# Data Processing Agreement

Between the customer ('**Controller**') and **Enrevia Technologies Ltd** ('**Processor**', operating the Enrevia Connect platform).

Document version: 2.0

Effective date: 2026-06-27

This DPA is the standard form referenced by the Enrevia Connect Terms of Service. Acceptance occurs by continued use of the service after the effective date; a countersigned PDF is available on request by emailing legal@enrevia-connect.com.

This agreement reflects the parties' arrangement on the processing of personal data as required by Article 28 of the EU General Data Protection Regulation ('**GDPR**'), the UK GDPR, and, where applicable, the California Consumer Privacy Act ('**CCPA**'). Where personal data is transferred outside the EEA or UK, the Standard Contractual Clauses ('**SCCs**') incorporated as Annex II of this document apply.

## 1. Definitions

**'Applicable Data Protection Laws'** means the GDPR, the UK GDPR, the CCPA, and any other privacy or data protection law applicable to the processing of Personal Data under this DPA.

**'Personal Data'** means any information relating to an identified or identifiable natural person processed by Processor on behalf of Controller under the principal agreement.

**'Process' / 'Processing'** means has the meaning given in Article 4(2) of the GDPR.

**'Data Subject'** means the identified or identifiable natural person to whom Personal Data relates.

**'Sub-processor'** means any third party engaged by Processor to Process Personal Data on Controller's behalf.

**'Standard Contractual Clauses' / 'SCCs'** means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission and, where applicable, the UK International Data Transfer Addendum.

**'Security Incident'** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

## 2. Subject Matter and Duration of Processing

Subject matter: the Processing necessary to provide the Enrevia Connect sales, marketing, prospecting, and customer engagement platform to Controller in accordance with the principal agreement.

Duration: this DPA takes effect on the Effective Date and continues for the duration of the principal agreement plus any post-termination data export period (30 days by default, extended for Enterprise customers per the principal agreement).

## 3. Nature and Purpose of Processing

Processor processes Personal Data only to provide the platform features Controller has enabled, including: customer relationship management, contact enrichment, outbound email + social outreach, AI-assisted content

generation, analytics and reporting, billing administration, and account support. Processor will not Process Personal Data for any other purpose without Controller's prior written instructions.

## 4. Type of Personal Data and Categories of Data Subjects

### Types of Personal Data (illustrative, not exhaustive):

- Identification data: name, email, phone, job title, employer, public profile URLs
- Communication data: email + message bodies, attachments, calendar events, meeting transcripts
- Behavioural data: app usage, click events, opens, page views, integration sync history
- Inferred data: lead scores, intent signals, AI-generated summaries and classifications
- Authentication data: hashed passwords, SSO assertions, refresh tokens (encrypted at rest)
- Billing data: company name, billing address, VAT/TIN, payment status (card data handled exclusively by Stripe)

### Categories of Data Subjects:

- Controller's employees, contractors, and agents using the platform
- Controller's customers, prospects, leads, and contacts whose data is uploaded, integrated, or scraped through the platform
- Recipients of email, SMS, or social messages sent through the platform

## 5. Obligations of the Processor

Processor shall:

- Process Personal Data only on documented instructions from Controller, including with regard to transfers to a third country, unless required to do so by Union or Member State law
- Ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Implement the technical and organisational measures set out in Annex II
- Respect the conditions for engaging Sub-processors set out in clause 8 of this DPA
- Assist Controller in fulfilling its obligation to respond to Data Subject requests under Articles 12-23 of the GDPR
- Assist Controller in ensuring compliance with the obligations under Articles 32-36 of the GDPR taking into account the nature of Processing and the information available to Processor
- At Controller's choice, delete or return all Personal Data after the end of the provision of services, unless retention is required by Applicable Data Protection Laws
- Make available to Controller all information necessary to demonstrate compliance with Article 28 of the GDPR
- Immediately inform Controller if, in its opinion, an instruction infringes Applicable Data Protection Laws

## 6. Security Measures

Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including those set out in Annex II of this DPA. The current state of these measures is also published on the public security page at https://enrevia-connect.com/legal/security, which is updated whenever a material control changes. The published page and Annex II must agree; any conflict is to be reported to security@enrevia-connect.com.

