Data Processing Agreement

Last updated: 12 May 2026 — version 1.0

This Data Processing Agreement ("**DPA**") forms part of the Terms of Service between Eclipt UG (haftungsbeschränkt) ("**Processor**", "we", "CostCanary") and the customer that has subscribed to the CostCanary service ("**Controller**", "you", "Customer"). It is automatically incorporated into the Terms of Service for every paying customer and applies to all processing of personal data that we carry out on the Customer's behalf in providing the Service.

By accepting the Terms of Service, the Customer enters into this DPA on its own behalf and, where applicable, on behalf of the Slack workspaces, AWS accounts, and affiliates for which the Customer is responsible.

If you require this DPA on a signed paper version, or with modifications, contact info@costcanary.com.

1. Definitions

Terms not defined here have the meaning given to them in the General Data Protection Regulation (Regulation (EU) 2016/679, "**GDPR**"). In addition:

- "**Customer Personal Data**" means personal data that we process on the Customer's behalf in providing the Service, including Slack workspace-member data, AWS account metadata, and report content.
- "**Sub-processor**" means any third party that we engage to process Customer Personal Data on the Customer's behalf.
- "**Service**" has the meaning given in the Terms of Service.

2. Subject Matter, Duration, Nature, and Purpose

Subject matter and duration: the processing is carried out for the duration of the Customer's subscription to the Service, plus the retention periods set out in the Privacy Policy.

Nature and purpose: automated processing in connection with the operation of a cost-monitoring SaaS — authenticating users, reading AWS cost data via assumed IAM role, generating reports, delivering reports to Slack channels and other destinations the Customer configures, and administering subscriptions.

Type of personal data processed:

- Slack identifiers and profile data (user ID, team ID, display name, real name, email, locale, time zone, account-status flags) for the installing user, administrators, and every member of the connected workspace.
- AWS account identifiers, account names, IAM role ARNs, and cost-and-usage data retrieved from AWS Cost Explorer and AWS Organizations APIs. Cost data may incidentally contain resource names that include personal identifiers chosen by the Customer.
- Server logs containing IP address, user agent, request path, response code, and trace identifiers for requests originating from the Customer.

Categories of data subjects:

- the Customer's personnel and contractors who interact with the Service (users, administrators, billing contacts);
- members of the Customer's connected Slack workspaces, whether or not they personally interact with CostCanary;
- AWS account owners and authorized users named in IAM role configurations or resource tags.

3. Roles of the Parties

The Customer is the controller of the Customer Personal Data. CostCanary is the processor. Each Party will comply with its obligations under applicable data-protection law.

Where the Customer's own data-subject contracts (e.g. with its employees or end users) require additional terms beyond those in this DPA, the Customer is responsible for putting those terms in place; we will reasonably cooperate.

4. Customer Instructions

We process Customer Personal Data only on documented instructions from the Customer. The Customer's instructions for the processing of Customer Personal Data are:

- the Terms of Service, this DPA, and the Privacy Policy;
- the in-product configuration choices that the Customer makes (e.g. which AWS accounts to connect, which Slack channels to post to, which users to assign administrator roles);
- any subsequent written instructions agreed between the Parties.

If we believe an instruction infringes data-protection law, we will notify the Customer without undue delay (Art. 28(3) sentence 3 GDPR).

5. Confidentiality

We ensure that persons authorized to process Customer Personal Data are bound by appropriate contractual or statutory confidentiality obligations and have received data-protection training proportionate to their role.

6. Security of Processing

We implement and maintain appropriate technical and organizational measures ("**TOMs**") to ensure a level of security appropriate to the risk, in accordance with Art. 32 GDPR. The current set of TOMs is described in the Annex to this DPA. We may update the TOMs from time to time provided that the overall level of security does not materially decrease.

7. Sub-processors

General authorization. The Customer grants CostCanary a general authorization, under Art. 28(2) GDPR, to engage Sub-processors for the provision of the Service.

