Data Processing Agreement

Effective as of 1 November 2026

Spend Brake Data Processing Agreement. The current version is published at https://spendbrake.dev/dpa.

In short

- When your organization sends personal data through the hosted Spend Brake service, your organization is the controller and I, Kristiyan Ivanov, am its processor. This agreement sets out the terms Article 28 GDPR requires for that.
- It forms part of the Terms of Service and applies automatically when you use the Hosted Service. No signature is needed; if your records need a countersigned copy, email me and I will return one.
- Request and response bodies and query strings pass through the proxy and are never stored. What is stored is metadata about each call, your team and your configuration, in DigitalOcean's Frankfurt region, with the security measures in Annex II.
- Sub-processors are listed in Annex III. I will tell you 30 days before adding one, and you may object.
- I will tell you about a personal data breach affecting your data without undue delay and in any case within 48 hours of becoming aware of it.
- A self-hosted install is not covered: I process nothing for you there.

This Data Processing Agreement (the “DPA”) is between the organization that holds an account on the hosted Spend Brake service (“you” or the “Customer”) and Kristiyan Ivanov, a self-employed individual registered in Bulgaria (BULSTAT 180490275), of zh.k. Hadzhi Dimitar 16, entrance B, floor 1, apt. 13, Poduyane district, 1510 Sofia, Bulgaria (“I,” “me” or the “Processor”). It supplements the Terms of Service (the “Terms”) and governs the processing of personal data that you, your applications, agents and team members send to or through the Hosted Service. Capitalized terms not defined here have the meaning given in the Terms.

How this DPA is concluded. This DPA forms part of the Terms. It applies automatically, without signature, from the moment you create an org on the Hosted Service or first send a request through it, whichever is earlier, and it binds the organization you named when registering. If your organization needs a signed copy for its records, email kristiyan@spendbrake.dev with your organization's legal name and address, and I will

return a countersigned copy of the current version. A signed copy does not change its terms.

1. Definitions
2. Scope and roles
3. Details of the processing
4. My obligations as processor
5. Sub-processors
6. International transfers
7. Assistance
8. Personal data breaches
9. Deletion and return
10. Audits and information
11. Your obligations
12. Liability
13. Term, precedence and governing law
Annex I: Details of processing
Annex II: Technical and organisational measures
Annex III: Sub-processors

1. Definitions

- **“Data Protection Law”** means Regulation (EU) 2016/679 (the “GDPR”), the GDPR as it forms part of the law of the United Kingdom (the “UK GDPR”) and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection, and any national law implementing or supplementing them, in each case as they apply to the processing under this DPA.
- **“Customer Data”** means personal data that you, your applications, agents or team members send to or through the Hosted Service, as described in Annex I. It includes the contents of proxied requests while they pass through the proxy, the usage events and server logs the Hosted Service records about them, and the team-member, alert-recipient and configuration data you enter.
- **“Hosted Service”** has the meaning given in the Terms: the hosted Spend Brake service at app.spendbrake.dev, including its proxy endpoints, dashboard, admin API and the `brake` command-line tool when it talks to it.
- **“Sub-processor”** means a third party I engage to process Customer Data on my behalf.
- **“Personal data,” “controller,” “processor,” “data subject,” “processing,” “personal data breach”** and **“supervisory authority”** have the meaning given in the GDPR.

2. Scope and roles

2.1 You are the controller, I am the processor

For Customer Data, you are the controller (or a processor acting for your own customers, in which case you warrant that your instructions to me are covered by their instructions to

you) and I am your processor. I process Customer Data only to provide the Hosted Service to you under the Terms and this DPA.

