposes of account administration, billing and invoicing, managing its commercial relationship with Customer, security and fraud prevention, license compliance verification, and compliance with its legal obligations (including sanctions and export controls). Customer authorizes hosted·ai to create anonymized and aggregated data from telemetry, performance, usage and other technical data ("Aggregate Data"), as described in clause 7.4 of the GTCs and section 4 of Schedule 2 (Software Terms) of the MLA. Data that no longer identifies Customer or any individual, and cannot reasonably be re-identified, is not Customer Personal Data, and hosted·ai shall not attempt to re-identify it. Creating and using such data is a permitted business purpose for the purposes of Section 10.

4. Scope and Details of Processing

The subject matter, duration, nature and purpose of Processing, and the categories of Data Subjects and Personal Data Processed under this DPA are described in Annex 1 (Details of Processing). hosted·ai shall Process Customer Personal Data only for the purposes described in Annex 1 and as necessary to provide the Services under the MLA.

hosted·ai shall not use Customer Personal Data or other Customer Data (other than Aggregate Data that does not identify Customer or any individual) to train, fine-tune, or evaluate any machine learning or artificial intelligence model without Customer's prior written consent.

5. Processing on Customer's Instructions

hosted·ai shall Process Customer Personal Data only on the documented instructions of Customer, which shall consist of the MLA, the applicable Order, this DPA (including Customer's instruction to transfer Customer Personal Data internationally in accordance with Section 13), and any additional written instructions given by Customer and agreed by hosted·ai, unless Processing is required by law applicable to hosted·ai, in which case hosted·ai shall inform Customer of that legal requirement before Processing, unless the law prohibits such notice on important grounds of public interest. hosted·ai shall promptly notify Customer if, in hosted·ai's opinion, an instruction infringes Applicable Data Protection Laws.

6. Confidentiality of Personnel

hosted·ai shall ensure that any person it authorizes to Process Customer Personal Data (including its employees, agents, and contractors) is subject to a binding written obligation of confidentiality, whether by contract or statutory duty, and Processes Customer Personal Data only as necessary to perform that person's role.

7. Security of Processing

hosted·ai shall implement and maintain appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, consistent with Section 12 (Information Security) of the MLA and as further described in Annex 2 (Technical and Organizational Security Measures). hosted·ai may update these measures from time to time provided that such updates do not materially decrease the overall level of protection.

8. Sub-processors

8.1 General Authorization

Customer generally authorizes hosted·ai to engage Sub-processors to Process Customer Personal Data in connection with the Services. hosted·ai's current list of Sub-processors is available at https://hosted.ai/legal/subprocessors and is set out for reference in Annex 3.

8.2 Notice and Objection

hosted·ai shall provide Customer with at least fourteen (14) days' advance notice (by posting an update to the list referenced in Section 8.1 and, where Customer has provided a designated notice contact, by email) before engaging a new Sub-processor. Customer may object to a new Sub-processor within fourteen (14) days of such notice in accordance with this Section 8.2.

Where a new Sub-processor must be engaged urgently to protect the security, integrity or continuity of the Services (including the replacement of a Sub-processor that has failed, become unavailable or been

compromised), hosted·ai may engage that Sub-processor without prior notice, provided that hosted·ai notifies Customer as soon as reasonably practicable and in any event within five (5) Business Days of the engagement. In that case, Customer's right to object under this Section 8.2 applies from the date of that notice.

Customer may object to a new Sub-processor only where Customer reasonably demonstrates that: (a) the Sub-processor is unable to Process Customer Personal Data in accordance with obligations materially equivalent to those set out in this DPA; or (b) the Sub-processor's Processing of Customer Personal Data would cause Customer to breach Applicable Data Protection Laws. Any objection must be made in writing, must identify which of these grounds applies, and must include reasonable supporting detail. An objection may only be made in respect of a Sub-processor that will Process Customer's Customer Personal Data in connection with the Services Customer receives.

If Customer validly objects, the parties shall discuss in good faith a commercially reasonable resolution, which may include hosted·ai (at its option) not using the Sub-processor to Process Customer's Customer Personal Data, putting in place additional safeguards, or proposing a reasonable change to the Services. If hosted·ai is unable or unwilling to offer such a resolution within thirty (30) days of Customer's objection, Customer may, as its sole remedy, terminate only the affected Order (or the part of it that depends on the Sub-processor) without penalty by written notice to hosted·ai, notwithstanding Clause 20.5 of the MLA, and hosted·ai shall refund any prepaid Fees for the unused portion of the terminated Services.

8.3 Flow-Down Obligations

hosted·ai shall impose on each Sub-processor, by written contract, data protection obligations materially equivalent to those set out in this DPA, and shall remain liable to Customer for each Sub-processor's performance of those obligations to the same extent hosted·ai would be liable for performing the services itself.

