CLEARPATH

Programme Management

DATA PROCESSING ADDENDUM

Last updated: April 2026

This Data Processing Addendum ("DPA") forms part of the Clearpath Terms and Conditions of Service (the "Agreement") and sets out the terms on which the Provider will process Personal Data on behalf of the Customer in connection with the provision of the Clearpath programme management platform, in compliance with Article 28 of the UK General Data Protection Regulation.

1. DEFINITIONS

1.1 In this Data Processing Addendum ("DPA"), the following definitions apply in addition to those set out in the Terms and Conditions:

"Data Protection Law" means the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, the Data Use and Access Act 2025, and any successor or amending legislation, together with all applicable guidance and codes of practice issued by the Information Commissioner's Office (ICO).

"Personal Data", "Data Controller", "Data Processor", "Data Subject", "Processing", "Personal Data Breach", and "Special Categories of Personal Data" have the meanings given in Data Protection Law.

"Customer Personal Data" means any Personal Data that the Provider processes on behalf of the Customer in connection with the provision of the Service.

"Sub-processor" means any third party engaged by the Provider to process Customer Personal Data on behalf of the Customer.

"Approved Jurisdiction" means the United Kingdom, the European Economic Area, or any country or territory recognised as providing an adequate level of data protection by the UK Secretary of State under section 17A of the Data Protection Act 2018.

2. SCOPE AND ROLES

2.1 This DPA applies to all Processing of Customer Personal Data by the Provider in connection with the Service. It is incorporated into and forms part of the Terms and Conditions of Service between the Provider and the Customer (the "Agreement").

2.2 The Customer is the Data Controller in respect of Customer Personal Data. The Provider is the Data Processor.

2.3 Nothing in this DPA relieves the Customer of its own obligations under Data Protection Law, including its obligation to establish a lawful basis for processing and to provide appropriate notices to Data Subjects.

2.4 The details of the processing are set out in Schedule 1 to this DPA. The Customer may update the description of processing by written notice to the Provider, provided that any such update does not impose obligations on the Provider beyond those contemplated by the Agreement.

3. PROVIDER OBLIGATIONS

3.1 The Provider shall process Customer Personal Data only in accordance with the Customer's documented instructions, which are deemed to include: (a) the instructions set out in this DPA and the Agreement; (b) instructions given through the Customer's configuration and use of the Service; and (c) any additional written instructions agreed between the parties. The Provider shall not process Customer Personal Data for any other purpose.

3.2 If the Provider is required by applicable law to process Customer Personal Data other than in accordance with the Customer's instructions, the Provider shall inform the Customer of that legal requirement before processing, unless the law prohibits such notification on important grounds of public interest.

3.3 The Provider shall promptly inform the Customer if, in the Provider's reasonable opinion, an instruction from the Customer infringes Data Protection Law.

3.4 The Provider shall ensure that all personnel who have access to Customer Personal Data: (a) are subject to binding obligations of confidentiality; (b) process Customer Personal Data only on the Provider's instructions; and (c) have received appropriate training in data protection.

3.5 The Provider shall implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, or damage, as further described in Schedule 2 to this DPA.

3.6 The Provider shall, taking into account the nature of the processing, assist the Customer by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests from Data Subjects exercising their rights under Data Protection Law (including rights of access, rectification, erasure, restriction, portability, and objection).

3.7 The Provider shall assist the Customer in ensuring compliance with the Customer's obligations under Articles 32 to 36 of the UK GDPR (security of processing, notification of personal data breaches, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to the Provider.

4. PERSONAL DATA BREACH

4.1 The Provider shall notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

4.2 The notification shall include, to the extent reasonably available at the time of notification: (a) a description of the nature of the Personal Data Breach, including (where possible) the categories and approximate number of Data Subjects and Personal Data records concerned; (b) the name and contact details of the Provider's point of contact; (c) a description of the likely consequences of the Personal Data Breach; and (d) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

4.3 The Provider shall cooperate with the Customer and take all reasonable steps to assist the Customer in investigating, mitigating, and remediating the effects of the Personal Data Breach.

4.4 The Provider's notification of or response to a Personal Data Breach shall not be construed as an acknowledgement of any fault or liability on the part of the Provider.

5. SUB-PROCESSORS

5.1 The Customer provides general written authorisation for the Provider to engage Sub-processors to process Customer Personal Data, subject to the requirements of this clause 5.

5.2 The Provider shall maintain a list of current Sub-processors (the "Sub-processor List"), which is set out in Schedule 3 and shall be made available to the Customer on request or via the Provider's website.

5.3 The Provider shall give the Customer not less than 14 days' prior written notice before engaging any new Sub-processor or replacing an existing Sub-processor, specifying the identity of the proposed Sub-processor, the processing it will perform, and the location of processing.

