

RepoQL Privacy Policy

Effective date: 11 September 2026

Last updated: 11 September 2026

RepoQL is operated by **Clanker Gear Limited**, a New Zealand company ("RepoQL", "we", "us" or "our"). This policy explains how we handle personal information through our websites, software, cloud services and related communications.

Address: 156 Stredwick Drive, Torbay, Auckland 0630, New Zealand

Privacy contact: support@repoql.ai

1. Scope and responsibility

Personal information is information about an identifiable individual. This may include account details, online identifiers and information contained in repository material, queries or messages submitted through RepoQL. Hashing or converting information to an embedding does not necessarily make it anonymous.

We handle account, billing and service-administration information for the purposes described here. Where we process information solely on behalf of a customer organisation, the applicable customer agreement also governs that processing. Your organisation may have its own privacy notice and control your access to RepoQL.

Independently supplied agents and other services you connect have their own privacy arrangements. This policy does not govern their independent processing. Service eligibility restrictions do not limit privacy rights that apply to information we hold.

2. Local operation and cloud processing

Your local repositories and index remain on the infrastructure where you run RepoQL. Local processing does not itself give us access to them. When you are signed out, the software does not send us repository content or tool-usage telemetry. Download and update requests expose normal connection information, including IP addresses and request details.

When you use cloud features, we process the information needed to provide them. This includes repository text and queries for embeddings and reranking, prompts and relevant context for inference, and requests and results relayed through Uplink. Relevant inputs are shared with the providers described in section 7.

Cloud request payloads are processed for the request and then discarded. We do not retain copies of those payloads in application storage or logs. We use our embedding, reranking and inference providers under zero-retention, no-training configurations.

Embeddings, telemetry, error messages and feedback are separate retained records, as described below. They can contain or be derived from material supplied through RepoQL.

We do not use your data to train AI models, and require providers receiving that data from us not to use it for model training. This commitment does not govern providers you independently engage.

3. Information we collect and retain

Category	Information involved
Account and organisation information	Names, email addresses, account identifiers, membership, roles, access permissions and subscription status
Billing and service records	Payment and subscription references, transaction information, service usage and repository identifiers used for billing and administration; payment-card information is submitted through our payment provider
Integration information	Authorisation and repository-access metadata for integrations you enable, including the GitHub App
Tool-usage telemetry	Tool and interface used, supplied parameters, outcomes and errors, performance and usage measurements, software and device information, installation and session identifiers, and associated account and organisation identifiers
Embedding cache	Numerical vectors derived from content, associated content hashes and cache-management information; the cache does not store the source text

Category	Information involved
Uplink audits	Metadata about relayed activity, including the member, organisation, instance, tool, target, outcome and timing; audit records do not contain the relayed payload
Feedback and communications	Messages you submit and associated diagnostics, contact information and information needed to respond to enquiries, complaints or privacy requests
Website and operational information	Website analytics and replay information described in section 6, and request, connection and error information used to operate and protect the services

Signed-in tool-usage telemetry is collected unless you opt out. **Recorded parameters and error messages can contain code, credentials, personal information or other confidential material supplied by you or your agent.** Telemetry does not separately attach repository files, your index or returned tool results. Disabling parameter collection does not remove information echoed in error messages.

Cached results may serve matching requests from different customers using the same source identity and content-derived cache keys. We treat content-derived cached embeddings as confidential and provide deletion on an authorised request as described in section 11. Any stricter restrictions in an applicable DPA continue to apply.

Your organisation can view activity recorded through its Uplink access. Feedback submissions include host diagnostics concerning performance, memory and index statistics, without attaching file contents. Feedback messages may contain anything you choose to include and also appear in operational logs.

4. Sources and purposes

We receive information from you, the software and browser you use, organisations administering your access, and providers involved in sign-in, payments and integrations you enable. Repository material and other submissions can include information about other people. We provide any notice required when collecting information indirectly, subject to applicable exceptions.

We use this information to:

- provide requested features, authenticate users and manage accounts and organisations;
- administer subscriptions, billing, plan limits and transactions;
- operate, secure and troubleshoot the services and investigate misuse;
- understand usage and improve RepoQL and our websites;
- provide organisation audit records;
- respond to feedback, enquiries and privacy requests; and
- meet legal obligations and establish, exercise or defend legal rights.

You may choose not to provide information. If it is needed for an account, payment or requested feature, we may be unable to provide that service. Optional telemetry controls are described below. We obtain consent or provide additional notices where required by applicable law.

5. Your choices about the software

You can disable tool-usage telemetry or disable collection of parameter values through RepoQL's telemetry controls. Instructions are available in our [Your data disclosure](#). Disabling parameter values leaves other telemetry, including error messages, enabled.

These controls do not disable records needed to operate cloud features and billing, Uplink audit records, update requests, feedback you submit, or website analytics. They do not delete information already received. You can avoid cloud-feature processing by not using those features and choose whether to submit feedback.

6. Websites, cookies and session replay

We use cookies and similar technologies to operate our websites and portal, support sign-in, understand usage and improve performance. Blocking functional cookies may prevent some features from working.

We use third-party analytics and session replay services to understand usage and diagnose problems. These services collect usage and performance information, device and browser details, and connection information such as IP addresses. Session replay can capture displayed

page content and interactions to reconstruct a visit. For signed-in portal users, we associate this information with account and organisation information, including email address and role. Our providers are described in section 7.

