DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is entered into as of [Date] by and between:

1. MoonMath.ai Ltd., a company incorporated in Israel with its registered office at Yitzhak Rabin road 1, Petach Tikva, Israel ("Processor" or "MoonMath"); and
2. [Company]., a company incorporated in [Company incorporation country] with its registered office at [Customer registered address] ("Customer").

Processor provides the Zro inference service (the "Service") under the parties' applicable services agreement or online terms (the "Agreement"). This DPA forms part of the Agreement and applies only to the Covered Models identified in Schedule 1, Part B, and the related processing described in Schedule 1, Part A.

1. Scope, roles, and definitions

1.1 Customer is the controller, or a processor acting on behalf of a third-party controller, for Customer Personal Data. Processor acts as processor or subprocessor, as applicable. Where Customer acts as processor, Customer warrants that it is authorized by the relevant controller to engage Processor and give the instructions contemplated by this DPA.

1.2 Processor processes Customer Personal Data only on Customer's documented instructions, unless applicable law requires otherwise. To the extent legally permitted, Processor will inform Customer of that legal requirement before processing. The processing details are set out in Schedule 1.

1.3 Customer is responsible for its instructions, applications and end users. Customer represents and warrants that it has established a lawful basis and provided all notices and obtained all consents, permissions and rights necessary for the processing contemplated by the Agreement and this DPA, and that its instructions comply with Applicable Data Protection Laws.

1.4 “Covered Model” means a model identified by its exact API model identifier in Schedule 1, Part B. This DPA applies only to Customer Personal Data submitted to, or generated by, a Covered Model and related processing described in Schedule 1, Part A. Customer must not submit Customer Personal Data to any other model unless the parties add that model to Schedule 1, Part B in writing. Nothing in this Section limits any right or obligation that cannot be excluded under applicable law.

1.5 The parties may add, remove, or modify a Covered Model only by a written amendment, order form, or other written instrument that expressly references this DPA. Enabling a model in Zro's catalog, dashboard, API, or other product interface does not by itself make that model a Covered Model.

1.6 “Applicable Data Protection Laws” means the data protection and privacy laws applicable to the processing of Customer Personal Data under this DPA, including [Country specific Data Protection Act] to the extent applicable. “Personal Data” and “Data Subject” have the meanings given under those laws; a Data Subject is an identified or identifiable natural person to whom Personal Data relates.

1.7 “Customer Personal Data” means Personal Data processed by Processor on Customer's behalf through a Covered Model or in the related activities described in Schedule 1, Part A. “Personal Data Breach” means a breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorized disclosure of, or access to, Customer Personal Data processed by Processor or its subprocessors, and any other breach of that data within the meaning of Applicable Data Protection Laws. “Subprocessor” means a third party engaged by Processor to process Customer Personal Data on Customer's behalf.

1.8 The Agreement, this DPA, and Customer's use of the Service in accordance with them constitute Customer's complete documented instructions. Additional instructions outside the agreed scope require a separate written agreement and may be subject to additional charges. This does not limit assistance or processing restrictions required by Applicable Data Protection Laws.

1.9 Customer must not submit Personal Data for which the Service is inappropriate under the Agreement, including special categories of personal data, data relating to criminal convictions or offenses, government-issued identifiers, payment card data (other than through Processor's payment provider for billing), or data subject to sector-specific regulation, unless the parties separately agree in writing to that processing and any necessary safeguards.

2. Processor obligations

2.1 Processor shall process Customer Personal Data only as needed to provide, secure, support, and maintain the Service, and on Customer's documented instructions. Processor shall promptly inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws, and may suspend the affected processing while the parties resolve the instruction. Where the law requires immediate notice, Processor shall notify Customer immediately.

2.2 Processor shall ensure that persons authorized to process Customer Personal Data are bound by contractual or statutory confidentiality obligations and receive appropriate instruction or training on their data protection responsibilities. Processor shall implement appropriate technical and organizational measures, taking account of the nature of processing and risks to individuals, as described in Schedule 3.

