

Data Processing Agreement

Version: 1.0 · Effective 18 July 2026 **Applies to:** the CodePulse engineering-analytics service ("the Service")

This Data Processing Agreement ("DPA") forms part of the agreement between the customer ("Customer", "Controller", "you") and **Keep Pushing Forward Ltd**, a company registered in England and Wales, trading as **CodePulse** ("CodePulse", "Processor", "we", "us"), governing the processing of Personal Data by CodePulse on the Customer's behalf in connection with the Service (together, the "Agreement").

Where there is any conflict between this DPA and the CodePulse Terms of Service, this DPA prevails in respect of the processing of Personal Data.

1. Definitions

Terms not defined here have the meaning given in the UK GDPR and the Data Protection Act 2018.

- **"UK GDPR"** and **"EU GDPR"** mean, respectively, the retained EU law version of the General Data Protection Regulation as it forms part of the law of England and Wales, and Regulation (EU) 2016/679, in each case together with any applicable national implementing laws.
- **"Data Protection Laws"** means all laws and regulations applicable to the processing of Personal Data under the Agreement, including the UK GDPR, the EU GDPR (where applicable) and the Data Protection Act 2018.
- **"Controller", "Processor", "Data Subject", "Personal Data", "Processing" and "Personal Data Breach"** have the meanings given in the UK GDPR.
- **"Sub-processor"** means any third party engaged by CodePulse to process Personal Data on the Customer's behalf in connection with the Service.
- **"Customer Personal Data"** means Personal Data that CodePulse processes on behalf of the Customer under the Agreement, as described in **Annex I**.

2. Roles and scope of processing

2.1 As between the parties, the Customer is the Controller and CodePulse is the Processor of Customer Personal Data.

2.2 CodePulse processes Customer Personal Data only to provide the Service and only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by law (in which case CodePulse will inform the Customer of that legal requirement before processing, unless the law prohibits it). The Agreement, this DPA and the Customer's configuration and use of the Service constitute the Customer's complete and final documented instructions.

2.3 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex I**.

2.4 The Customer is responsible for the accuracy of, and for having a lawful basis for, the Personal Data it makes available to the Service, including for informing its developers and other Data Subjects about the processing where required.

3. CodePulse obligations

CodePulse shall:

- **(a) Instructions.** Process Customer Personal Data only on the Customer's documented instructions, and inform the Customer if, in its opinion, an instruction infringes Data Protection Laws.
- **(b) Confidentiality.** Ensure that persons authorised to process Customer Personal Data are bound by an appropriate duty of confidentiality.
- **(c) Security.** Implement and maintain the technical and organisational measures set out in **Annex II**, taking into account the state of the art, costs, and the nature, scope, context and purposes of processing.
- **(d) Sub-processors.** Engage Sub-processors only in accordance with clause 4.
- **(e) Data Subject rights.** Taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as possible, to respond to requests to exercise Data Subject rights under Chapter III of the UK GDPR (see clause 6).
- **(f) Controller assistance.** Assist the Customer in ensuring compliance with its obligations under Articles 32 to 36 of the UK GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of processing and the information available to CodePulse.
- **(g) Deletion and return.** At the Customer's choice, delete or return Customer Personal Data on termination as set out in clause 8.
- **(h) Audits.** Make available to the Customer information necessary to demonstrate compliance with this DPA and allow for and contribute to audits as set out in clause 9.

4. Sub-processors

4.1 The Customer provides a general written authorisation for CodePulse to engage the Sub-processors listed in **Annex III** to process Customer Personal Data.

4.2 CodePulse imposes on each Sub-processor, by written contract, data protection obligations materially equivalent to those in this DPA, and remains liable to the Customer for a Sub-processor's performance of its data protection obligations.

4.3 CodePulse will give the Customer prior notice of the addition or replacement of a Sub-processor (by updating the published sub-processor list at the CodePulse [/dpa](#) page and, where the Customer has subscribed to notifications, by email), giving the Customer a reasonable opportunity (at least 30 days) to object on reasonable data protection grounds. If the Customer objects and the parties cannot resolve the objection, the Customer may terminate the affected part of the Service.