2.2 What this DPA does not cover

- **Data for which I am the controller.** The email address and name you use to open an account, billing data, support correspondence, and analytics about the use of the website and dashboard are processed by me as controller, as described in the Privacy Policy. Where the same piece of data serves both purposes (for example a team member's email address, which I need to sign them in and which you entered to give them access to your org), this DPA governs my processing of it on your instructions and the Privacy Policy governs my own.
- **API providers.** Every request through the proxy is forwarded to the provider you addressed (for example Google Maps Platform or Twilio) with your own provider key, exactly as your application sent it. The provider processes it under your agreement with them. It is not my Sub-processor, and I do not control what it does with the request.
- **Destinations you configure.** Alerts, webhooks, emails and OpenTelemetry spans go to the Slack, Discord, Microsoft Teams, webhook, email or OTLP endpoints you set up. Sending them is your instruction; the recipients are your processors or third parties, not mine.
- **Self-hosted installs.** If you run the Spend Brake software on your own infrastructure, I do not process any data for you and this DPA does not apply. A Business or Enterprise License is verified offline and sends nothing to me.

3. Details of the processing

The subject matter, duration, nature and purpose of the processing, the categories of data subjects and the categories of personal data are set out in Annex I. In outline: your applications and agents send API requests to the proxy; the proxy prices each request, checks it against your caps, forwards it to the provider with your key, streams the response back and records metadata about the call. Request and response bodies and query strings are handled in memory only and are never stored.

4. My obligations as processor

4.1 Instructions

I will process Customer Data only on your documented instructions, including with regard to transfers to a third country, unless EU or Member State law to which I am subject

requires otherwise; in that case I will tell you about the legal requirement before processing, unless that law prohibits it on important grounds of public interest. Your documented instructions are: the Terms; this DPA; the settings you make in the dashboard, the admin API and the command-line tool (keys, caps, labels, alert and telemetry destinations, team members, plan and therefore retention); the requests your applications and agents send; and any further written instruction you email me and I agree to. If I believe an instruction infringes Data Protection Law, I will tell you without delay and may pause the processing it concerns until it is resolved.

4.2 Confidentiality

I run the Hosted Service myself. No employee or contractor of mine has access to Customer Data. If I ever give anyone access, they will first be bound by a written confidentiality obligation at least as protective as this DPA, and where they act as a Sub-processor they will be added to Annex III under Section 5.

4.3 Security

I will implement and maintain the technical and organisational measures in Annex II, and at least those required by Article 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing and the risks to data subjects. I may update Annex II as the software changes, provided the overall level of protection does not fall. The current measures are also described on the security page, and the code that implements them is public.

4.4 Records and cooperation

I keep the record of processing activities that Article 30(2) GDPR requires of a processor and will cooperate, on request, with the supervisory authority competent for you in the performance of its tasks.

4.5 Only what is needed

I will not use Customer Data for any purpose other than providing the Hosted Service to you: not to train models, not to build profiles, not for advertising, and not for marketing to third parties. I may inspect metadata to operate the Hosted Service, enforce the Terms and protect the providers behind the proxy, as Section 4.3 of the Terms says.

5. Sub-processors

5.1 General authorisation

You give me general written authorisation to engage the Sub-processors listed in Annex III, and to replace or add Sub-processors under Section 5.2. Annex III states what each Sub-processor does and what it sees; it matches the service providers listed in the Privacy Policy.

5.2 Changes and objections

Before I add or replace a Sub-processor that will process Customer Data, I will email the owners of your org at least 30 days in advance and update Annex III. You may object within those 30 days on reasonable, documented data protection grounds. If you do, we will discuss the concern in good faith; if I cannot address it within a further 30 days (for example by not using the Sub-processor for your org), either of us may terminate the affected org's use of the Hosted Service on written notice, and I will refund any prepaid fees for the period after termination. Continued use of the Hosted Service after the 30-day notice period without an objection is acceptance of the change.

5.3 Flow-down and responsibility

I engage each Sub-processor under a written contract that imposes data protection obligations at least as protective, in substance, as those in this DPA, in particular regarding security. Where a Sub-processor fails to fulfil its data protection obligations, I remain fully liable to you for its performance, as Article 28(4) GDPR provides.