5.4 If the Customer objects to a proposed Sub-processor on reasonable grounds relating to data protection, the Customer shall notify the Provider in writing within 14 days of receiving the notice. The parties shall discuss the Customer's concerns in good faith. If the parties are unable to resolve the objection within 30 days, the Customer may terminate the Agreement on written notice without penalty, and the Provider shall refund any prepaid fees for the unused portion of the Subscription Term.

5.5 The Provider shall impose on each Sub-processor, by way of a written contract, data protection obligations no less onerous than those set out in this DPA. The Provider shall remain fully liable to the Customer for the performance of each Sub-processor's obligations.

6. INTERNATIONAL DATA TRANSFERS

6.1 The Provider shall not transfer Customer Personal Data outside of an Approved Jurisdiction without: (a) the Customer's prior written consent; and (b) ensuring that appropriate safeguards are in place in accordance with Data Protection Law.

6.2 Where a transfer requires safeguards, the Provider shall rely on one of the following mechanisms: (a) the UK International Data Transfer Agreement (IDTA) issued by the ICO; (b) the International Data Transfer Addendum to the EU Standard Contractual Clauses; or (c) any other mechanism approved under Data Protection Law.

6.3 The Provider shall conduct and document a transfer risk assessment before making any international transfer, and shall make the results available to the Customer on request.

7. AUDIT AND COMPLIANCE

7.1 The Provider shall make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations set out in this DPA and in Article 28 of the UK GDPR.

7.2 The Provider shall allow for and contribute to audits, including inspections, conducted by the Customer or an independent auditor mandated by the Customer. Such audits shall: (a) be conducted no more than once per year, unless a Personal Data Breach or regulatory investigation necessitates an additional audit; (b) be conducted during normal business hours with not less than 30 days' prior written notice; (c) be at the Customer's sole expense; (d) be conducted in a manner that is minimally disruptive to the Provider's operations; and (e) be subject to reasonable confidentiality obligations.

7.3 Where permitted by Data Protection Law, the Provider may satisfy its audit obligations under clause 7.2 by making available to the Customer: (a) a summary of a relevant third-party audit report (such as SOC 2 Type II or ISO 27001 certification); or (b) responses to a reasonable data protection questionnaire provided by the Customer.

8. DATA RETENTION AND DELETION

8.1 Upon termination or expiry of the Agreement, the Provider shall: (a) at the Customer's election, return all Customer Personal Data to the Customer in a commonly used, machine-readable format, or delete all Customer Personal Data from the Provider's systems (including all copies and backups); and (b) provide written certification of deletion within 30 days of completing the deletion.

8.2 The Provider shall complete the deletion of Customer Personal Data within 60 days of the end of the data export period specified in the Agreement (currently 30 days post-termination), except to the extent that applicable law requires continued storage of any Customer Personal Data.

8.3 Where the Provider is required by applicable law to retain any Customer Personal Data after termination, the Provider shall: (a) inform the Customer of that requirement; (b) limit processing of such data to the purposes required by law; and (c) continue to protect such data in accordance with this DPA.

9. DATA PROTECTION IMPACT ASSESSMENTS

9.1 The Provider shall provide reasonable assistance to the Customer with any data protection impact assessment (DPIA) and any prior consultation with the ICO or other supervisory authority that the Customer is required to undertake under Data Protection Law, in each case to the extent that such assistance relates to the processing of Customer Personal Data by the Provider.

10. GENERAL

10.1 In the event of any conflict between this DPA and the Agreement, this DPA shall prevail in respect of the processing of Customer Personal Data.

10.2 This DPA shall be governed by and construed in accordance with the law of England and Wales.

10.3 The Provider shall maintain a record of all categories of processing activities carried out on behalf of the Customer, in accordance with Article 30(2) of the UK GDPR.

10.4 The parties shall review this DPA at least annually and update it as necessary to reflect changes in processing activities, Data Protection Law, or regulatory guidance.

SCHEDULE 1 — DETAILS OF PROCESSING

Subject matter of processing	The provision of the Clearpath cloud-hosted programme management platform, including hosting, storage, display, and processing of Customer Data as required to deliver the Service.
Duration of processing	The processing will continue for the duration of the Agreement, plus any post-termination data export and deletion period specified in the Agreement and this DPA.
Nature of processing	Collection, storage, organisation, structuring, retrieval, consultation, use, disclosure by transmission to Authorised Users, alignment, combination, restriction, erasure, and destruction of Customer Personal Data, each as necessary to provide the Service.
Purpose of processing	To provide the Customer with programme management, activity tracking, delay recording, site diary, document register, notification, and reporting functionality as described in the Agreement.
Categories of Data Subjects	Employees, agents, subcontractors, and representatives of the Customer and its Authorised Users; employees, agents, and representatives of the Customer's clients, main contractors, and project stakeholders whose contact details or names are entered into the Service by the Customer.
Types of Personal Data	Names, email addresses, job titles, login credentials (hashed passwords), IP addresses and browser metadata, organisational membership and project assignments, activity update and diary entry authorship, timestamps of user actions, photographs uploaded to site diaries or delay evidence, and any other Personal Data that the Customer or its Authorised Users choose to enter into free-text fields within the Service.
Special Categories of Personal Data	The Service is not designed to process Special Categories of Personal Data. The Customer shall not upload or enter Special Categories of Personal Data into the Service. If the Customer does so, it does so at its own risk and is solely responsible for ensuring a lawful basis for such processing.