You can manage cookies through your browser. Cookie controls may affect functionality and do not necessarily prevent all analytics collection. The software telemetry controls in section 5 do not control website analytics.

Our website analytics do not automatically switch off in response to browser Do Not Track or Global Privacy Control signals. To exercise privacy rights that apply to your information, contact support@repoql.ai. This does not limit rights or obligations under applicable law.

7. Recipients of information

We share information with providers that support the following functions:

Function	Providers and information involved
Hosting and website delivery	Google Cloud and Cloudflare process information passing through or stored on the infrastructure they provide
Embeddings and reranking	Voyage AI processes relevant text, queries and context
Inference	Fireworks AI processes prompts, context and relevant tool traffic
Monitoring and analytics	Datadog receives tool-usage records and website and portal analytics and replay information
Identity and authentication	WorkOS processes account, sign-in and organisation information
Payments and subscriptions	Stripe processes payment, billing and subscription information
Repository integration	GitHub exchanges information needed to authorise and operate the GitHub App integration

A provider's role and obligations depend on the service and applicable arrangements. Your organisation and its authorised administrators also receive membership, access and activity information relevant to the services they administer.

We may disclose relevant information to professional advisers under confidentiality obligations, in connection with a business sale or reorganisation subject to applicable privacy protections, or where required or permitted by law to meet a specific obligation, resolve a dispute or protect rights and safety. We may also disclose information at your direction or with any consent required by law.

8. Overseas processing

We are based in New Zealand and use infrastructure and providers outside New Zealand, including in the United States. Information may be processed in countries where those providers operate.

Where an overseas disclosure requires comparable safeguards or another legal basis, we comply with the applicable requirements. We remain responsible for our obligations when using providers to process information on our behalf. Contact support@repoql.ai for information about arrangements relevant to your use.

9. Retention

We retain personal information only for as long as needed for the purposes described in this policy or another lawful purpose.

Category	Retention period or criteria
Cloud request payloads	Discarded after the request is processed, as described in section 2
Binary tool-usage telemetry	30 days in the primary store; all operational copies expire within 90 days
Cached embeddings	For cache operation, subject to deletion requests and cache maintenance
Account and subscription records	For administration and, after closure, as needed for outstanding transactions, lawful record-keeping, security or disputes
Billing and related service records	For billing, reconciliation, applicable tax and accounting requirements, and related disputes

Category	Retention period or criteria
Uplink audits	For organisation auditability and investigation of relevant activity
Feedback and correspondence	To address the submission or request and keep an appropriate record of its outcome
Website analytics and session replay	For usage analysis, performance monitoring and troubleshooting; retention is limited by those purposes and any applicable legal requirements
Operational logs	For service operation, fault and abuse investigation, security and applicable legal preservation requirements

The telemetry periods do not apply to other categories. Cancelling a subscription or changing telemetry settings does not itself delete existing records. Retained information remains protected. You control the retention of information held only on your infrastructure.

10. Security

We take reasonable security safeguards appropriate to the information and risks involved. No security measure eliminates every risk. You are responsible for the security, credentials and access settings of infrastructure you operate.

We notify affected people, customer organisations and authorities of privacy breaches as required by applicable law and our agreements.

11. Access, correction, deletion and complaints

Contact support@repoql.ai to request access to or correction of personal information, request deletion, or raise a concern. We may require proportionate verification of your identity and authority.

For access and correction requests under New Zealand law, we communicate our decision as soon as reasonably practicable and normally within **20 working days**, subject to permitted extensions notified to you. Information we agree to provide is supplied without undue delay. If

we decline a correction, you may ask us to attach a statement of the correction sought. We explain refusals and complaint rights as required by law.

We delete cached embeddings derived from repositories you control on request, after verifying your authority and locating the relevant entries, except where retention is required by law.

Requests concerning other records are assessed against applicable rights, retention requirements and agreements. We cannot delete information held only on your infrastructure.

Where your organisation controls the relevant processing, we may coordinate with it or direct the relevant part of your request to it, while meeting our own obligations.

You may complain to the [New Zealand Office of the Privacy Commissioner](#) or another regulator with jurisdiction.

12. Additional privacy rights

Depending on the law that applies, you may have additional rights to obtain a copy of information, correct or delete it, restrict or object to processing, withdraw consent or opt out of particular uses or disclosures. Where applicable, you may use an authorised agent or appeal our decision. Contact support@repoql.ai with your request or appeal. We apply the relevant deadlines, verification requirements and exceptions and do not unlawfully discriminate against people exercising privacy rights.

The information categories described above include identifiers, commercial information, internet and device activity, and submitted content. Submitted content may include sensitive personal information. Sources, purposes, recipients and retention are described in sections 3–9.

13. Children

RepoQL is a developer tool and is not directed at children. Contact support@repoql.ai if you believe a child has supplied information in circumstances requiring protection that has not been provided. We take action required by applicable law.

14. Changes to this policy

We may update this policy and its date. We notify you of material changes through a website or account notice, or by email, before the change takes effect where required by law. We obtain consent where required. An update does not reduce mandatory rights or override an applicable customer agreement.

Contact [**support@repoql.ai**](mailto:support@repoql.ai), or write to Clanker Gear Limited at the address above, with questions about this policy.