9. Assistance with Data Subject Requests

Taking into account the nature of the Processing, hosted·ai shall provide reasonable assistance to Customer, at Customer's expense for any material additional cost, to enable Customer to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Laws (including access, rectification, erasure, restriction, portability, and objection). If hosted·ai receives a request directly from a Data Subject concerning Customer Personal Data, hosted·ai shall promptly inform Customer and shall not itself respond to the request except as necessary to confirm receipt and redirect the Data Subject to Customer, unless otherwise required by law.

10. CCPA/CPRA Terms

To the extent hosted·ai Processes Customer Personal Data that constitutes "personal information" under the CCPA/CPRA, hosted·ai shall:

- Process such personal information only for the business purposes specified in the MLA and this DPA, and not retain, use, or disclose it for any other purpose, including any commercial purpose other than providing the Services;

- not sell or share such personal information, as those terms are defined under the CCPA/CPRA;
- not combine such personal information with personal information hosted·ai receives from other sources, except as permitted under the CCPA/CPRA for the purpose of detecting security incidents or verifying quality;
- comply with applicable restrictions and requirements of the CCPA/CPRA that apply to a Service Provider or Contractor, and certify that it understands and will comply with the same;
- notify Customer promptly if hosted·ai determines that it can no longer meet its obligations under the CCPA/CPRA; and
- permit Customer, on notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of such personal information, and to help ensure that hosted·ai uses it in a manner consistent with Customer's obligations under the CCPA/CPRA.

11. Data Protection Impact Assessments and Prior Consultation

hosted·ai shall provide reasonable assistance to Customer, at Customer's expense for any material additional cost, with any data protection impact assessment and, where required, prior consultation with a supervisory authority, that Customer reasonably considers necessary in connection with the Processing of Customer Personal Data under the MLA, taking into account the nature of the Processing and information reasonably available to hosted·ai.

12. Personal Data Breach Notification

hosted·ai shall notify Customer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data, and this Section 12 applies to Customer Personal Data in place of the incident notification standard in clause 12 (Information Security) of the MLA. Such notice shall include, to the extent known at the time and as subsequently updated, a description of the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the Personal Data Breach and mitigate its effects. hosted·ai shall reasonably cooperate with Customer's investigation and any notifications Customer is required to make to supervisory authorities or affected Data Subjects.

13. International Data Transfers

hosted·ai may Process Customer Personal Data, and transfer it internationally, in accordance with clause 11 (Data Residency) of the MLA. Where hosted·ai transfers Customer Personal Data originating in the European Economic Area, the United Kingdom, or Switzerland to a country not recognized as providing an adequate level of data protection, the transfer shall be governed by the Standard Contractual Clauses (including the UK Addendum, where applicable), the details of which are set out in Annex 4, which are hereby incorporated into this DPA by reference, with hosted·ai as the data importer. Where hosted·ai maintains a valid self-certification under the EU-U.S. Data Privacy Framework (or successor framework) covering the relevant transfer, that certification may be relied upon as an additional or alternative transfer mechanism. hosted·ai shall not make an onward transfer of Customer Personal Data to a Sub-processor outside the European Economic Area, the

United Kingdom, or Switzerland unless it has put in place the Standard Contractual Clauses (Module Three) or another valid transfer mechanism with that Sub-processor, and has documented a transfer impact assessment where required by Applicable Data Protection Laws.

14. Audit Rights

hosted·ai shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer, in accordance with this Section 14. hosted·ai may satisfy this obligation, in whole or in part, by providing Customer with a current third-party audit report (such as a SOC 2 Type II report), summary of penetration test results, or equivalent certification, where reasonably sufficient to demonstrate compliance and where an on-site audit is not otherwise required by Applicable Data Protection Laws.

Customer, or an independent auditor bound by confidentiality that is not a competitor of hosted·ai, may conduct an on-site audit or inspection only where the information provided under this Section 14 is not reasonably sufficient to demonstrate compliance, following a Personal Data Breach affecting Customer, or where required by a supervisory authority. Any such audit shall be on at least thirty (30) days' prior written notice (or shorter where a supervisory authority requires), take place no more than once in any twelve (12) month period except following a Personal Data Breach or at the request of a supervisory authority, follow a scope agreed in advance, take place during normal business hours, and be at Customer's expense. Clause 18 (Audit Rights) of the MLA governs hosted·ai's audit of Customer's license compliance and does not apply to audits under this Section 14.