SCHEDULE 2 — TECHNICAL AND ORGANISATIONAL MEASURES

The Provider implements and maintains the following measures to protect Customer Personal Data. These measures are subject to ongoing review and improvement in line with industry best practices and changes in the threat landscape.

Encryption

All data in transit between the Customer's browser and the Service is encrypted using TLS 1.2 or higher.

Customer Data at rest is encrypted using AES-256 encryption provided by the hosting infrastructure.

Database backups are encrypted using the hosting provider's native encryption capabilities.

User passwords are stored using industry-standard one-way cryptographic hashing (Werkzeug/PBKDF2) and are never stored or transmitted in plaintext.

Access Controls

Access to the Service is controlled by individual email/password authentication with enforced minimum password complexity requirements.

The Service implements role-based access control distinguishing between organisation administrators and standard members.

Project-level access controls restrict users to only the projects to which they have been assigned.

Administrative access to the hosting infrastructure is restricted to authorised Provider personnel using multi-factor authentication.

Login rate limiting and progressive account lockout are enforced to prevent brute-force attacks.

Infrastructure and Hosting

The Service is hosted on Railway (railway.app) with PostgreSQL database infrastructure located within the European Economic Area or the United Kingdom.

The hosting provider maintains ISO 27001 certification and SOC 2 Type II compliance.

Automated database backups are taken at least every seven (7) days and retained for a minimum of thirty (30) days.

The hosting environment provides automatic scaling, redundancy, and failover capabilities.

Application Security

Cross-Site Request Forgery (CSRF) protection is implemented on all form submissions.

Content Security Policy (CSP) headers are applied to mitigate cross-site scripting (XSS) attacks.

Input validation and parameterised queries are used throughout to prevent SQL injection.

File uploads are validated for type, size, and content before acceptance.

Security headers including X-Content-Type-Options, X-Frame-Options, and Referrer-Policy are applied to all responses.

Session cookies are configured with Secure, HttpOnly, and SameSite attributes.

Organisational Measures

All Provider personnel with access to Customer Personal Data are subject to binding obligations of confidentiality.

Access to production systems is granted on a least-privilege basis and reviewed periodically.

The Provider maintains an incident response procedure that includes identification, containment, investigation, notification, and remediation steps.

The Provider conducts periodic reviews of its security measures and updates them as necessary to address emerging threats.

Data Minimisation and Retention

The Service collects only the Personal Data necessary to provide the functionality described in the Agreement.

Customer Data is retained only for the duration of the Agreement, plus any post-termination export and deletion period.

Deleted organisations, projects, and user accounts are purged from the database in accordance with the retention schedule.

Server access logs containing IP addresses are retained for a maximum of 90 days for security monitoring purposes.

SCHEDULE 3 — APPROVED SUB-PROCESSORS

The following Sub-processors are authorised to process Customer Personal Data as at the date of this DPA. The Provider shall update this list and notify the Customer in accordance with clause 5.3.

Sub-processor	Location	Purpose	Data Processed
Railway Corp.	United States (EU adequacy / SCCs)	Cloud hosting infrastructure — application servers and PostgreSQL database	All Customer Data stored within the Service
Cloudflare, Inc. (Cloudflare R2)	European Union (UK adequacy)	Object storage for uploaded photographs, delay evidence, and project images (S3-compatible storage via Cloudflare R2)	Uploaded image files, PDF documents, and associated filenames
Twilio SendGrid	United States (EU adequacy / SCCs)	Transactional email delivery — account invitations, password resets, daily notifications, and overdue activity alerts	Recipient email addresses, user first names, project names, and activity names included in email content
Stripe Payments Europe Ltd.	Republic of Ireland (EU/UK adequacy)	Subscription billing & payment processing — processes subscription fees on behalf of the Provider	Billing contact name and email, billing address, organisation name, subscription tier, partial card data (last 4 digits and brand — full card numbers are tokenised by Stripe and never reach the Provider's systems)

Note on international transfers: Where a Sub-processor is located outside of an Approved Jurisdiction, the Provider relies on Standard Contractual Clauses (as supplemented by the UK International Data Transfer Addendum where applicable) or the relevant adequacy decision to provide appropriate safeguards for the transfer. The Provider has conducted transfer risk assessments for each Sub-processor and will make these available to the Customer on request.

END OF DATA PROCESSING ADDENDUM