Redpine

DATA PROCESSING AGREEMENT

- last updated 24 June, 2026

This Data Processing Agreement (the "DPA") is entered into between Redpine Technology AB, reg. no. 559499-8824 ("Redpine" or the "Processor"), and the customer named in the applicable Agreement (the "Customer" or the "Controller"). It forms part of, and is incorporated by reference into, the Customer's Content Partner Master Services Agreement or API Access Terms (the "Agreement"). Capitalized terms not defined here have the meanings given in the Agreement.

Scope. This DPA applies where the Customer submits queries or other data through the Platform that contain personal data of other individuals, which Redpine processes on the Customer's behalf as processor. Personal data that Redpine processes for its own operational purposes (onboarding, account administration, billing and support of the Customer's account) is processed by Redpine as an independent controller under Redpine's Privacy Policy and is not governed by this DPA.

1. Definitions

In this DPA:

"Data Protection Law" all applicable laws and regulations relating to the processing of personal data and privacy, including the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), the UK GDPR and the UK Data Protection Act 2018, the Swedish Data Protection Act (2018:218), the California Consumer Privacy Act / California Privacy Rights Act, and any other comparable laws in jurisdictions where Personal Data is processed.

"Personal Data" information protected as personal data, personal information or personally identifiable information under Data Protection Law, where processed by the Processor on behalf of the Controller under the Agreement (the "Processed Data").

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

"Processing" any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, erasure or destruction.

"Sub-processor" any third party engaged by the Processor to process Personal Data on its behalf.

"Personal Data Breach" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

"Supervisory Authority" an independent public authority established under Data Protection Law.

"Standard Contractual Clauses" or "SCCs" (i) for transfers from the EEA, the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021; and (ii) for transfers from the UK, the UK International Data Transfer Addendum, as the case may be.

"Platform" the Redpine platform, including its API, MCP and CLI interfaces, through which the services under the Agreement are provided.

2. Roles and Scope of Processing

2.1 Roles. The Controller is the controller and the Processor is the processor of the Processed Data. The Processor processes Personal Data only on documented instructions from the Controller, including the Agreement, this DPA and the parameters set out in Annex 1, unless required to act otherwise by Union or Member State law (in which case the Processor will inform the Controller before processing, unless that law prohibits it on important grounds of public interest).

2.2 Customer's instructions. The Controller's instructions to the Processor are: (i) the Agreement; (ii) this DPA; (iii) Annex 1 (Details of Processing); and (iv) any further instructions agreed in writing by the Parties. The Processor will inform the Controller if, in its opinion, an instruction infringes Data Protection Law.

Redpine

2.3 Out-of-scope data. Personal data contained in Content provided by content partners is processed under separate controller-to-controller terms and is outside the scope of this DPA.

3. Confidentiality

3.1 The Processor ensures that persons authorized to process the Personal Data are subject to appropriate confidentiality obligations or statutory duties of confidentiality, and process the Personal Data on a need-to-know basis.

4. Security

4.1 The Processor implements the technical and organizational measures set out in Annex 3 (Security Measures), which the Parties agree provide a level of security appropriate to the risk, taking into account the state of the art, costs, and the nature, scope, context and purposes of processing as well as the risk to Data Subjects (Article 32 GDPR). The Processor may update these measures from time to time provided the overall level of security is not materially reduced.

5. Sub-processors

5.1 General authorization. The Controller provides the Processor with general written authorization to engage Sub-processors, subject to this Section. A list of current Sub-processors is available on request to legal@redpine.ai.

5.2 Notice of changes. The Processor will give the Controller at least thirty (30) days' prior notice of any addition or replacement of a Sub-processor. The Controller may reasonably object on data-protection grounds within that period; the Parties will work in good faith to resolve the objection. Failing resolution, the Controller may terminate the affected processing or Agreement.

5.3 Sub-processor obligations and liability. The Processor imposes on each Sub-processor data-protection obligations no less protective than those in this DPA and remains liable to the Controller for the acts and omissions of its Sub-processors.

