RepoQL Data Processing Addendum

Version: 11 September 2026

This Data Processing Addendum ("DPA") forms part of the RepoQL Customer Terms or other written services agreement (the "Agreement") between **Clanker Gear Limited** ("RepoQL", "we" or "us") and the business customer identified in the Order ("Customer" or "you"). It takes effect when both parties accept it in writing or expressly incorporate this version into an accepted Order.

1. Scope

1.1 Customer Personal Information. This DPA covers personal information we process on your behalf to provide the Services ("Customer Personal Information"), including personal information in Customer Content and relevant derived records. A record does not fall outside this DPA merely because it is described as telemetry, an embedding or a log.

1.2 Roles. You determine the purposes of that processing, either for yourself or under authority from the person for whom you act. We process Customer Personal Information on your behalf as described in Schedule 1. "Applicable Privacy Law" means privacy and data-protection law that applies to the relevant processing and party; this DPA does not make an otherwise inapplicable law apply.

1.3 Separate activities. Personal information we independently process to manage our own customer relationships, billing, security and disclosed product analytics is governed by applicable law, the Agreement and our Privacy Policy. This provision does not permit us to reclassify or use Customer Personal Information for independent purposes contrary to this DPA. Shared embedding-cache processing must be addressed in Schedule 1.

1.4 Availability. This DPA does not expand the Agreement's territorial availability or authorise processing that needs a separate legal arrangement. If a required arrangement is absent, the affected processing must not begin or continue. It does not give us access to information held only on infrastructure you control.

2. Instructions and permitted processing

We process Customer Personal Information only to provide the Services described in Schedule 1, on your documented instructions, or as required by law. The Agreement, accepted Order and your authorised use of the Services constitute instructions within the agreed scope. We notify you of a legal requirement to process outside those instructions unless prohibited by law.

You are responsible for the authority, lawful basis, notices and permissions needed for your instructions and submissions. We remain responsible for our own obligations. You must not submit information requiring safeguards or agreements the Services do not provide, unless we have agreed the necessary arrangements in writing.

If we reasonably consider an instruction unlawful or outside the agreed Services, we will notify you and may decline or suspend the affected processing under the Agreement. Additional work or different technical arrangements require agreement; this does not restrict assistance we must provide under Applicable Privacy Law.

The Agreement's no-training and confidentiality protections apply. This DPA grants no right to sell Customer Personal Information, disclose it for advertising, or use it for unrelated purposes.

3. Confidentiality and security

We ensure people authorised to process Customer Personal Information are subject to confidentiality obligations and have access only as needed for their work.

We maintain technical and organisational safeguards appropriate to the nature of the information and the risks of processing, consistent with Applicable Privacy Law and the Agreement. These address access control, protection of stored and transmitted information, service security and incident handling. You remain responsible for infrastructure, credentials and permissions you control.

4. Service providers

You generally authorise us to engage providers to process Customer Personal Information for the Services. Schedule 1 identifies the relevant providers and functions. We require written obligations appropriate to their processing that meet Applicable Privacy Law and provide no less

protection for Customer Personal Information than the applicable obligations of this DPA. We remain responsible for performing our obligations when using providers.

We may replace or add providers, subject to those requirements. Where Applicable Privacy Law or an accepted Order requires notice or an opportunity to object, we provide it, including before the change affects Customer Personal Information where required. We provide information reasonably needed to identify the relevant providers and assess their processing. This does not authorise a materially different processing purpose.

Services you engage independently are governed by your arrangements with their providers.

5. Overseas processing

You authorise processing in the countries used to deliver the Services, including New Zealand and the United States, subject to Applicable Privacy Law. Each party meets its applicable transfer and overseas-disclosure obligations. Where comparable safeguards or a particular transfer instrument are required, they must be in place before the affected processing occurs. This DPA alone does not establish an international-transfer mechanism required by another law.

6. Requests and cooperation

Taking account of the processing and information available to us, we provide reasonable assistance needed for you to meet applicable obligations concerning individual rights, security, breach notifications, privacy and risk assessments, and regulatory enquiries relating to Customer Personal Information.

We refer requests concerning your processing to you unless we must respond directly. Each party remains responsible for duties that apply to it. Where practicable, you should use available service controls to obtain information or carry out requests.

We may agree reasonable charges for assistance beyond the Services, except for work needed to remedy our breach or work we must provide without charge by law. A charge or negotiation does not excuse a mandatory obligation or delay a legally required response.

7. Privacy incidents

We notify you without undue delay after becoming aware of a privacy breach affecting Customer Personal Information processed by us or our providers. This includes unauthorised access, disclosure, alteration, loss or destruction, and loss of availability where it constitutes a privacy breach under Applicable Privacy Law.