## 7. Personal Data Breach Notification

Processor shall notify Controller without undue delay, and in any event within 72 hours of becoming aware, of any Security Incident affecting Personal Data Processed under this DPA. The notification shall include, to the extent reasonably available at the time of notification:

- a description of the nature of the Security Incident, including the categories and approximate number of Data Subjects and Personal Data records concerned
- the name and contact details of the Processor's Data Protection Officer or other contact point
- the likely consequences of the Security Incident
- the measures taken or proposed to address the Security Incident and mitigate its possible adverse effects

## 8. Sub-processors

Controller provides a general authorisation for Processor to engage Sub-processors. A current list of Sub-processors is maintained as Annex III of this DPA and republished on the security page at https://enrevia-connect.com/legal/security.

Processor shall give Controller at least 30 days' prior notice of any intended addition or replacement of a Sub-processor. Notice is delivered via the in-app notification centre, an email to the Controller's billing contact, and a security-page changelog entry. Controller may object to a proposed change on reasonable data-protection grounds within the notice period; where the parties cannot resolve the objection, Controller may terminate the affected portion of the principal agreement.

Processor shall enter into a written agreement with each Sub-processor imposing data-protection obligations no less protective than those in this DPA, and remains fully liable to Controller for the performance of the Sub-processor's obligations.

## 9. Audit Rights

Processor shall make available to Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Controller or another auditor mandated by Controller.

In practice, Controller's audit rights are satisfied by: (a) the most recent SOC 2 Type II report (when available), (b) the most recent third-party penetration test executive summary, (c) responses to Controller's security questionnaire, and (d) the public security page. Controller may request an on-site audit no more than once per calendar year on at least 30 days' written notice; the parties shall agree the scope, duration, and cost allocation prior to the audit.

## 10. International Transfers

Where Processor transfers Personal Data outside the EEA, the UK, or Switzerland to a country not the subject of an adequacy decision, such transfers are made under the Standard Contractual Clauses (Module Two: controller-to-processor) incorporated by reference into this DPA. For transfers from the UK, the parties further incorporate the UK International Data Transfer Addendum to the SCCs issued by the Information Commissioner's Office.

Annex I (Description of Transfer) and Annex II (Technical and Organisational Measures) below complete the SCCs.

## 11. Liability and Indemnification

Each party's liability under or in connection with this DPA, whether in contract, tort (including negligence) or otherwise, is subject to the limitations and exclusions of liability set out in the principal agreement. Nothing in this DPA limits or excludes either party's liability for: (a) death or personal injury caused by its negligence; (b) fraud or fraudulent misrepresentation; or (c) any other liability which cannot be limited or excluded by Applicable Data Protection Laws.

[Placeholder for negotiated indemnification language. Default form to be supplied per principal agreement; Enterprise customers receive custom indemnification per their MNDA + order form.]

## 12. Term and Termination

This DPA terminates automatically on termination or expiry of the principal agreement. On termination, Processor shall, at Controller's choice expressed within 30 days of termination, delete or return all Personal Data Processed under this DPA, and delete existing copies, unless Applicable Data Protection Laws require storage of the Personal Data. The certified data export endpoint documented at https://enrevia-connect.com/legal/privacy satisfies Controller's portability rights for the avoidance of doubt.

# Annex I — Description of Transfer

## A. List of Parties

**Data exporter (Controller):** the customer of Enrevia Connect identified in the principal agreement.

**Data importer (Processor):** Enrevia Technologies Ltd, operating the Enrevia Connect platform. Contact for data-protection matters: dpo@enrevia-connect.com.

## B. Description of Transfer

Categories of Data Subjects: see clause 4.

Categories of Personal Data: see clause 4.

Sensitive data: the platform is not designed to Process special categories of personal data within the meaning of Article 9 of the GDPR. Controller is responsible for not uploading sensitive data outside of the platform's documented intended use.

Frequency of transfer: continuous, on a per-action basis as Controller uses the platform.

Nature of the processing: see clauses 2 and 3.

Purpose(s) of the data transfer and further processing: see clauses 2 and 3.

Retention period: for the duration of the principal agreement, plus 30 days post-termination for export, plus any retention period required by Applicable Data Protection Laws (e.g. financial records).

## C. Competent Supervisory Authority

Where Controller is established in the EEA: the supervisory authority of the EU Member State in which Controller is established. Where Controller is established in the UK: the Information Commissioner's Office.

## Annex II — Technical and Organisational Measures

Processor implements and maintains the following measures. Controller may verify their current state at https://enrevia-connect.com/legal/security; any divergence between this Annex and the security page is to be reported to security@enrevia-connect.com and treated as a documentation defect to be corrected without delay.