6. Assistance to the Controller

6.1 Data Subject rights. Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organizational measures, insofar as possible, to respond to Data Subject requests under Articles 12–23 GDPR. If a request is made directly to the Processor, the Processor will promptly forward it to the Controller and will not respond except on the Controller's instruction or as legally required.

6.2 Security, breach and DPIAs. The Processor assists the Controller in ensuring compliance with Articles 32–36 GDPR (security, breach notification, data-protection impact assessments and prior consultation), taking into account the information available to the Processor.

7. Personal Data Breach

7.1 The Processor notifies the Controller without undue delay and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting the Processed Data, and provides information reasonably available to enable the Controller to meet its breach-notification obligations under Data Protection Law.

7.2 The notification will include, where known, the nature of the breach (categories and approximate numbers of Data Subjects and records affected), likely consequences, and measures taken or proposed to address it and mitigate adverse effects.

8. Deletion or Return

8.1 At the Controller's choice, on termination or expiry of the Processing or this DPA, the Processor deletes or returns to the Controller all Personal Data and deletes existing copies, unless Union or Member State law requires further retention. Security backups and immutable logs are deleted in the ordinary course of the Processor's retention cycle.

9. Audits

9.1 The Processor makes available to the Controller the information necessary to demonstrate compliance with Article 28 GDPR and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor it

mandates (bound by confidentiality), on reasonable prior notice, no more than once per twelve (12) months (save where required by a Supervisory Authority or following a Personal Data Breach), subject to confidentiality and minimal disruption to the Processor's operations. Where applicable, audit obligations may also be discharged by providing recent independent assessment reports.

10. International Transfers

10.1 Where the Processor transfers Personal Data outside the EEA / UK to a country not offering an adequate level of protection under Data Protection Law, the Standard Contractual Clauses are incorporated by reference and apply between the Parties (Module 2: controller-to-processor; and Module 3 for any onward processor-to-processor transfer to Sub-processors). Where the Customer is located outside the EEA / UK, the Parties will reasonably cooperate to put in place an appropriate transfer mechanism (including, where relevant, the UK Addendum or comparable mechanism). Where the recipient of a transfer is certified under the EU-U.S. Data Privacy Framework (or, as applicable, the UK Extension to it or the Swiss-U.S. Data Privacy Framework) and the certification covers the relevant processing, the Parties may rely on that certification as the applicable transfer mechanism in place of the Standard Contractual Clauses, for so long as the certification and the underlying adequacy decision remain valid.

10.2 For transfers from the UK, the UK International Data Transfer Addendum to the SCCs applies.

10.3 Supplementary measures (e.g. encryption in transit and at rest, access controls, transfer impact assessments) are applied where required by Data Protection Law.

11. CCPA / US State Privacy Laws

11.1 Where the California Consumer Privacy Act / California Privacy Rights Act (or comparable US state privacy laws) applies, the Processor acts as a "service provider" / "processor" and does not (a) sell or share Personal Data; (b) retain, use or disclose Personal Data for any purpose other than the business purposes specified in the Agreement and this DPA; or (c) combine the Personal Data with personal information that the Processor receives from, or on behalf of, other persons, except as permitted by law. The Processor will provide the Controller with the assistance reasonably necessary to comply with consumer requests under such laws.

12. Liability and Relationship to the Agreement

12.1 Each Party's liability arising out of or in connection with this DPA is subject to the limitations and exclusions of liability in the Agreement. Nothing in this DPA varies the liability arrangements in the Agreement.

12.2 In the event of conflict between this DPA and the Agreement in relation to the processing of Personal Data, this DPA prevails.

13. Term and Survival

13.1 This DPA takes effect on the date of the Agreement (or the date of its execution if later) and remains in force for as long as the Processor processes Personal Data on the Controller's behalf. Provisions that by their nature should survive (including Sections 3, 4, 7, 8, 10 and 11) survive termination.

