HOONIFY

Data Protection Agreement

Hoonify AI Inference Platform · hoonify.ai

DRAFT FOR LEGAL REVIEW. This document was prepared as a starting point and is not legal advice. Bracketed items [LIKE THIS] are placeholders to confirm or complete. Have qualified counsel review and finalize before publication or execution.

1. Scope and Roles

1.1 Purpose. This Data Protection Agreement ("DPA") forms part of the Hoonify Terms and Conditions (the "Terms") between Customer and Hoonify Technologies Inc., a corporation with offices at 13170 Central Ave SE, Ste B #435, Albuquerque, NM 87123 ("Hoonify"), for the Hoonify inference platform (the "Service"), and governs Hoonify's processing of Personal Data on Customer's behalf. Where it conflicts with the Terms on data protection matters, this DPA controls.

1.2 Roles. For Personal Data contained in Customer Content, Customer is the Controller (or a Processor acting for its own customer) and Hoonify is the Processor. Where Hoonify routes requests to Operators, those Operators act as Subprocessors of Hoonify, as described in Section 7.

1.3 Definitions. "Personal Data," "Controller," "Processor," "Processing," "Data Subject," "Personal Data Breach," and "Supervisory Authority" have the meanings given in Data Protection Laws. "Data Protection Laws" means all laws applicable to the Processing under the Terms, including the EU GDPR, UK GDPR, and the California Consumer Privacy Act as amended ("CCPA/CPRA"). "Subprocessor" means any third party engaged by Hoonify to Process Personal Data, including Operators. Other capitalized terms have the meaning given in the Terms.

2. Processing Instructions

2.1 Documented Instructions. Hoonify shall Process Personal Data only on Customer's documented instructions, including as set out in this DPA and the Terms and as effected through Customer's configuration and use of the Service, unless required to do otherwise by law (in which case Hoonify will notify Customer where legally permitted).

2.2 Lawfulness. Customer is responsible for the lawfulness of Personal Data it submits and of Hoonify's Processing on its instructions, including providing required notices and obtaining required consents from Data Subjects.

2.3 Unlawful Instruction. Hoonify shall inform Customer if, in its reasonable opinion, an instruction infringes Data Protection Laws.

3. Zero Data Retention

3.1 Commitment. Hoonify operates the Service on a zero-data-retention ("ZDR") basis. Customer Content and Output submitted to the inference Service are Processed in transient, in-memory form solely for the time required to serve the request and are not written by Hoonify to persistent storage after the request completes.

3.2 No Secondary Use. Hoonify does not retain Customer Content or Output for model training, fine-tuning, product improvement, or abuse-monitoring purposes, and does not sell or share them or use them for any purpose beyond serving the immediate request.

3.3 Operational Metadata. Hoonify may retain limited operational and billing metadata that does not include the contents of prompts or Output (for example, timestamps, token or request counts, model identifiers, and status codes) as needed to operate, secure, meter, and bill the Service. The categories of such metadata are described in Annex I.

3.4 Flow-Down. Hoonify shall contractually require each Operator that may receive Customer Content to honor equivalent zero-data-retention and no-training obligations, as described in Section 7. Where an Operator cannot meet ZDR terms, Hoonify shall not route ZDR-designated traffic to that Operator.

Note for review: Because the Service aggregates third-party Operators, the integrity of the ZDR commitment depends on flow-down to every Operator in the routing pool. Confirm that all live Operators are under written ZDR/no-training terms before this DPA represents ZDR without qualification, and consider whether any non-ZDR Operators must be fenced off from ZDR traffic by configuration.

4. Confidentiality and Personnel

4.1 Confidentiality. Hoonify shall treat Personal Data as confidential and ensure that personnel authorized to Process it are bound by appropriate confidentiality obligations.

4.2 Least Privilege. Hoonify shall limit access to Personal Data to personnel who require it to provide the Service, on a least-privilege basis.

5. Security Measures

5.1 TOMs. Hoonify shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, taking into account the state of the art, costs, and the risks of the Processing. A summary of these measures is set out in Annex II.

5.2 Evolving Measures. Hoonify may update its measures provided that the level of protection is not materially decreased during the term.

6. Assistance to Customer

6.1 Data Subject Requests. Taking into account the nature of the Processing and the ZDR design of the Service, Hoonify shall provide reasonable assistance to enable Customer to respond to Data Subject requests to exercise their rights. Because Hoonify does not retain Customer Content, Hoonify's ability to locate or extract specific Personal Data after Processing is inherently limited, and Customer remains primarily responsible for fulfilling such requests from its own systems.