15. Return or Deletion of Customer Personal Data

On termination or expiration of an Order/MLA, hosted·ai shall make Customer Personal Data available for export and shall thereafter delete it from hosted·ai's production systems, in each case in accordance with Section 20.8 (Effect of Termination) of the MLA, subject to any retention required by legal hold, backup-cycle retention, or Applicable Data Protection Laws. Customer Personal Data held in backups shall be deleted as those backups expire on hosted·ai's normal rotation cycle, which shall not exceed thirty-five (35) days; until then, such backups remain subject to this DPA and are not restored except for disaster recovery. hosted·ai shall certify deletion in writing on Customer's request.

16. Liability

Each party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions set out in Clause 14 (Limitation of Liability) of the MLA, except to the extent Applicable Data Protection Laws prohibit the limitation of liability for the type of claim at issue (for example, statutory liability to a Data Subject or a supervisory authority), in which case such liability is not limited by this DPA or the MLA. Nothing in this DPA relieves either party of any liability it may have directly to a Data Subject or supervisory authority under Applicable Data Protection Laws.

17. Precedence, Term, and General Terms

This DPA takes effect on the Effective Date of the MLA (or, if later, the date Customer's Processing of Personal Data through the Services begins) and remains in effect for as long as hosted·ai Processes Customer Personal Data under the MLA. This DPA is governed by the same governing law and dispute-resolution provisions as the MLA (Clause 23.1), except that, to the extent the Standard Contractual Clauses incorporated under Section 13 apply to a given transfer, those clauses are governed by their own governing law as specified therein. Clause 23 (Miscellaneous) of the MLA applies to this DPA as if set out in full, including with respect to notices, amendment, severability, and waiver.

18. Updates to this DPA

hosted·ai may update this DPA to reflect changes in Applicable Data Protection Laws, regulatory guidance, transfer mechanisms, or its Sub-processors, or to improve the protection it provides, provided that no update materially reduces the protection given to Customer Personal Data unless required by law. hosted·ai shall notify Customer of any material update where reasonably practicable, and in any event shall notify Customer no later than the date the update takes effect. Updates required by law or by a supervisory authority may take effect immediately. If Customer reasonably demonstrates that a material update (a) materially reduces the protection given to Customer Personal Data, or (b) would cause Customer to breach Applicable Data Protection Laws, Customer may object in writing within fourteen (14) days of being notified of the update, identifying which of these grounds applies and including reasonable supporting detail. The parties shall then discuss in good faith a commercially reasonable resolution. If hosted·ai is unable or unwilling to offer such a resolution within thirty (30) days of Customer’s objection, Customer may, as its sole remedy, terminate only the affected Order (or the part of it affected by the update) without penalty by written notice to hosted·ai, notwithstanding Clause 20.5 of the MLA, and hosted·ai shall refund any prepaid Fees for the unused portion of the terminated Services.

19. Government and Third-Party Access Requests

If hosted·ai receives a request from a public authority or other third party to disclose Customer Personal Data, hosted·ai shall, unless prohibited by law: (a) redirect the requester to Customer where reasonably possible; (b) promptly notify Customer; (c) assess the lawfulness of the request and challenge it where there are reasonable grounds to consider it unlawful; and (d) disclose only the minimum Customer Personal Data necessary to comply. hosted·ai has not created back doors or similar programming that could be used to access the Services or Customer Personal Data.
Questions regarding this DPA may be directed to legal@hosted.ai.

Annex 1 — Details of Processing

Subject Matter

hosted·ai's provision of the GPU pool virtualization and orchestration Software and related Services to Customer under the MLA, including support, and the telemetry-related processing described in the End User DPA Addendum.

Duration

For the duration of the MLA and any applicable Order, plus any post-termination retention period described in Section 20.8 of the MLA or Section 15 of this DPA.

Nature and Purpose of Processing

Hosting, storage, transmission, and other processing operations necessary to: provide, operate, secure, and support the Services; and, where applicable, collect and process Platform Telemetry as described in the End User DPA Addendum; and, where hosted·ai operates GPU-as-a-Service infrastructure or hybrid components, or accesses Customer's environment to provide support, hosting and processing of Customer workloads, support requests, and diagnostic data.

Categories of Data Subjects

- Customer's Authorised Users, including administrators and technical and support contacts, in their use of the Services;
- Customer's End Users, only to the extent, if any, that Platform Telemetry or other data becomes reasonably identifiable to an individual End User, as described in Section 3.3 of the End User DPA Addendum.
- Individuals whose Personal Data is contained in support requests, diagnostic data, or Customer workloads that hosted·ai hosts or accesses to provide the Services.

Categories of Personal Data

- Contact information (name, business email address, phone number, job title);
- Account and authentication identifiers (usernames, license key identifiers);
- System and usage logs, only to the extent linked to an identifiable individual as described above.
- Support communications and attachments, diagnostic data, and any Personal Data contained in Customer workloads, datasets, or storage that hosted·ai hosts or accesses to provide the Services.