### Encryption in transit

All customer traffic terminates at Caddy with TLS 1.3 only; HSTS preload with 1-year max-age + includeSubDomains. Internal service-to-service calls inside the VPC use AWS PrivateLink where supported.

### Encryption at rest

Database storage encrypted via AWS EBS encryption (AES-256). S3 backup objects encrypted server-side with AES-256 + object versioning + 90-day retention. OAuth tokens and integration secrets additionally wrapped with AES-256-GCM application-level envelope encryption before storage.

### Password storage

User passwords hashed with bcrypt at cost factor 12. Plaintext passwords are never logged or stored. Passwordless flows are available for SSO customers.

### Tenant isolation

Multi-tenant via shared database with mandatory agencyId scoping on every query. Isolation enforced by Prisma model relationships, not just UI gating. Cross-tenant queries are explicitly opt-in and gated behind isPlatformAdmin checks.

### Access controls

Role-based permissions (Owner, Admin, Manager, Member, Viewer). Destructive operations require Manager or Admin. Sessions are JWT-based with 8-hour idle timeout + 1-hour refresh, server-side revocation via tokensValidAfter.

### SSO + SCIM

SAML 2.0 SSO + SCIM 2.0 user provisioning available on Business and Enterprise plans. Identity provider integrations include Okta, Microsoft Entra, Google Workspace, and JumpCloud.

### Backup + restore

Daily encrypted pg_dump exports to AWS S3 with 90-day retention. Backup recency monitored on every health check; stale snapshots trigger the public status page. Quarterly restore drills verify recoverability against a freshly provisioned Postgres container.

### Logging + auditing

Mutating actions captured in an append-only ActivityLog table. Business plan: 1-year retention; Enterprise: 7-year immutable retention with WORM semantics on the audit store.

### Vulnerability management

Dependabot on the main repo with weekly automated PRs. CVE advisories triaged within one business day. Annual third-party penetration test on the production application.

### Incident response

24/7 on-call rotation for security incidents. Personal-data breaches notified to Controller without undue delay and in any event within 72 hours of becoming aware.

### Sub-processor management

All sub-processors contractually bound to GDPR Article 28 obligations. Sub-processor changes published on the security page with at least 30 days' notice before they begin processing.

### Personnel security

All staff with production access complete annual security training. Background checks completed prior to grant of production access. Production access via SSO + hardware MFA.

## Annex III — Sub-processors

The Sub-processors listed below have been authorised by Controller in accordance with clause 8 of this DPA. The current list is also published on the security page; the published page is authoritative for any list-update timing questions.

| Sub-processor | Service | Location | Transfer mechanism |
|---|---|---|---|
| Amazon Web Services, Inc. (AWS) | Cloud hosting (EC2, S3, RDS in roadmap), database backups, transactional + marketing email (SES), AI inference (Bedrock) | United States (us-east-1) | EU-US DPF + SCCs |
| Stripe Payments Europe, Ltd. + Stripe, Inc. | Payment processing, subscription billing, invoicing | United States; Ireland (EU customers) | EU-US DPF + SCCs |
| Anthropic, PBC | AI inference for content generation, summarization, classification (also delivered via AWS Bedrock under the AWS contract) | United States | SCCs (zero-retention enterprise tier) |
| OpenAI, L.L.C. | Fallback AI inference + embeddings for search + classification | United States | SCCs (zero-retention API tier) |
| Resend (Plus Five Five, Inc.) | Transactional email delivery fallback for non-SES regions | United States | SCCs |
| Sentry (Functional Software, Inc.) | Error tracking and performance monitoring | United States | SCCs (PII scrubbing enabled) |

Sub-processor changes are notified per clause 8. To subscribe to change notifications without checking the page, email security@enrevia-connect.com with subject 'Sub-processor notifications'.

## Signatures

This static PDF is the template form of the agreement. A countersigned copy with the Controller's details filled in is available by emailing legal@enrevia-connect.com; the executed version supersedes this template for the parties that signed it.

| For Controller | For Processor |
|---|---|
| | Enrevia Technologies Ltd |
| Signature: _____ | Signature: _____ |
| Name: _____ | Name: _____ |
| Title: _____ | Title: _____ |
| Date: _____ | Date: _____ |
| Email: _____ | Email: legal@enrevia-connect.com |

Questions about this DPA: legal@enrevia-connect.com. Security questions: security@enrevia-connect.com. Data-protection enquiries: dpo@enrevia-connect.com.