2.3 Processor shall provide reasonable assistance with data-subject requests, security obligations, impact assessments, and prior regulator consultations to the extent required by Applicable Data Protection Laws, taking account of the nature of processing and information available to Processor. Assistance with impact assessments and prior consultations is at Customer's cost. Processor may charge a reasonable fee for data-subject assistance beyond the Service's standard functionality, to the extent permitted by law; mandatory assistance shall not be withheld pending a fee dispute.

2.4 Processor shall notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data. Where Applicable Data Protection Laws require earlier notice, including when Processor has reason to believe a breach has occurred, that earlier requirement applies. Section 7 describes notification and cooperation requirements.

2.5 On termination or expiration of the Agreement or the affected Service, Processor shall, at Customer's written election, delete or return Customer Personal Data in its possession or control and delete existing copies within a reasonable period not exceeding ninety (90) days, unless applicable law requires retention. If Customer has not made an election within thirty (30) days, Processor may delete the data. Legally retained Customer Personal Data remains protected by this DPA for as long as it is retained. Processor is not required to reconstruct inference content that was not retained under Section 3.1.

3. Service data handling and security

3.1 Zro's current service design disables storage of prompt text, completion text, and request bodies at the gateway. Such content is processed transiently to generate and return a response. Gateway operational logs may record request metadata, including timestamps, request identifiers, model identifiers, token counts, latency and HTTP status codes, but shall not contain prompt text, completion text or request bodies. This gateway commitment does not itself represent that every infrastructure provider maintains no operational logs; any provider retention must be documented in Schedule 2 and comply with this DPA.

3.2 Processor does not use Customer prompts, completions, request bodies, conversation histories, or content-bearing logs for model training, fine-tuning, evaluation datasets, or product analytics unless Customer separately and explicitly agrees in writing. Processor shall not authorize a subprocessor to use that content to train or fine-tune any Processor or third-party model without that separate written agreement.

3.3 This DPA does not create a commitment to any particular certification, service level, or security standard unless the parties expressly agree to it in writing. The specific measures agreed in Schedule 3 remain applicable.

3.4 Processor may route a request for a Covered Model only through the inference provider(s) and processing region(s) listed for that model in Schedule 1, Part B. This restriction applies to routing for high traffic, capacity overflow, failover, disaster recovery, and any other operational reason. Processor shall not route Customer Personal Data for a Covered Model to an unlisted inference provider or location without Customer's prior written authorization and a written update to Schedule 1, Part B.

3.5 Account, authentication, billing, security, support and usage metadata necessary to operate Customer's account may be retained in accordance with the Agreement and Processor's privacy notice, subject to this DPA to the extent that metadata is Customer Personal Data. Those references do not extend the retention permitted by Section 2.5.

3.6 Processor may update the technical and organizational measures in Schedule 3 to reflect technical progress or operational changes, provided that the updates do not materially diminish the overall level of protection of Customer Personal Data. Such updates do not amend the Covered Models or permitted inference routes.

4. Subprocessors

4.1 Subject to Section 3.4, Customer gives Processor general written authorization to engage the subprocessors identified in Schedule 2 and replacements or additions permitted under this Section. Processor remains responsible to Customer for each subprocessor's performance of its applicable data protection obligations to the same extent as if Processor performed the relevant acts or omissions itself, subject to Section 8.2 and Applicable Data Protection Laws.

4.2 Processor will impose written data-protection obligations on subprocessors that are no less protective than the applicable obligations in this DPA, taking account of the nature of the services they provide.

4.3 Except for changes to inference providers or processing locations authorized for a Covered Model, which remain governed by Section 3.4, Processor will give Customer at least thirty (30) days' advance

written notice of an intended addition or replacement of a subprocessor, including by email to Customer's designated administrative contact or written service communication identifying the updated list. Customer may object in writing within that notice period on reasonable, documented data-protection grounds.

4.4 The parties will seek in good faith to resolve a timely objection, considering commercially reasonable alternatives. If unresolved, either party may terminate the affected Service by written notice. Customer will receive a pro-rata refund of unused prepaid fees for the remaining term after termination. Unless required otherwise by applicable law, this is Customer's sole contractual remedy for an unresolved objection to a permitted change; it does not excuse a breach of this DPA. Processor shall not use an objected-to subprocessor for Customer Personal Data before resolution or termination of the affected Service. Silence under this procedure does not authorize an inference route requiring prior written authorization under Section 3.4.