6. International transfers

I am based in Bulgaria, and the Hosted Service, its database and its cache run in DigitalOcean's Frankfurt, Germany (FRA1) region. Product analytics are stored in PostHog's EU Cloud, also in Frankfurt. Stripe, Resend, Vercel and PostHog are United States companies and may process data in the United States and elsewhere.

I will not transfer Customer Data outside the European Economic Area, the United Kingdom or Switzerland, or allow a Sub-processor to, except as described in Annex III and in compliance with Chapter V GDPR (and the equivalent provisions of the UK GDPR and Swiss law where they apply). For each Sub-processor that processes Customer Data in a country without an adequacy decision, I rely on an appropriate safeguard offered by that Sub-processor: the EU Standard Contractual Clauses adopted by the European Commission (Decision (EU) 2021/914), Module 3 (processor to processor), with the UK International Data Transfer Addendum and the Swiss adaptations where they apply, or,

where the Sub-processor is certified under the EU-US Data Privacy Framework and its UK and Swiss extensions, that certification. I check which applies when I engage a Sub-processor and when its terms change; copies of or links to the relevant clauses or certification are available on request. If a safeguard I rely on is invalidated, I will work with you in good faith to put an alternative in place or stop the transfer.

If you instruct me to send Customer Data to a destination outside those territories (for example a webhook endpoint, an OpenTelemetry collector, or an API provider in the United States), that transfer is made on your instruction and you are responsible for its lawfulness.

7. Assistance

7.1 Data subject requests

Taking into account the nature of the processing, I will assist you with appropriate technical and organisational measures, insofar as this is possible, in responding to requests from data subjects exercising their rights under Chapter III GDPR (access, rectification, erasure, restriction, portability, objection). Much of this you can do yourself: the dashboard and the admin API let you see and delete keys, credentials, labels and team members, and export usage events and the audit log as CSV. For anything the tools do not cover, email me and I will help within a reasonable time, normally within 10 business days. If a data subject contacts me directly about Customer Data, I will not respond beyond acknowledging the request and pointing them to you, unless the law requires me to, and I will forward the request to you without undue delay.

7.2 Security, breaches, impact assessments and prior consultation

Taking into account the nature of the processing and the information available to me, I will assist you in meeting your obligations under Articles 32 to 36 GDPR: security of processing, notification of personal data breaches to the supervisory authority and to data subjects, data protection impact assessments, and prior consultation. The information in this DPA, its Annexes, the security page and the public source code will usually be what you need for an impact assessment; if you need more, email me.

7.3 Costs

Assistance under this Section is free of charge unless your requests are manifestly excessive or repetitive, in which case I may charge a reasonable fee that we agree in advance.

8. Personal data breaches

If I become aware of a personal data breach affecting Customer Data, I will notify the owners of your org by email without undue delay, and in any case within 48 hours of becoming aware of it. The notification will describe, to the extent then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed to address it and mitigate its effects, and a point of contact. Where I cannot provide all of this at once, I will provide it in phases without undue further delay. I will cooperate with you and take the reasonable steps you ask of me to investigate, contain and remedy the breach. My notification is not an admission of fault or liability.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data. Unsuccessful attempts (such as blocked requests, refused sign-in links or port scans) are not breaches and will not be notified.

9. Deletion and return

9.1 During the term

- **Usage events** are deleted automatically after your plan's retention period: 7 days on Free and Indie, 30 days on Team, 365 days on Agents. The cleanup job runs every six hours. Downgrading shortens the period from the next billing period.
- **Server logs** are kept for 14 days and then deleted.
- **Provider credentials, keys, labels and team members** are deleted or marked removed when you delete them in the dashboard or through the admin API. A removed team member's entry is kept so the audit log still names who did what.
- **Export.** At any time you can export usage events and the audit log as CSV from the dashboard or with `GET /v1/events.csv`, and read your configuration through the admin API.