6.2 DPIAs and Consultations. Hoonify shall provide reasonable assistance to Customer with data protection impact assessments and prior consultations with Supervisory Authorities, to the extent relevant to Hoonify's Processing and not otherwise available to Customer.

7. Subprocessors and Operators

7.1 Authorization. Customer provides general authorization for Hoonify to engage Subprocessors, including Operators, to Process Personal Data, subject to this Section. A current list of Subprocessors is maintained at [hoonify.ai/subprocessors] and summarized in Annex III.

7.2 Flow-Down Obligations. Hoonify shall impose on each Subprocessor data protection obligations that are substantially equivalent to those in this DPA, including the ZDR and no-training commitments in Section 3, by written agreement. Hoonify remains responsible to Customer for monitoring the ZDR and no-training performance of each Subprocessor.

7.3 Operator Selection and Routing. Hoonify selects Operators based on, among other factors, their ability to meet Hoonify's security and data protection requirements. Where Customer selects jurisdictional or sovereign routing controls, Hoonify shall route eligible Personal Data only to Operators consistent with those controls, subject to the Documentation.

7.4 Changes and Objection. Hoonify shall give Customer prior notice of the addition or replacement of a Subprocessor (for example, by updating the list and providing a subscription to changes). Customer may object on reasonable data protection grounds within ten (10) business days; the parties shall work in good faith to resolve the objection, and if they cannot, Customer may terminate the affected Service without penalty for the unused, prepaid portion. [Confirm notice period and remedy.]

8. International Transfers

8.1 Transfer Mechanism. Where Processing involves transfers of Personal Data from the EEA, UK, or Switzerland to a country without an adequacy decision, the parties agree that the EU Standard Contractual Clauses ("SCCs") apply and are incorporated by reference, with Module Two (Controller-to-Processor) or Module Three (Processor-to-Processor) applying as appropriate to the relationship, completed as set out in Annex IV. For UK transfers, the UK International Data Transfer Addendum applies; for Switzerland, the SCCs apply with Swiss adaptations.

8.2 Operator Transfers. For onward transfers to Operators outside the relevant jurisdiction, Hoonify shall ensure an appropriate transfer mechanism is in place. The ZDR design and routing controls in Section 7 support Customer's data residency requirements.

8.3 Government Access. Hoonify shall handle government or law-enforcement requests for Personal Data in accordance with the SCCs and applicable law, and shall, where lawfully able, notify Customer and challenge overbroad requests.

9. Personal Data Breach

9.1 Notification. Hoonify shall notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer's Personal Data, and in any event within seventy-two (72) hours, with the information reasonably available to enable Customer to meet its own notification obligations.

9.2 Cooperation. Hoonify shall take reasonable steps to mitigate the breach and cooperate with Customer's investigation. Notification is not an acknowledgment of fault.

10. Audits and Compliance

10.1 Records and Reports. Hoonify shall make available information reasonably necessary to demonstrate compliance with this DPA, including third-party audit reports and certifications where available (for example, SOC 2 Type II, ISO 27001, ISO 42001).

10.2 Audit Rights. Where reports are insufficient to demonstrate compliance, Hoonify shall allow for and contribute to audits, including inspections, conducted by Customer or a mutually agreed independent auditor on reasonable prior notice, no more than once per year absent a breach or regulator requirement, subject to confidentiality and minimizing disruption. [Confirm audit cadence and cost allocation.]

11. Return and Deletion

11.1 On the Service. Given the ZDR design, Customer Content submitted to the inference Service is not retained beyond Processing and therefore requires no separate deletion step at termination.

11.2 Account and Metadata. On termination, Hoonify shall, at Customer's election, delete or return any account-level Personal Data and operational metadata associated with Customer within thirty (30) days, except where retention is required by law. Hoonify shall confirm deletion in writing on request.

12. CCPA / CPRA Terms

12.1 Service Provider. To the extent the CCPA/CPRA applies, Hoonify acts as a "Service Provider" and Processes Personal Information only to perform the Service under the Terms.

12.2 Restrictions. Hoonify shall not sell or share Personal Information, retain, use, or disclose it for any purpose other than performing the Service or as permitted by the CCPA/CPRA, or combine it with information from other sources except as permitted. Hoonify certifies it understands and will comply with these restrictions.

13. Governing Law, Liability, and Term

13.1 Governing Law. Except as otherwise required by Data Protection Laws, this DPA is governed by and construed in accordance with the internal laws of the State of Delaware, excluding its conflict-of-laws rules, and the dispute-resolution and forum provisions of the Terms apply to this DPA. Notwithstanding the foregoing, the Standard Contractual Clauses and any other transfer mechanism incorporated under Section 8 are governed by the law and subject to the forum specified in those clauses, and nothing in this Section overrides any governing law, forum, or supervisory-authority jurisdiction mandated by Data Protection Laws.