Current Sub-processors. As of the "Last updated" date of this DPA, the following Sub-processors are engaged:

Sub-processor	Location	Purpose
Amazon Web Services EMEA SARL	Frankfurt, Germany (eu-central-1)	Hosting infrastructure, compute, database, object storage, queues
Slack Technologies, LLC (a Salesforce, Inc. company)	United States	Required platform integration — authentication and report delivery to Customer's workspace
Stripe Payments Europe Ltd. / Stripe, Inc.	Ireland / United States	Subscription billing and payment processing
Cloudflare, Inc.	United States	CDN, DNS, and DDoS protection for the public website

Changes. We will notify the Customer at least 30 days in advance of adding or replacing a Sub-processor by updating this list and, where the Customer has provided a notification address, by email or in-product notice. Within 30 days of notification, the Customer may object to the change on reasonable data-protection grounds. If the objection cannot be resolved between the Parties, the Customer may terminate the affected portion of the Service with effect at the end of the then-current billing period; pre-paid fees for the remaining term will be refunded on a pro-rata basis.

Processor terms with Sub-processors. We impose on each Sub-processor data-protection obligations no less protective than those in this DPA, including the obligations of Art. 28(3) GDPR. We remain fully liable to the Customer for the performance of each Sub-processor's obligations.

8. Data Subject Requests

Taking into account the nature of the processing, we assist the Customer through appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Customer's obligations to respond to requests from data subjects to exercise their rights under Chapter III of the GDPR.

If we receive a request from a data subject that relates to Customer Personal Data, we will not respond directly except to confirm that the request should be addressed to the Customer, and will forward the request to the Customer without undue delay. For requests by members of a Customer's Slack workspace whose data we hold for access-management purposes (see Privacy Policy Section 2.a.1), we may respond directly insofar as the request concerns processing for which CostCanary itself relies on Art. 6(1)(f) GDPR.

9. Personal Data Breach

We notify the Customer without undue delay, and in any event within 48 hours, of becoming aware of a personal data breach affecting Customer Personal Data. The notification will include, to the extent then known, the information required by Art. 33(3) GDPR and a contact point for further inquiries. We will reasonably cooperate with the Customer's own breach-notification obligations under Art. 33 and Art. 34 GDPR.

10. Data Protection Impact Assessments

Where required under Art. 35 or Art. 36 GDPR, we provide the Customer, on request, with reasonable cooperation and information necessary for the Customer to carry out a data protection impact assessment or prior consultation relating to the Service.

11. Return or Deletion at the End of Processing

On termination of the Customer's subscription, we delete Customer Personal Data in accordance with the retention periods set out in the Privacy Policy, except where longer storage is required by Union or Member State law (in particular for billing records under §§ 147 AO and 257 HGB). The Customer may, before deletion, export Customer Personal Data using the Service's in-product export features or, where those features are insufficient, by written request to info@costcanary.com.

12. Audit Rights

The Customer has the right to verify our compliance with this DPA in accordance with Art. 28(3)(h) GDPR. We satisfy this right primarily by making available to the Customer, on request and subject to confidentiality obligations:

- the current TOMs description (Annex);
- relevant third-party certifications, audit reports, or SOC-type reports of our Sub-processors that we have obtained (e.g. AWS SOC 2);
- written responses to reasonable due-diligence questionnaires.

If the foregoing is insufficient to demonstrate compliance for a specific concern, the Customer may, with at least 30 days' written notice, no more than once per calendar year (and additionally following a personal data breach or upon documented regulator request), carry out or commission an audit. The audit will be conducted during regular business hours, will not unreasonably interfere with our operations, and the auditor must enter into appropriate confidentiality obligations. The Customer bears its own audit costs and reimburses our reasonable costs of cooperating, unless the audit reveals material non-compliance.

13. International Data Transfers

To the extent processing under this DPA involves transfer of Customer Personal Data outside the European Economic Area to a country without an adequacy decision under Art. 45 GDPR, the Parties:

- rely on the EU–U.S. Data Privacy Framework where the recipient is certified; and otherwise
- incorporate by reference the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module 2 (controller-to-processor) between the Customer (as data exporter) and CostCanary (as data importer), and Module 3 (processor-to-processor) between CostCanary and onward Sub-processors;
- with the following selections: Clause 7 (docking) included; Clause 9 option 2 (general authorization, 30 days' notice as per Section 7); Clause 11(a) optional independent dispute-resolution language excluded; Clause 17 (governing law) — the law of the Federal Republic of Germany; Clause 18 (forum and jurisdiction) — courts of Berlin, Germany; Annex I, II, and III are populated by reference to this DPA and the Privacy Policy.