5. International transfers and regions

5.1 For each Covered Model, Schedule 1, Part B specifies the region(s) in which model inference may run. A Zro API-key setting may impose a more restrictive region configuration but does not expand the regions permitted by Schedule 1, Part B. If the settings conflict, the more restrictive limitation controls.

5.2 Every inference request is authenticated and routed through Zro's EU gateway. Prompt content may be transferred to US inference infrastructure only where both Customer's API-key configuration and Schedule 1, Part B permit United States processing for the applicable Covered Model.

5.3 Where applicable law requires a transfer mechanism, the parties will cooperate in good faith to implement an applicable adequacy decision, standard contractual clauses, or another lawful transfer mechanism.

5.4 Processor shall ensure that cross-border transfers of Customer Personal Data comply with Applicable Data Protection Laws and this DPA. Non-inference account, authentication, billing and supporting processing may occur in the jurisdictions identified in Schedule 2, subject to Section 4. These supporting locations do not expand the inference regions permitted by Schedule 1, Part B or Customer's API-key settings.

6. Audits and information rights

6.1 Upon Customer's reasonable written request, no more than once in any twelve-month period, Processor shall provide information reasonably necessary to demonstrate compliance with this DPA. This may include responses to a reasonable security questionnaire, summaries of relevant policies and procedures, and summaries of available independent third-party assessments. The frequency limit does not apply where additional information is required by Applicable Data Protection Laws or a supervisory authority, or following a confirmed Personal Data Breach affecting Customer Personal Data.

6.2 Customer shall first use the information available under Section 6.1. If that information is insufficient to demonstrate compliance, audits or inspections may be requested only to the extent required by Applicable Data Protection Laws. An audit shall be limited in scope and duration to what is reasonably necessary, occur during normal business hours on at least thirty (30) days' prior written notice, and be at Customer's cost, subject to reasonable confidentiality, security and operational safeguards. A shorter

notice period or other variation shall apply where required by law or a supervisory authority. An on-site audit is available only where required by Applicable Data Protection Laws.

6.3 A third-party auditor must be independent, suitably qualified, and bound by written confidentiality obligations. An audit must not unreasonably interfere with Processor's operations or compromise other customers' security or confidentiality. The parties shall use reasonable scope limits and redactions to protect unrelated confidential information without preventing disclosure or access required by Applicable Data Protection Laws. Nothing in this Section limits mandatory audit or regulator access rights.

7. Data-subject requests and incidents

7.1 Processor will promptly forward to Customer any data-subject request it receives that relates to Customer Personal Data, unless legally prohibited. Processor will not respond substantively except as instructed by Customer or required by law, but may acknowledge receipt. Customer is responsible for determining the response and responding to the request.

7.2 Processor will provide reasonable assistance to Customer in responding to data-subject requests and security incidents to the extent required by Applicable Data Protection Laws, taking account of the nature of processing and information available to Processor. Fees for assistance are governed by Section 2.3.

7.3 A breach notification will describe, to the extent then known to Processor, the nature of the Personal Data Breach; the categories and approximate numbers of affected Data Subjects and records where available; likely consequences; measures taken or proposed to address it and mitigate its effects; and a contact point for further information. Processor may provide information in phases and will update Customer as further information becomes available without undue further delay.

7.4 Processor will take reasonable steps to contain, investigate and mitigate a Personal Data Breach affecting Customer Personal Data. Notification of, or response to, a Personal Data Breach is not an acknowledgement of fault or liability. Customer is responsible for determining and making notifications to Data Subjects and authorities concerning Customer Personal Data, except where Processor has an independent legal duty to do so.

7.5 Notices under this DPA may be sent to Customer's designated administrative contact, except that breach notices shall use the incident contact designated below or, if none is designated, Customer's administrative contact. Customer is responsible for keeping its contact information current. MoonMath privacy/security contact: [email and responsible contact]. Customer incident contact: [email and responsible contact].

8. Order of precedence, liability, and term

8.1 If this DPA conflicts with the Agreement on the processing of Customer Personal Data, this DPA controls to the extent of that conflict.

