Prody

Data Processing Agreement

Effective: March 16, 2026 | Version 1.0

This Data Processing Agreement ("DPA") forms part of the Master Service Agreement or Terms of Service ("Agreement") between Prody ("Processor," "we," "us") and the entity identified in the signature block below ("Controller," "Customer," "you") for the provision of the Prody product analytics platform ("Service").

1. Definitions

- **"Customer Data"** means all data submitted to the Service by or on behalf of Controller.
- **"Personal Data"** means any Customer Data that relates to an identified or identifiable natural person, as defined under applicable Data Protection Laws.
- **"Data Protection Laws"** means all applicable data protection and privacy laws, including the EU General Data Protection Regulation (GDPR), the UK GDPR, the California Consumer Privacy Act (CCPA), and any amendments thereto.
- **"Processing"** means any operation performed on Personal Data, including collection, storage, use, disclosure, and deletion.
- **"Sub-Processor"** means a third party engaged by Processor to process Personal Data on behalf of Controller.
- **"Data Subject"** means an identified or identifiable natural person whose Personal Data is processed.
- **"DSAR"** means a Data Subject Access Request under applicable Data Protection Laws.

2. Scope and Roles

2.1 Controller determines the purposes and means of Processing Personal Data. Processor processes Personal Data solely on behalf of Controller and in accordance with Controller's documented instructions.

2.2 This DPA applies to all Personal Data processed by Processor in connection with the Service.

3. Data Processing Details

Subject Matter	Provision of product analytics services as described in the Agreement
Duration	The Subscription Term plus any data retention period
Nature and Purpose	Collection, storage, analysis, and visualization of product usage data; AI-powered anomaly detection,
Types of Personal Data	User identifiers (email, name, external ID), IP addresses, device information, behavioral events, page
Data Subject Categories	End users of Controller's product(s), Controller's employees and contractors
Processing Location	United States

4. Processor Obligations

4.1 **Instructions.** Process Personal Data only on documented instructions from Controller, unless required by law.

4.2 **Confidentiality.** Ensure that persons authorized to process Personal Data are bound by confidentiality obligations.

4.3 **Security.** Implement appropriate technical and organizational measures to protect Personal Data (see Section 7).

4.4 **Sub-Processors.** Not engage a new Sub-Processor without prior notice to Controller (see Section 5).

4.5 **DSAR Assistance.** Assist Controller in responding to Data Subject requests using built-in PII tools (lookup, export, anonymization, deletion).

4.6 **Breach Notification.** Notify Controller without undue delay (and in any event within 72 hours) after becoming aware of a Personal Data breach (see Section 8).

4.7 **Deletion.** Upon termination of the Agreement, delete or return all Personal Data within 30 days, unless retention is required by law.

4.8 **Audit Cooperation.** Make available to Controller all information necessary to demonstrate compliance with this DPA (see Section 10).

5. Sub-Processors

5.1 Controller authorizes Processor to engage the Sub-Processors listed below. Processor will impose data protection obligations on each Sub-Processor that are no less protective than those in this DPA.

Sub-Processor	Purpose	Location
Anthropic	AI processing (Signals, Ask Prody, Discoveries)	United States
Railway	Application and database hosting	United States
Resend	Transactional email delivery	United States
Cloudflare	DNS management and marketing site hosting	United States

5.2 Processor will notify Controller at least 30 days before engaging a new Sub-Processor. If Controller objects, Controller may terminate the Agreement as described in Section 9.

6. Data Subject Rights

The Service provides built-in tools for Controller to fulfill Data Subject rights:

- **Right of Access:** PII Lookup tool retrieves all data associated with an email or external ID.
- **Right to Portability:** PII Export generates a CSV export of all user data.

- **Right to Erasure:** PII Anonymization replaces identifying information with hashed values. Full deletion permanently removes all user records.
- **Right to Rectification:** User attributes (name, email, external ID) can be updated via the admin interface or API.

7. Security Measures

Processor implements the following technical and organizational security measures:

- Encryption in transit (TLS 1.2+) and at rest (infrastructure-level database encryption)
- Per-tenant data isolation via tenant-scoped database queries on all routes, jobs, and API endpoints
- bcrypt password hashing (cost factor 10)
- httpOnly, Secure, SameSite=Strict session cookies with 24-hour expiration
- Security headers via Helmet.js (CSP, X-Frame-Options, HSTS, X-Content-Type-Options)
- XSS protection via HTML escaping on all user-supplied content
- SQL injection prevention via parameterized queries
- Rate limiting on authentication endpoints and API routes
- Input validation with max length enforcement, HTML tag stripping, and control character rejection
- Environment variable storage for all secrets (no credentials in source code)

8. Breach Notification

8.1 Processor will notify Controller without undue delay, and in any event within 72 hours, after becoming aware of a breach of Personal Data.

8.2 The notification will include: (a) the nature of the breach including the categories and approximate number of Data Subjects and records affected; (b) the likely consequences of the breach; (c) the measures taken or proposed to address the breach.

8.3 Processor maintains a formal incident response procedure with 4-level severity classification (P0-P3), defined response times, and a 5-step process: Contain, Assess, Notify, Remediate, Post-Incident Review.

9. Data Retention and Deletion

9.1 Processor retains Customer Data for the duration of the Subscription Term plus any customer-configured retention period. Automated nightly cleanup enforces retention limits.

9.2 Upon termination of the Agreement, Processor will: (a) make Customer Data available for export for 30 days; (b) delete all Customer Data within 30 days of the export period ending, unless retention is required by applicable law.

10. Audit Rights

10.1 Controller may audit Processor's compliance with this DPA once per year, with at least 30 days written notice. Audits will be conducted during business hours and will not unreasonably interfere with Processor's operations.

10.2 Processor will provide Controller with copies of relevant security certifications, audit reports, or completed security questionnaires upon reasonable request.

11. International Transfers

11.1 Customer Data is processed and stored in the United States. If Controller is located in the European Economic Area (EEA), United Kingdom, or Switzerland, the parties agree that transfers of Personal Data to the United States are governed by the EU Standard Contractual Clauses (SCCs) as approved by the European Commission, which are incorporated by reference.

11.2 Processor will promptly inform Controller if it becomes aware that it can no longer comply with the SCCs or any applicable transfer mechanism.

12. General Provisions

12.1 **Governing Law.** This DPA is governed by the laws of the State of Delaware, USA, to the extent not superseded by applicable Data Protection Laws.

12.2 **Conflicts.** In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

12.3 **Term.** This DPA shall remain in effect for the duration of the Agreement and for as long as Processor continues to process Personal Data on behalf of Controller.

12.4 **Contact.** For questions about this DPA, contact privacy@prody.com.

PRODY

Signature: ______________________________

Name: __________________________________

Title: ___________________________________

Date: ___________________________________

CUSTOMER

Signature: ______________________________

Name: __________________________________

Title: ___________________________________

Date: ___________________________________