

Data Processing Agreement

Version: 1.1 · Effective 10 September 2026 (supersedes version 1.0 of 18 July 2026; see "Updates in version 1.1" at the end)

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 (company number 15087012), 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 Service runs on Oracle Cloud Infrastructure in the United Kingdom (London), and encrypted database backups are stored in the EEA (see **Annex II**). Certain Sub-processors identified in **Annex III** process limited categories of Customer Personal Data in the United States.

5.2 Transfers of Customer Personal Data from the EEA to the United Kingdom rely on the European Commission's adequacy decision for the United Kingdom or, should that decision cease to apply, on the EU Standard Contractual Clauses. Each transfer of Customer Personal Data to a country outside the UK or the EEA that is not subject to an adequacy decision is made under an appropriate transfer mechanism: the EU Standard Contractual Clauses (and, for UK data, the UK International Data Transfer Addendum) incorporated in the relevant Sub-processor's data processing terms, or the EU-US Data Privacy Framework and its UK Extension where the recipient is certified under it, 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 48 hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data, including a Personal Data Breach at a Sub-processor.

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, deletes the external access tokens held for that account, and revokes them with the provider where the provider supports revocation (for example Linear, and Stripe subscriptions are cancelled). Access through the CodePulse GitHub App ends when the Customer removes the App installation from its GitHub organisation settings, which the Customer may do at any time.

8.3 Encrypted backups containing Customer Personal Data are retained for up to 8 days, as described in **Annex II**, and are then deleted automatically. Operational logs are retained only as long as needed to operate and secure the Service.

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, reports and email communications (such as digests, alerts and personalised summaries of the Customer's own metrics) for the Customer's internal use. Communications built from Customer Personal Data are sent only to the Customer's own account users.

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.
- Members of the Customer's connected source-control organisations, whose membership is read for access control and team configuration.

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, and the short diff context GitHub attaches to an inline review comment is stored with that comment. The Service does not clone the Customer's repositories or retrieve their file contents.
- **Product-usage data (account users):** interactions with the Service interface, recorded as usage events that carry no on-screen text and as session replays in which on-screen text and form inputs are masked (see PostHog in **Annex III**), and error diagnostics.
- **Survey responses:** answers to developer surveys, where the Customer runs them in the Service.
- **AI-tool usage data:** per-developer usage and spend reported by AI coding tools the Customer connects.
- **Derived metrics:** team and per-developer metrics the Service calculates from the data above, including review-quality and comment-sentiment scores.
- **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 and HTTP Strict Transport Security (HSTS) enabled.
- **Encryption at rest.** The production database and its storage volumes are encrypted at rest by Oracle Cloud Infrastructure.
- **Encryption of secrets at rest.** Access tokens and secrets for connected services (source-control, issue-tracker, AI-tool and notification credentials) are encrypted at the application layer using authenticated symmetric encryption (Fernet: AES with HMAC-SHA256) before they are written to the database.
- **Authentication.** The Service holds no passwords of its own. Users sign in through GitHub or Azure DevOps, so the Customer's multi-factor authentication and identity policies on those accounts apply.
- **Key management.** The GitHub App private key, the application encryption key and the backup encryption key are held by CodePulse's Security Lead. Apart from the production systems that use them, no other person or system has access to them.
- **Administrative access.** Multi-factor authentication is enforced on CodePulse's hosting (Oracle Cloud), source-control, backup-storage and email accounts.
- **Hosting.** Compute and database services are hosted on Oracle Cloud Infrastructure in the United Kingdom (London region). The database is reachable only on a private network within the hosting environment.
- **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 before processing: by HMAC signature where the provider signs its webhooks (GitHub, Stripe), and by a per-connection secret where it does not (Azure DevOps).
- **Change management.** Production changes are made through peer-reviewed pull requests with automated tests, and dependencies are scanned for known vulnerabilities in continuous integration.
- **Security testing.** The Service is tested periodically with automated penetration-testing and vulnerability-scanning tools, most recently in June 2026. CodePulse has not yet commissioned an independent third-party penetration test.
- **Monitoring and logging.** The Service maintains application error monitoring. Secret-bearing values are redacted from server-side error reports before they are sent, and error-session replays mask all on-screen text and media. Session replays used for product analytics likewise mask all on-screen text and form inputs. Privileged administrative actions by CodePulse personnel are recorded in an audit log (acting user, action, timestamp, and source IP/user-agent).