8.2 Each party's liability arising out of or in connection with this DPA, whether in contract, tort or under any other theory of liability, is subject to the Agreement's exclusions, limitations and applicable aggregate liability caps, to the extent permitted by applicable law. Claims under this DPA and the Agreement share the applicable caps and do not create a separate or additional cap. Nothing in this DPA

limits a Data Subject's rights under Applicable Data Protection Laws or liability that cannot lawfully be limited.

8.3 This DPA takes effect on the Effective Date stated above and remains in effect while Processor processes Customer Personal Data on Customer's behalf. Sections that by their nature must survive will survive termination.

8.4 If a provision of this DPA is held invalid or unenforceable, the remainder remains in effect to the extent legally permitted.

8.5 This DPA may be amended only by a written instrument signed by both parties, except for the written model and routing approvals expressly permitted by Sections 1.5 and 3.4, subprocessor updates permitted by Section 4, and security-measure updates permitted by Section 3.6. No update to Schedule 2, Schedule 3 or a privacy notice may add a Covered Model or expand a permitted inference route.

9. Signatures

Company:	MoonMath.ai Ltd.
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Schedule 1 — Processing details and Covered Models

Part A — General processing details

Item	Details
Subject matter	Provision of Zro's OpenAI-compatible inference API only for the Covered Models in Part B, and related account, authentication, security, support and billing operations. A model being open-source or Zro-optimized does not make it a Covered Model.
Duration	For the term of the Agreement and any additional period of processing on Customer's behalf, subject to Sections 2.5 and 3.
Nature of processing	Receiving, routing and transiently processing API requests submitted to Covered Models; generating and returning outputs; authentication and account management; metering and billing; monitoring and troubleshooting; preventing abuse; securing and supporting the Service; and compliance with applicable law.
Purpose	To provide the Service according to Customer's documented instructions and the Agreement.
Data subjects	Customer's authorized users, personnel, representatives, customers and end users who administer or access the Service, and other individuals whose data Customer submits, subject to Section 1.9.
Personal data	Inference data: prompts, requests and outputs. Account and billing data: names, emails, organizations, login credentials, account identifiers, IP addresses, billing contacts and payment identifiers handled by the billing provider. Operational data: API-key metadata, selected region, timestamps, request/model identifiers, token and cost totals, latency, status codes, security/reliability logs and support information. Gateway logs exclude payload content under Section 3.1.
Special categories	None intended. Special categories and the other sensitive or regulated data in Section 1.9 are prohibited unless separately agreed in writing with necessary safeguards.
Processing location	EU gateway; model inference only in regions approved for each Covered Model in Part B and permitted by the API-key setting. Supporting processing locations are set out in Schedule 2 and do not expand permitted inference routes.
Retention	Prompts, completions and request bodies are not stored by Zro's gateway and are processed transiently. Account, billing, security, support and usage metadata are retained as necessary to operate the account, subject to Sections 2.5 and 3.5. Subprocessor retention must be completed in Schedule 2.
Transfer frequency	Continuous, on demand, for the duration of Customer's use of the Covered Models and related Service activities.

Part B — Covered Models and approved inference routes

Only the models listed below are Covered Models under this DPA. For each model, list every inference provider and processing location that may receive Customer Personal Data, including any provider used for high traffic, capacity overflow, failover, or disaster recovery. Write “None” if no alternate provider is permitted.

Model name and exact API model identifier	Permitted inference region(s)	Primary inference provider(s) and location(s)	Permitted overflow / fallback provider(s) and location(s)
DeepSeek V4.1 Flash deepseek-v4.1-flash	EU	MoonMath.ai, Israel	None
GLM 5.3 Flash glm-5.3-flash	US	MoonMath.ai, Israel	None

A model's availability in Zro's public catalog or user interface does not add it to this DPA. Any addition or routing change must be documented as required by Sections 1.5 and 3.4.

Schedule 2 — Subprocessors and service providers

The providers below may be used as relevant to the Service. A provider is a subprocessor under this DPA only to the extent it processes Customer Personal Data on Customer's behalf. No provider entry authorizes processing beyond the purposes, models and routes permitted by this DPA. Changes are governed by Section 4; inference changes also require Section 3.4 approval.