9.2 At the end

When the Terms end for your org, or earlier if you ask me in writing to delete the org, I will delete all Customer Data within a reasonable time, normally within 30 days, including encrypted provider credentials, usage events, team members and configuration, and I will confirm the deletion by email on request. Two exceptions: data I must keep under EU or Member State law is kept only as long as that law requires and remains protected by this DPA; and copies in database backups persist until the backups rotate, which happens

after 14 days, during which they are used only to recover the service. Export what you need before closing your account, because after deletion I cannot return it.

10. Audits and information

I will make available to you all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and allow for and contribute to audits, including inspections, conducted by you or an auditor you mandate. Because the Hosted Service is run by one person on a cloud provider's infrastructure, the following is how that works in practice:

- **Documentation first.** This DPA, its Annexes, the security page, the Privacy Policy and the public source code at github.com/KIvanow/spend-brake describe what the Hosted Service does and how it is protected. Spend Brake has no SOC 2 or ISO 27001 report, and I do not claim one.
- **Questionnaires on request.** I will answer a reasonable written security or data protection questionnaire once in any 12-month period, and more often after a personal data breach affecting your Customer Data or when a supervisory authority requires it. I will answer within 30 days of receiving it.
- **On-site inspections** only where Data Protection Law or a supervisory authority requires one that documentation and a questionnaire cannot satisfy. They take place on at least 30 days' written notice, during business hours, no more than once a year, at your cost, under a confidentiality agreement, and must not disturb other customers' data or the service. I cannot give access to DigitalOcean's data centres; for those you rely on DigitalOcean's own compliance documentation, which I will help you obtain.

If an audit finds that I am not complying with this DPA, I will fix the problem without undue delay and tell you what I changed.

11. Your obligations

- You are responsible for the lawfulness of the Customer Data you send through the Hosted Service, including having a legal basis, giving any notices to and obtaining any consents from data subjects that Data Protection Law requires, and for your instructions to me being lawful.

- You decide what your applications and agents send through the proxy and what you put in key names, agent and session labels, alert destinations and other free-text configuration. Those values are stored; keep personal data out of them unless you need it there. The Hosted Service is not designed for special categories of personal data (Article 9 GDPR) or data about criminal convictions; request contents pass through without being stored, but do not put such data in stored configuration.
- You keep the owners' email addresses on your org current, since that is where I send Sub-processor notices and breach notifications, and you tell me without delay if you believe a notice has not reached you.
- You remain responsible for your agreements with API providers and with the recipients of the alerts, webhooks and telemetry you configure.

12. Liability

Each party's liability arising out of or relating to this DPA, whether in contract, tort or otherwise, is subject to the exclusions and limitations in Section 13 (Limitation of Liability) of the Terms, and the amounts under this DPA and the Terms together count towards the single cap in Section 13.2 of the Terms. Nothing in this DPA limits either party's liability where Data Protection Law does not allow it to be limited, or affects a data subject's rights under Article 82 GDPR.

13. Term, precedence and governing law

13.1 Term

This DPA takes effect when the Terms do for your org and remains in force for as long as I process Customer Data for you, including the deletion period in Section 9.2.

13.2 Precedence

For matters of data protection, this DPA takes precedence over the Terms and any other agreement between us to the extent they conflict. Where a Sub-processor's Standard Contractual Clauses apply to a transfer and conflict with this DPA, the Clauses prevail for that transfer. Everything else about our relationship, including fees, warranties, liability and termination, is governed by the Terms.

13.3 Changes

I may update this DPA where Data Protection Law, a supervisory authority, a change in Sub-processors or a change in the Hosted Service requires it, in the way the “Changes” paragraph of the Terms allows: by posting the new version on the website with a new

effective date and, for material changes, emailing the owners of your org at least 30 days before it takes effect. Changes that reduce protection for data subjects require your agreement, which may be given by continuing to use the Hosted Service after the notice period.