- **Backups.** The database is backed up every 6 hours. Backups are encrypted before they leave the hosting environment, stored with Backblaze in the EEA (see **Annex III**), retained for up to 8 days and then deleted automatically. Restoration is tested weekly by an automated restore drill.

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 that never receive Customer Personal Data (for example sales prospecting tools) are addressed in the CodePulse privacy notice, not here. Systems the Customer connects with its own credentials are the Customer's own systems that supply data to the Service and are not CodePulse Sub-processors: the Customer's source-control and issue-tracking providers (for example GitHub, Azure DevOps, Linear, Jira) and the AI-tool providers whose usage reports the Customer connects (for example Anthropic, OpenAI, Cursor, GitHub Copilot). An organisation admin can switch the Service's AI features off. While they are off, CodePulse sends none of that organisation's data to AI providers for processing; AI-tool usage reports that the Customer has connected with its own credentials continue to be retrieved.

Sub-processor	Purpose	Data categories	Location
Oracle (Oracle Cloud Infrastructure)	Cloud hosting, compute and database	All Customer Personal Data	United Kingdom (London)
Backblaze (B2 Cloud Storage)	Encrypted database backups, retained up to 8 days	All Customer Personal Data, encrypted before upload	EEA (Netherlands)
Anthropic	AI features within the Service: pull-request summaries, matching AI-tool accounts to developers, optional review-quality analysis, and drafting support replies and personalised summary emails for the Customer's own account users	Pull request titles, descriptions and file paths; developer names, logins and email addresses; review comments with their attached diff context (only where review-quality analysis is enabled); support messages; summary metrics about the Customer's organisation, used only to write communications to that Customer	United States †
OpenAI	Matching support messages to help-centre articles (text embeddings)	Text of support messages sent by account users	United States †
Stripe	Subscription billing and payments	Billing identifiers, organisation name and contact email	United States †
Resend	Transactional and service email delivery	Account user email addresses and email content, which can include digest content such as pull request titles and developer logins	United States †

Sub-processor	Purpose	Data categories	Location
PostHog	Product-usage analytics and session replay	Usage events (pages viewed and elements clicked, without on-screen text) linked to the account user's name, email, login and organisation; session replays of the Service interface with all on-screen text and form inputs masked	United States †
Self-hosted error monitoring (Sentry)	Application error and performance monitoring, operated by CodePulse	Diagnostic telemetry; account user ID, email and login; organisation identifiers; error-session replays with all on-screen text and media masked	United Kingdom (CodePulse-operated server)
Google (Analytics and Ads)	Product analytics and advertising conversion measurement	Account user ID, organisation identifiers and pages viewed; a hashed account user email for conversion measurement	United States †
LinkedIn (Insight Tag)	Advertising conversion measurement	Cookie identifiers, IP address and pages viewed	United States †
Slack (CodePulse's internal workspace)	Internal notifications to CodePulse staff, including staff review of personalised summary emails before they are sent to the Customer	Account user names and email addresses, organisation names, support and feedback messages, and drafts of summary emails addressed to the Customer's account users	United States †

† Where a Sub-processor processes Customer Personal Data outside the UK or the EEA, the transfer is made under an appropriate safeguard as described in clause 5.2.

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, company number 15087012. Data protection contact: privacy@codepulsehq.com · Legal: legal@codepulsehq.com · Security contact: security@codepulsehq.com

Updates in version 1.1

Version 1.1 (10 September 2026) updates version 1.0 as follows:

- Hosting: version 1.0 named Amazon Web Services (Ireland) as the hosting provider. The Service has been hosted on Oracle Cloud Infrastructure in the United Kingdom (London) since early 2026, with encrypted backups stored in the EEA. Clause 5 and Annex II are updated accordingly.
- Clause 7 shortens breach notification to within 48 hours and covers breaches at Sub-processors.

- Annex III sets out the current Sub-processors, the data each receives and its location, and the organisation-level switch that turns AI features off.
- Clause 8 and Annex II state the backup retention period (up to 8 days) and how access through the CodePulse GitHub App ends.
- Annex I describes product-usage data, survey responses, AI-tool usage data, derived metrics and the summary emails the Service sends to the Customer's own account users.
- Annex I adds the members of connected source-control organisations as a category of Data Subject.
- Annex II adds HTTP Strict Transport Security, encryption at rest, authentication, key management, administrative access, change management, vulnerability scanning, security testing and restore testing.