14. Contact

14.1 Privacy contact for both Parties. All notices and communications under this DPA, including breach notifications and sub-processor change notices, are to be sent to legal@redpine.ai (Processor) and to the Controller contact specified in the Agreement (or, if none, to the privacy / data-protection contact identified in the Controller's privacy policy).

Annex 1 - Details of Processing

A.1 Subject matter. Processing of personal data submitted by the Controller through the Platform as part of its queries and use of the Platform (authentication and query processing). Account administration, billing and support data is processed by Redpine as an independent controller and is outside the scope of this DPA.

A.2 Duration. For the term of the Agreement and for any retention period required by Data Protection Law.

Redpine

A.3 Nature and purpose. Hosting, transmission, indexing, retrieval and generation of Outputs in respect of personal data submitted through the Platform.

A.4 Categories of Personal Data. (Personal data that the Controller submits as part of queries to, or other use of, the Platform.

A.5 Categories of Data Subjects. Where the Controller submits queries or other data containing personal data of other individuals, those Data Subjects (whose categories the Controller is responsible for identifying in advance).

A.6 Sensitive data. Sensitive or special-category data should not be submitted to the Platform except where the Controller has confirmed in writing it has a valid basis. The Processor implements heightened protections where the Controller flags such data.

A.7 Frequency and method. Continuous, as required to operate the Platform; via the Agreement's technical interfaces (API, MCP, CLI, Dashboard) and standard support channels.

Annex 2 - Standard Contractual Clauses

D.1 EU SCCs. Where personal data is transferred from the EEA to a country not offering an adequate level of protection, the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are incorporated by reference and apply between the Parties. Module 2 (controller-to-processor) applies between the Parties; Module 3 (processor-to-processor) applies to onward transfers to Sub-processors. Optional clauses are selected as follows: Clause 7 (docking) — included; Clause 9(a) — general authorisation (30 days' notice); Clause 11(a) (independent dispute-resolution) — not selected; Clause 17 (governing law) — Sweden; Clause 18 (forum and jurisdiction) — Sweden.

D.2 UK transfers. For transfers subject to the UK GDPR, the UK International Data Transfer Addendum to the EU SCCs (the "UK Addendum") is incorporated by reference, with Tables 1, 2 and 3 populated from this DPA and its Annexes. Either Party may invoke the right to terminate under the UK Addendum where required.

D.3 Swiss transfers. For transfers subject to the Swiss Federal Act on Data Protection (FADP), the EU SCCs apply with the following adjustments: references to "Member State" include Switzerland; the Swiss Federal Data Protection and Information Commissioner is the competent authority; and "personal data" includes data relating to legal entities where protected by the FADP.

Annex 3 — Security Measures

This Annex sets out the technical and organizational measures the Processor maintains under Section 4 (Article 32 GDPR). The Processor may update these measures from time to time provided the overall level of security is not materially reduced.

S.1 Access architecture. All access to Content and the services occurs exclusively through the Platform's API, MCP and CLI interfaces; there is no direct access to underlying storage. A valid, authenticated key is required and is bound to a specific person; unauthenticated requests are rejected. Access is transaction-limited (stateless micro-access), and the Platform does not provide persistent bulk access, database replication or dataset delivery.

S.2 Controls and monitoring. Dynamic rate limiting at key and organization level; logging of every transaction with an available audit trail; an immediate kill-switch to disable access per key, per organization or platform-wide; and least-privilege, need-to-know access controls with authentication for Processor personnel. The Processor may apply further safeguards such as anomaly detection and output marking.

S.3 Standard, hosting and resilience. Industry-standard administrative, technical and physical safeguards appropriate to the risk; Content encrypted in transit and at rest; personnel bound by confidentiality obligations; vulnerability management and tested change-control processes; and backup and business-continuity measures appropriate to the service.

S.4 Sub-processors. Where the Processor uses third-party infrastructure or service providers, it imposes obligations consistent with this DPA and remains responsible for their performance (see Section 5).

S.5 Incident notification. The Processor notifies affected parties of any confirmed security incident without undue delay and cooperates in good faith on remediation (see Section 7).