Special Categories of Personal Data

None Intended. The parties do not anticipate the Processing of special categories of Personal Data (as defined under Applicable Data Protection Laws) under the MLA, but Customer workloads, datasets or storage that hosted·ai hosts or accesses to provide the Services may incidentally contain them. Customer remains responsible for any such data it submits, and the measures in Annex 2 apply to it.

Annex 2 — Technical and Organizational Security Measures

- Access control: role-based access control and multi-factor authentication for systems handling Customer Personal Data;
- Encryption: encryption of Customer Personal Data in transit using TLS 1.2 or higher, and encryption at rest (AES-256 or equivalent) for stored account, billing, and telemetry data;
- Tenant isolation: logical isolation between tenants within the Services, consistent with the architecture described in the Documentation;
- Logging and monitoring: centralized logging and monitoring of access to production systems, with alerting on anomalous access patterns;
- Incident response: a documented security incident response plan, tested periodically, supporting the notification obligations in Section 12;
- Personnel security: background checks where legally permissible, confidentiality obligations and periodic security awareness training for personnel with access to Customer Personal Data;
- Vendor management: security review of Sub-processors prior to engagement and periodically thereafter;
- Vulnerability management: routine vulnerability scanning and patch management for systems supporting the Services;
- Business continuity: backup and disaster recovery procedures designed to restore availability of the Services following a disruptive incident, with documented recovery time and recovery point objectives, tested at least annually.
- Testing and physical security: regular testing and evaluation of the effectiveness of these measures, including periodic penetration testing, and hosting of production systems in data centers with controlled physical access.

These measures are illustrative of the level of security hosted·ai maintains as of the Effective Date and are consistent with Clause 12 (Information Security) of the MLA. hosted·ai may update specific measures over time provided the overall level of protection is not materially reduced.

Annex 3 — Sub-processors

hosted·ai's current list of Sub-processors engaged to Process Customer Personal Data is maintained at https://hosted.ai/legal/subprocessors and updated from time to time in accordance with Section 8 of this DPA. As of the Effective Date, categories of Sub-processors include:

- cloud infrastructure and hosting providers supporting production and customer support systems;
- collaboration, messaging and issue-tracking providers used for customer support and engineering;
- transactional email providers;
- affiliated and contracted support and engineering providers, including Accomply Solutions Inc. (United States) and its affiliate Infravine Technologies Private Limited (India), which provide customer

support, software development and platform operations, including review of logs and diagnostic data, and remote access to Customer environments to provide support;

- individual contractors engaged directly by hosted·ai for research and development, with time-limited access to support data where required to resolve escalated issues;

Annex 4 — International Transfer Mechanism

Where required under Section 13 of this DPA, the parties incorporate the Standard Contractual Clauses as follows:

- Module Two (Controller to Processor) applies where Customer is a Controller of the transferred Personal Data;
- Module Three (Processor to Processor) applies where Customer is a Processor of the transferred Personal Data;
- Customer is the data exporter and hosted·ai is the data importer;
- the optional docking clause (Clause 7) is not used;
- Clause 9(a) option 2 (general written authorization for Sub-processors) applies, with the time period for prior notice of Sub-processor changes as set out in Section 8.2 of this DPA;
- Annex I.C (competent supervisory authority) is determined in accordance with Clause 13(a): (i) where Customer is established in an EU Member State, the supervisory authority responsible for ensuring Customer's compliance with the GDPR as regards the data transfer; (ii) where Customer is not established in an EU Member State but falls within the territorial scope of the GDPR under Article 3(2) and has appointed a representative under Article 27(1), the supervisory authority of the Member State in which its representative is established; and (iii) where Customer is not established in an EU Member State but falls within Article 3(2) without being required to appoint a representative under Article 27(2), the supervisory authority of the Member State in which the Data Subjects whose Personal Data is transferred are located. Customer shall confirm its competent supervisory authority to hosted·ai on request;
- for UK transfers, the UK Addendum is incorporated to apply the Clauses with the modifications required for UK GDPR;
- the optional independent dispute resolution body in Clause 11(a) is not used;
- Clause 17 (governing law): Option 1 applies, and the Clauses are governed by the law of Ireland;
- Clause 18 (choice of forum and jurisdiction): the courts of Ireland;
- for the UK Addendum, Table 1 is completed by reference to Annex 1, Tables 2 and 3 by reference to this Annex 4 and Annexes 1 to 3, and, for Table 4, neither party may end the UK Addendum when the Approved Addendum changes;
- for transfers subject to the FADP, the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority for those transfers, references to a "Member State" include Switzerland so that Swiss Data Subjects may bring claims in their place of habitual residence, and references to the GDPR include the FADP;

- the technical and organizational measures in Annex 2 of this DPA serve as Annex II to the Clauses, and the processing details in Annex 1 of this DPA serve as Annex I to the Clauses.