13.4 Governing law and venue

This DPA and any dispute arising out of or relating to it are governed by the laws of the Republic of Bulgaria and subject to the exclusive jurisdiction of the courts of Sofia, Bulgaria, as Section 16 of the Terms provides, without prejudice to any right a data subject or supervisory authority has under Data Protection Law. Where Data Protection Law requires that a provision of this DPA be governed by the law of an EU Member State, Bulgarian law applies.

13.5 Severability and notices

If any provision of this DPA is held invalid, the rest remains in force and the invalid provision is replaced by one that comes closest to its purpose and complies with Article 28 GDPR. Notices under this DPA go to the owners of your org by email, and to me at kristiyan@spendbrake.dev or by post to the address at the top of this DPA.

Annex I: Details of processing

Parties

- **Controller (data exporter):** the Customer, the organization holding the org on the Hosted Service, acting through its owners.
- **Processor (data importer):** Kristiyan Ivanov, self-employed individual registered in Bulgaria (BULSTAT 180490275), zh.k. Hadzhi Dimitar 16, entrance B, floor 1, apt. 13, Poduyane district, 1510 Sofia, Bulgaria, kristiyan@spendbrake.dev.

Subject matter

Operation of the Hosted Service for the Customer: a proxy that enforces spend caps on the paid APIs the Customer's applications and agents call, with the dashboard, admin API, alerts, telemetry and command-line tool around it.

Duration

For as long as the Customer holds an org on the Hosted Service, plus the deletion period in Section 9.2 of the DPA.

Nature of the processing

- Receiving each request the Customer's applications and agents send to the proxy; reading its route and parameters in memory to price it, to check it against caps, to detect identical repeated calls (by a one-way hash) and to enforce IP allowlists; forwarding it to the API provider the Customer addressed with the Customer's own provider key; streaming the provider's response back to the Customer without caching it.
- Recording a usage event with metadata about each call; keeping request logs; storing the Customer's configuration, encrypted provider credentials, team members and audit log; showing all of this in the dashboard, the admin API, Prometheus metrics and CSV exports; sending the alerts, webhooks, emails and OpenTelemetry spans the Customer configures.
- Hosting, backing up and deleting the above.

Purpose

To enforce the spend caps, loop rules and kill switches the Customer sets; to account for and show what each call cost; to alert the Customer; and otherwise to provide the Hosted Service as described in the Terms. No other purpose.

Categories of data subjects

- **People whose data is in proxied requests:** the Customer's end users, customers, contacts and other persons whose data the Customer's applications and agents include in API requests, for example an address in a geocoding request, a place search, or a phone number and message in a Twilio request. This data is processed in transit only.
- **People and systems calling the proxy:** the Customer's developers, staff, automated agents and, where the Customer calls the proxy from end-user devices, its end users, whose client IP address, user agent and trace context are seen by the proxy.
- **The Customer's team and contacts:** owners, admins and viewers the Customer invites to its org, people named in the audit log, and the recipients of the alert emails the Customer configures.

Categories of personal data

- **In transit, never stored:** request bodies, response bodies and query strings of proxied calls, which may contain whatever the Customer's applications put in them. They are held in memory for the duration of the call and are not written to the database, logs, traces or caches.

- **Usage events:** timestamp; org, key, environment, agent and session labels (free text chosen by the Customer, which may identify a person if the Customer puts a name or id there); provider, route and SKU; worst-case and actual cost; whether the route was underpriced; outcome (allowed, blocked, loop detected, upstream error); the provider's HTTP status and latency; the caller's trace context (`traceparent`), user agent, and request and response sizes in bytes; and a one-way hash of the request that cannot be turned back into it.
- **Server logs:** HTTP method, URL with secret query parameters redacted, the client IP address as seen by the proxy (behind the HTTPS front, the forwarded address), status code and timing. Client IP addresses are also used transiently to rate-limit sign-in and admin endpoints and to check IP allowlists; they are not part of usage events.
- **Team and configuration:** team members' email addresses (stored lower-case) and roles; hashed sign-in and API tokens; audit log entries naming who changed caps, keys, credentials, team members and kill switches, and when; key names, caps, environments, loop rules and IP allowlists; alert email addresses; webhook URLs, Slack, Discord and Teams webhooks, and OpenTelemetry endpoints and headers (webhook URLs and telemetry headers stored encrypted); the Customer's provider API keys, stored encrypted.