Provider / purpose	Data processed	Location(s)	Retention / transfer mechanism
Clerk, Inc. Authentication and identity	Account identifiers, email, IP address and session data.	Clerk and subprocesses may process globally under DPA	https://clerk.com/legal/dpa
Dodo Payments Inc. Billing and payments.	Billing contacts, payment identifiers and account status.	N/A – independent controller for merchant-of-record payments	https://dodopayments.com/legal/data-processing-agreement
PostHog Inc. Product analytics	Account identifier, email, referral source and product events; no prompt or completion bodies.	EU Cloud, Frankfurt, Germany	https://posthog.com/dpa
Google LLC Website / product analytics	Device/browser information, IP address and page paths; no prompt or completion bodies.	Global Processing under accepted Google terms	https://business.safety.google/adsprocessorterms/
Linkup technologies. Optional web search	Search queries and related parameters only when Customer invokes the feature.	Multi-region	https://docs.linkup.so/pages/security-and-privacy/data-processing-privacy ZDR enabled

A named provider may rely on upstream infrastructure as part of its service, subject to the applicable data-protection obligations and lawful transfer requirements. This does not relieve Processor of its obligations or permit an unlisted inference provider or location. Optional web search may disclose query content to the listed search provider; its authorization does not authorize additional inference routes.

The public service-provider description is available at https://zro.moonmath.ai/privacy. It supplements this Schedule and does not expand permissions under this DPA.

Schedule 3 — Technical and organizational measures

Processor shall maintain technical and organizational measures appropriate to the Service and Customer Personal Data, including a written information security program. The agreed measures may be updated under Section 3.6 without materially diminishing the overall level of protection.

S3.1 Access control

Role-based access to production systems and Personal Data is limited to personnel with a documented business need. Multi-factor authentication is mandatory for administrative access to production systems and identity providers. Administrative users have unique accounts and do not share credentials. Access is removed or adjusted on departure or role change; credentials are rotated on those events and suspected compromise.

S3.2 Encryption and secrets

All API traffic and administrative sessions use TLS 1.2 or higher. Account-related Personal Data and backups are encrypted at rest using AES-256 or equivalent industry-standard encryption. Secrets and cryptographic keys are stored in a managed secrets system with role-limited access.

S3.3 Inference data handling

Prompt text, completion text and request bodies are processed transiently and are not stored by Zro's gateway as described in Section 3.1. The no-training and other secondary-use restrictions in Section 3.2 apply to Processor and the subprocessor uses specified there. Permitted primary and overflow inference routes remain limited by Schedule 1, Part B.

S3.4 Network and infrastructure security

Production infrastructure is segmented from corporate systems. Firewalls, security groups and least-privilege network policies restrict inbound and outbound traffic to that required for the Service. Rate limits and abuse-prevention controls address denial-of-service and enumeration attacks. Regular vulnerability scanning supports severity-based triage and remediation.

S3.5 Logging and monitoring

Authentication, administrative actions and privileged-access events are logged for a period appropriate to operational and investigative needs, subject to the DPA's retention and content restrictions. Anomalous activity and production incidents generate alerts handled through an on-call rotation and a documented incident-response process.

S3.6 Personnel security

Authorized personnel are subject to contractual or statutory confidentiality duties under Section 2.2. Background checks are performed for personnel with production-system access to the extent permitted by law. Security-awareness training is provided on onboarding and periodically thereafter.

S3.7 Vendor management

Subprocessors are reviewed for their security and privacy posture before engagement. Written subprocessor agreements impose the protections required by Section 4.2. Inference-provider selection and changes must also comply with Schedule 1, Part B and Section 3.4.

S3.8 Incident response and continuity

A documented incident-response plan covers identification, containment, eradication, recovery and post-incident review. Account-related data is backed up with documented recovery procedures. Operational readiness is reviewed periodically, including tabletop exercises where appropriate. Backups do not authorize retention of inference content contrary to Section 3.1.

S3.9 Secure development

Source code is maintained in a version-controlled repository. Changes to production services require peer review. Dependency and secret scanning are applied to code repositories. Development, staging and production environments are separated.

S3.10 Physical security

Production systems are hosted in third-party data centers whose infrastructure providers maintain physical security controls appropriate to commercial cloud and GPU infrastructure.