13.2 Liability. Each party's liability under this DPA is subject to the limitations and exclusions in the Terms. Nothing limits liability that cannot be limited under Data Protection Laws.

13.3 Term. This DPA takes effect on the effective date of the Terms and continues until Hoonify ceases all Processing of Personal Data for Customer.

Annex I — Details of Processing

Item	Detail
Subject matter	Provision of AI inference and related Service to Customer.
Duration	For the term of the Terms; inference content is Processed only transiently per request (ZDR).
Nature and purpose	Receiving inference requests, executing Models, returning Output, and metering/securing the Service.
Categories of Data Subjects	Determined by Customer; may include Customer's end users, employees, or any individuals referenced in Customer Content. [Confirm.]
Categories of Personal Data	Any Personal Data Customer includes in prompts/inputs; Hoonify does not require or control these categories. [Confirm; note any prohibited categories.]
Special category data	Customer should not submit special-category data unless agreed in writing and lawful. [Confirm position.]

Item	Detail
Operational metadata retained	Timestamps, request/token counts, model identifiers, status codes, account identifiers — excluding prompt and Output contents.
Frequency	Continuous, on Customer's use of the Service.

Annex II — Technical and Organizational Measures

The following summarizes Hoonify's security measures. [Align this list to Hoonify's actual controls and any SOC 2 / ISO scope before finalizing.]

Access control

- Role-based access on a least-privilege basis; centralized identity and SSO for personnel.
- Multi-factor authentication for administrative access; periodic access reviews.

Encryption

- Encryption in transit (TLS) for Service endpoints.
- Encryption at rest for systems holding operational metadata and credentials.

ZDR and data minimization

- Inference content Processed in-memory only; no persistence of prompts/Output after request completion.
- Routing controls to constrain Operator selection by Customer preference and jurisdiction.

Network and platform security

- Network segmentation, firewalling, and monitoring; secrets management for keys and credentials.
- Vulnerability management, patching, and hardened baselines across the fleet.

Operational resilience and governance

- Logging of operational events (excluding inference content), alerting, and incident response procedures.
- Backup and recovery for systems holding account/metadata; periodic testing.
- Security awareness training and confidentiality obligations for personnel; vendor/Operator due diligence.

Annex III — Subprocessors and Operators

Current Subprocessors are maintained at [hoonify.ai/subprocessors]. The table below is illustrative; complete it with the live list, including each entity's legal name, role, processing location, and whether it is under ZDR/no-training terms.

Legal entity	Role / purpose	Location(s)	ZDR terms in place?
[Operator A legal name]	GPU compute / inference Operator	[Country/region]	[Yes / No]
[Operator B legal name]	GPU compute / inference Operator	[Country/region]	[Yes / No]

Legal entity	Role / purpose	Location(s)	ZDR terms in place?
[Cloud / hosting provider]	Platform hosting, metadata	[Country/region]	[Yes / No]
[Identity / auth provider]	Authentication	[Country/region]	[N/A — no inference content]
[Analytics / billing]	Usage metering (no content)	[Country/region]	[N/A — no inference content]

Annex IV — SCC Completion Details

Complete the following for incorporation of the EU SCCs (and UK Addendum where applicable). [Confirm all selections with counsel.]

SCC item	Selection
Modules	Module Two (Controller–Processor) and/or Module Three (Processor–Processor), as applicable.
Clause 7 (docking)	[Applies / Does not apply]
Clause 9 (subprocessors)	Option 2 (general authorization), with 10-business-day notice of changes.
Clause 11 (redress)	[Optional independent dispute resolution — select]
Clause 17 (governing law)	Law of [EU Member State, e.g., Ireland].
Clause 18 (forum)	Courts of [EU Member State].
Annex I.A (parties)	Customer (data exporter); Hoonify Technologies Inc. (data importer).
Annex I.B (description)	As set out in Annex I of this DPA.
Annex I.C (supervisory authority)	[Lead authority per GDPR / Clause 13].
Annex II (TOMs)	As set out in Annex II of this DPA.
UK Addendum	[Applies for UK transfers — complete Tables 1–4].

Signatures

For negotiated DPAs, add signature blocks for Customer and Hoonify. For click-through acceptance, the DPA is accepted with the Terms.

Effective date: Upon account signup and acceptance **Version: [v1.0 Draft]**