5. International transfers

5.1 CodePulse hosts and processes Customer Personal Data primarily within the United Kingdom and the European Economic Area (EEA). The current hosting region is set out in **Annex II**.

5.2 Where providing the Service involves a transfer of Customer Personal Data to a country outside the UK or the EEA that is not subject to an adequacy decision (for example, to a Sub-processor located in the United States as identified in **Annex III**), such transfer is made under an appropriate transfer mechanism, including the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, together with any supplementary measures required.

5.3 The parties agree to cooperate to put in place, and keep in place, a valid transfer mechanism for each such transfer for the duration of the Agreement.

6. Data Subject rights

6.1 The Service provides the Customer's administrators with functionality to access, correct and delete Customer Personal Data within their organisation's account.

6.2 Where CodePulse receives a request directly from a Data Subject in respect of Customer Personal Data, CodePulse will not respond to the request itself (except to confirm that the request has been forwarded) but will, without undue delay, forward the request to the Customer.

6.3 Taking into account the nature of the processing, CodePulse will assist the Customer, insofar as possible, in fulfilling the Customer's obligation to respond to Data Subject requests, including requests for access, rectification, erasure, restriction, portability and objection, by making available the functionality described in clause 6.1 and, where that functionality is insufficient, by providing reasonable assistance on the Customer's documented request.

7. Personal Data Breach

7.1 CodePulse will notify the Customer without undue delay, and in any event within 72 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

7.2 The notification will, to the extent known and taking into account the information available to CodePulse, describe the nature of the breach, the likely consequences, the measures taken or proposed to address it, and a point of contact. CodePulse will provide further information in phases as it becomes available.

7.3 CodePulse maintains error and availability monitoring to support the detection of incidents. The Customer remains responsible for assessing whether a breach must be notified to a supervisory authority or to Data Subjects and for making any such notification.

8. Deletion and return on termination

8.1 On termination or expiry of the Agreement, CodePulse will, at the Customer's choice, delete or return all Customer Personal Data, and delete existing copies, unless retention is required by law.

8.2 If the Customer does not request return within 30 days of termination, CodePulse will delete Customer Personal Data associated with the Customer's account. Deletion of an organisation account cascades to the associated repositories, pull requests, commits, reviews, comments, developer records and derived metrics, and triggers revocation of the external access tokens held for that account (for example the GitHub, and where connected Stripe and issue-tracker, tokens).

8.3 Backups and logs containing Customer Personal Data are retained only for the limited period described in **Annex II** and are then deleted or overwritten in the ordinary course.

8.4 During the term, the Service limits how far back each subscription tier can query historical data (the tier's data-history window). Data outside a tier's window remains stored but is not accessible through the Service until the Customer upgrades. The applicable window for each tier is stated in the Service's pricing terms.

9. Audit

9.1 CodePulse will make available to the Customer, on reasonable written request and no more than once per 12-month period (unless required by a supervisory authority or following a Personal Data Breach), the information reasonably necessary to demonstrate compliance with this DPA, including relevant policies, its current sub-processor list, and summaries of any third-party security assessments.

9.2 Any audit will be conducted on reasonable notice, during business hours, subject to confidentiality, and in a manner that does not disrupt the Service or compromise the security of other customers.

10. Liability and general

10.1 Each party's liability arising out of or related to this DPA is subject to the limitations and exclusions of liability set out in the Agreement.

10.2 This DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction, in each case as set out in the Agreement.

10.3 If any provision of this DPA is held to be unenforceable, the remaining provisions continue in full force and effect.

Annex I — Details of processing

Subject matter. Provision of the CodePulse engineering-analytics Service to the Customer.

Duration. For the term of the Agreement, plus the deletion period described in clause 8.

Nature and purpose. Collection, storage, organisation, analysis and display of software-delivery activity data drawn from the Customer's connected source-control and issue-tracking accounts, in order to produce engineering metrics, dashboards and reports for the Customer's internal use.

Categories of Data Subjects.

- The Customer's developers and other contributors whose activity appears in the connected repositories and issue trackers (the primary population).

- The Customer's account users and administrators who authenticate to the Service.