In addition, we apply supplementary measures consistent with EDPB Recommendations 01/2020, including encryption in transit and at rest, role-scoped access, and resistance to unauthorized disclosure requests from public authorities to the extent legally possible.

14. Liability

The liability provisions of the Terms of Service apply to this DPA. Nothing in this DPA limits or excludes either Party's liability towards data subjects under Art. 82 GDPR.

15. Term and Termination

This DPA enters into force when the Customer accepts the Terms of Service and remains in effect for as long as we process Customer Personal Data on the Customer's behalf. Sections that by

their nature should survive termination (in particular Sections 5, 11, 12, 14, and 16) survive.

16. Order of Precedence

In the event of a conflict between this DPA and the Terms of Service in matters concerning the processing of personal data, this DPA prevails. In the event of a conflict between this DPA and the Standard Contractual Clauses incorporated by reference in Section 13, the Standard Contractual Clauses prevail.

17. Governing Law

This DPA is governed by the laws of the Federal Republic of Germany, without prejudice to mandatory data-protection law applicable to the Customer or the data subjects.

Annex — Technical and Organizational Measures (Art. 32 GDPR)

The following measures describe CostCanary's TOMs as of the "Last updated" date of this DPA. We may improve or modify these measures over time; the overall level of security will not be materially reduced.

1. Pseudonymization and encryption (Art. 32(1)(a)).

- TLS 1.2+ for all data in transit between Customer browsers/APIs and our infrastructure, and between our infrastructure and Sub-processors.
- Encryption at rest for all persistent storage — DynamoDB, S3, EBS, and database backups — using AWS KMS-managed keys.
- Cognito user-pool secrets and OAuth tokens are encrypted at rest with KMS.

2. Confidentiality (Art. 32(1)(b)).

- Access to production systems is restricted to a minimum set of personnel and granted on a least-privilege basis.
- Production access requires SSO with multi-factor authentication.
- Workstation security: full-disk encryption, automatic screen lock, current operating-system updates.
- Office and remote-work environments have no on-premises Customer Personal Data.

3. Integrity (Art. 32(1)(b)).

- Infrastructure is defined and provisioned through code (OpenTofu + Terragrunt) under version control with peer review.
- Application changes go through code review and automated test pipelines before deployment.
- AWS CloudTrail and application logs record administrative actions; logs are write-once for audit purposes within their retention window.

4. Availability and resilience (Art. 32(1)(b)).

- Serverless and managed AWS services (Lambda, DynamoDB, S3) used to inherit AWS availability characteristics in eu-central-1.
- Automated backups for stateful services; point-in-time recovery enabled on production databases.
- Health checks and alerting on core service paths.

5. Restoration (Art. 32(1)(c)).

- Backups tested through periodic restoration exercises.
- Documented runbooks for service recovery.

6. Process for regular testing, assessment, and evaluation (Art. 32(1)(d)).

- Dependency-vulnerability scanning on each build.
- Periodic security review of changes that touch authentication, authorization, billing, or external integrations.
- Incident-response playbook reviewed at least annually.

7. Sub-processor management.

- Sub-processors are selected based on their data-protection commitments and security certifications.
- AWS is engaged under the AWS GDPR Data Processing Addendum.
- Stripe is engaged under Stripe's Data Processing Agreement.
- Slack is engaged under Salesforce's Data Processing Agreement.
- Cloudflare is engaged under Cloudflare's Data Processing Addendum.

8. Pseudonymous customer-facing logging.

- Application logs do not include Slack OAuth tokens, AWS access credentials, or full cost-data payloads. Identifiers in logs (user IDs, organization IDs, request IDs) are sufficient to debug a request without exposing personal data in the clear.

The Customer may request a current copy of this Annex by emailing info@costcanary.com.