We provide available information reasonably needed for you to assess and respond, with material updates as information becomes available, and take reasonable steps to contain and address the breach. We do not wait for a completed investigation before giving required notice. Each party is responsible for notifications required of it by law. Notification does not itself admit liability.

8. Return and deletion

At the end of the relevant Services, or on your lawful instruction, we return or delete Customer Personal Information as required by Applicable Privacy Law and the Agreement. Where applicable law gives you a choice, we follow your choice. This obligation covers relevant copies held by our providers.

Information retained because law requires it, or temporarily held in backups under lawful disclosed retention arrangements, remains protected and is not used for unrelated purposes. Backup arrangements do not extend a shorter binding deletion deadline. Information already discarded through transient processing cannot be returned. You retain control of material held only on your infrastructure.

9. Compliance information

We provide information reasonably necessary to demonstrate compliance with this DPA. We use relevant documentation, responses and available independent reports first. Where Applicable Privacy Law requires further assessment or audit, we allow and cooperate with it under reasonable arrangements for confidentiality, security, timing and scope.

Reviews must protect other customers' information and avoid unnecessary disruption. These arrangements do not prevent a legally required review or access by a competent authority. Charges for extraordinary assistance follow section 6.

10. Conditional US requirements

This section applies to Customer Personal Information subject to an applicable US state privacy law where we process that information on your behalf. Where the California Consumer Privacy Act applies to information disclosed by or on behalf of a customer acting as a business, we undertake the obligations applicable to a service provider or contractor for that processing. Terms used in the applicable law have their statutory meanings.

We process Customer Personal Information only for the limited and specified purposes in this DPA, comply with applicable obligations and provide the level of protection that law requires. In particular, where required by the California Consumer Privacy Act, we will not:

- sell or share Customer Personal Information;
- retain, use or disclose it outside the purposes specified in this DPA or the direct business relationship with you, except as that law permits; or
- combine it with personal information from other customers or our own interactions with individuals, except as that law permits.

We certify that we understand and will comply with those restrictions where applicable. We notify you if we determine we can no longer meet applicable obligations. You may take reasonable and appropriate steps to verify consistent processing and, on notice, stop and remediate unauthorised use. Required assistance, provider contracts and assessment rights apply under sections 4, 6 and 9; contractual procedures must not frustrate statutory rights.

11. Relationship with the Agreement

This DPA controls a conflict concerning Customer Personal Information. Mandatory law and any mandatory transfer terms take priority. The Agreement otherwise continues to apply, including its governing law, dispute provisions, remedies and liability limitations. In the standard RepoQL Customer Terms, DPA claims share the general aggregate cap in section 13.3, subject to sections 13.4 and 13.5. This DPA creates no separate indemnity or additional liability cap and does not limit rights or liabilities that cannot lawfully be limited.

This DPA continues while we or our providers hold Customer Personal Information. Changes require written agreement or acceptance under an agreed variation process; a change to a public notice does not itself amend it.

Schedule 1 — Processing details

Item	Agreed scope
Customer and Services	The customer, Services and relevant subscription or Order identified in the accepted Agreement
Subject matter and purposes	Processing needed to provide the selected repository-analysis features: cloud embeddings, reranking, inference and Uplink; related customer-directed support, troubleshooting and organisation auditing
Operations	Receipt, transmission, analysis and transformation of submitted material; creation and retrieval of embeddings; relay of requests and results; retention of relevant records; return and deletion
People concerned	Authorised users, repository contributors, customer personnel and other individuals whose information the customer lawfully includes in submitted material
Information types	Identifiers, contact and professional details, repository and contribution information, queries and submitted content, and associated service or audit information; sensitive information may appear in submitted material, subject to section 2
Duration	For the relevant Services and any lawful retention required under the Agreement, subject to instructions, deletion obligations and the published limits applicable to each record category
Providers	Google Cloud for cloud hosting and storage; Voyage AI for embeddings and reranking; Fireworks AI for inference; Cloudflare for requests passing through its delivery and routing infrastructure; Datadog where monitoring records contain Customer Personal Information. Each is relevant only to features and records it actually processes.
Privacy contact	RepoQL: **support@repoql.ai**. Customer: its designated privacy or administrative contact under the Order.
Embedding cache	We retain embeddings to avoid repeated computation. Cached results may serve matching requests from different customers using the same source identity and content-derived cache keys. The cache stores

Item	Agreed scope
	vectors rather than source text. Reuse remains subject to this DPA and Applicable Privacy Law.