Categories of Personal Data.

- **Account/identity data:** name, username/login, email address, avatar URL, authentication and session records, and sign-up context (for account users).
- **Contributor identity data:** developer name, source-control login, email address and avatar, and publicly available repository activity associated with a login.
- **Software-delivery activity data:** pull request, commit, review and comment records and their timing, authorship and status.
- **User-authored text:** pull request titles and descriptions, commit messages, code-review summaries and code-review/discussion comments. Code-review comments may include short fragments of source code quoted inline within the comment. The Service does not clone or store the Customer's full source-code tree by default.
- **Technical data:** IP address and user-agent recorded in security, audit and email-delivery logs.
- **Billing data (account users):** billing identifiers associated with the Customer's subscription.

Sensitive/special-category data. The Service is not intended to process special categories of Personal Data. The Customer should not use free-text fields in its source-control tooling to submit special-category data.

Frequency of processing. Continuous / on an ongoing automated basis for the term.

Annex II — Technical and organisational measures (TOMs)

CodePulse maintains the following measures. These describe the Service as currently operated; they are reviewed and updated as the Service evolves.

- **Encryption in transit.** Connections to the Service are encrypted using TLS, with HTTP redirected to HTTPS.
- **Encryption of secrets at rest.** External access tokens and secrets (for example connected source-control, billing and notification credentials) are encrypted at the application layer using authenticated symmetric encryption (AES). Account passwords, where used, are hashed with bcrypt.
- **Hosting.** Compute and database services are hosted on Amazon Web Services in the EU (Ireland, `eu-west-1`) region.
- **Tenant isolation.** The Service is multi-tenant. Data is partitioned per organisation, and access is enforced at the application layer by authenticated membership and role checks; every data query is scoped to the requesting organisation.
- **Access control.** Role-based access control governs what account users can do within their organisation. Administrative access to production systems is limited to authorised personnel.
- **Integrity of inbound data.** Inbound webhooks are verified using signature/HMAC validation before processing.
- **Monitoring and logging.** The Service maintains application error monitoring (with secret-bearing values redacted from error reports before they are sent) and audit logging of administrative actions (including the acting user, action, timestamp, and source IP/user-agent).

- **Backups.** Operational backups are maintained for resilience and are subject to the retention and deletion practices described in clause 8.

Annex III — Sub-processors

The following Sub-processors may process Customer Personal Data in connection with the Service. Only Sub-processors that process **Customer** Personal Data are listed; CodePulse's own business-operations vendors (for example marketing and sales tooling) are addressed in the CodePulse privacy notice, not here. Connected source-control and issue-tracking providers (for example GitHub, Azure DevOps, Linear, Jira) are the Customer's own systems that supply data to the Service and are not CodePulse Sub-processors.

Sub-processor	Purpose	Data categories	Location
Amazon Web Services (AWS)	Cloud hosting, compute and database	All Customer Personal Data at rest	EU — Ireland (eu - west - 1)
Stripe	Subscription billing and payments	Account/billing identifiers and contact email	Per the Stripe DPA and its transfer safeguards
Resend	Transactional and service email delivery	Account/administrator email addresses and email content	Per the Resend DPA and its transfer safeguards
PostHog	Product-usage analytics	Product-usage events with account/organisation identifiers	United States †
Self-hosted error monitoring (Sentry)	Application error and performance monitoring	Diagnostic telemetry, which may include account/organisation identifiers	Operator-controlled †
OpenRouter (routing to an AI model provider)	Automated classification of work type	Pull request titles and file paths only	Operator-confirmed region †

† Where a Sub-processor processes Customer Personal Data outside the UK or the EEA, the transfer is made under an appropriate safeguard — the Sub-processor's own data processing agreement together with the applicable Standard Contractual Clauses / UK Addendum, or another lawful transfer mechanism.

Acceptance

This DPA is entered into by the Customer and Keep Pushing Forward Ltd (trading as CodePulse) and is incorporated into the Agreement.

Keep Pushing Forward Ltd, trading as CodePulse. Registered in England and Wales. Data protection contact: legal@codepulsehq.com · Security contact: security@codepulsehq.com