Special categories of data

None intended. The Hosted Service does not store request contents and is not designed for special categories of personal data or data about criminal convictions; the Customer must not put such data in stored configuration (Section 11 of the DPA).

Frequency, retention and location

- **Frequency:** continuous, for every request made with one of the Customer's Spend Brake keys and every action in the dashboard or admin API.
- **Retention:** usage events for the Customer's plan's retention period (7 days on Free and Indie, 30 days on Team, 365 days on Agents); server logs 14 days; team, keys and configuration while the org exists; provider credentials until the Customer removes them or deletes the org; database backups 14 days.
- **Location:** DigitalOcean's Frankfurt, Germany (FRA1) region, with the Sub-processors in Annex III for the functions stated there.

Annex II: Technical and organisational measures

These are the measures in place as of the effective date, written from the code, which is public at github.com/KIvanow/spend-brake. The security page describes them in

more detail and names the files that implement them. Spend Brake has no SOC 2 or ISO 27001 certification.

Encryption of secrets at rest

- Provider API keys, webhook URLs and their signing secrets, OpenTelemetry headers, SSO client secrets and billing-export service accounts are sealed with envelope encryption: a fresh random 32-byte data key per secret, used once with AES-256-GCM and a random 12-byte nonce, then wrapped by a master key held in the service's environment or in AWS KMS. Only the wrapped data key is stored.
- Both layers carry associated data naming the purpose, the org id and the credential id, so a ciphertext moved to another org or row fails to decrypt. Data keys are zeroed in memory after use.
- Plaintext secrets exist only in the proxy's memory (cached for at most five minutes) and, for Twilio price lookups, in the worker's. Nothing writes a decrypted key to disk, to a log, to a trace or to a response. The master key is not part of any backup.

Encryption in transit

- The hosted proxy and dashboard sit behind Caddy, which obtains and renews certificates from Let's Encrypt. Both send `Strict-Transport-Security: max-age=31536000; includeSubDomains`. Server version headers are removed.
- Requests to API providers are forwarded over HTTPS with the Customer's key injected by the proxy; the credential headers the Customer's application sent (`Authorization`, `Cookie`, `X-Goog-Api-Key`, `X-Api-Key`, `X-Subscription-Token`, `X-Brake-*`) are dropped before forwarding.

Data minimisation

- Request bodies, response bodies and query strings are never stored. Responses are streamed through and not cached. Only the metadata listed in Annex I is recorded.
- A redacting logger replaces credential headers with `[redacted]`, strips the values of secret query parameters (`key`, `api_key`, `apikey`, `access_token`, `token`, `signature`, `client_secret`) and removes anything shaped like a Spend Brake key from free text, including error messages, before a log line is written.
- Product analytics on the dashboard are linked to internal user and org ids, never to email addresses or names, contain no key values, credentials, amounts or request content, and the PostHog project is set to discard IP addresses. No session recordings, surveys or autocapture.

Access control and authentication

- Spend Brake keys and admin API tokens are stored as SHA-256 hashes; keys are shown once when created, can be scoped, capped, restricted to an IP allowlist and revoked at any time; tokens can carry an expiry and be revoked.
- Dashboard sign-in is by one-time emailed link carrying a random 32-byte code in the URL fragment (so it does not appear in server logs); only the code's hash is stored, it is valid for 15 minutes and works once; at most five links an hour are sent to one address; a session lasts seven days. There are no passwords. Orgs may instead use single sign-on (OIDC, SAML) with a Business or Enterprise License.
- Org roles (owner, admin, viewer; with more roles under a License) limit what each team member can do. Admin endpoints are rate-limited per client address; behind the HTTPS front only the private hops in front of the service are trusted to say what that address is.
- Operationally, one person, the Processor, administers the Hosted Service. No employees or contractors have access to production systems or Customer Data.

Integrity and accountability

- Changes to caps, keys, credentials, team members and kill switches are recorded in an audit log with who made them and when; the audit log can be exported as CSV.
- Outgoing webhooks and alert action links (Kill, Raise, Mute) are signed with HMAC-SHA256 over a timestamp and the raw body, so recipients can verify them.
- Every cap check is one atomic step in the budget store; if the store is unavailable the proxy fails closed (HTTP 503) unless a key has opted into a bounded fail-open allowance.

Network and platform security

- Outbound connections to URLs the Customer supplies (webhooks, OpenTelemetry collectors, custom APIs, SSO issuers) go through a guarded HTTP client that refuses loopback, private, link-local (including cloud metadata), carrier-grade NAT, multicast, unspecified, NAT64 and IPv4-mapped addresses, checked on the address actually connected to.
- Postgres and Valkey are not published outside the service's container network; the application ports bind to the loopback interface and are reached only through Caddy.
- The dashboard is served with a Content Security Policy that allows scripts and styles from itself only, connections to its own API and PostHog EU, and forbids framing. The website has a stricter policy still and sends `X-Content-Type-Options`, `X-Frame-Options` and `Referrer-Policy` headers.

Availability, backups and retention

- The Hosted Service, its database and cache run on DigitalOcean in the Frankfurt, Germany (FRA1) region.
- Backups of Postgres (configuration, ledger, audit log) and Valkey (live counters, reservations, kill switches) are taken nightly and kept for 14 days. They are stored on the same server as the service, contain the encrypted credential envelopes and not the master key, and are used only to recover the service.
- Usage events are deleted automatically after the plan's retention period by a cleanup job that runs every six hours; server logs are kept 14 days.

Incident handling and transparency

- Personal data breaches affecting Customer Data are notified to the Customer without undue delay and in any case within 48 hours of my becoming aware of them (Section 8 of the DPA).
- Security problems can be reported to kristiyan@spendbrake.dev, which I read myself. The whole codebase, including the proxy, the budget engine, the encryption and the infrastructure files, is public, so the measures above can be verified by reading it.

Annex III: Sub-processors

The Sub-processors engaged as of the effective date. The purpose and “what they see” columns match the service providers table in the Privacy Policy. API providers the Customer addresses and destinations the Customer configures are not Sub-processors (Section 2.2 of the DPA).

Sub-processor	Purpose	What they see	Location and transfer basis
DigitalOcean	Hosting the hosted service, its database and cache	All data stored by the Service, on their infrastructure	Frankfurt, Germany (FRA1 region), European Economic Area
Stripe	Payments, subscriptions, invoices	Billing details, email, plan	United States company; may process in the United States. Transfer relies on Stripe's Standard Contractual Clauses or Data Privacy Framework certification.

Sub-processor	Purpose	What they see	Location and transfer basis
Resend	Transactional email	Recipient email, message content (sign-in links, alerts, invitations, licenses)	United States company; may process in the United States. Transfer relies on Resend's Standard Contractual Clauses or Data Privacy Framework certification.
Vercel	Hosting this website	Web request logs for spendbrake.dev	United States company; serves the website from its edge network worldwide. Transfer relies on Vercel's Standard Contractual Clauses or Data Privacy Framework certification.
PostHog	Product analytics (PostHog, Inc.; EU Cloud, hosted in Frankfurt, Germany)	Pages viewed, button clicks and the product events above, browser and device details, coarse location; on the dashboard, your internal user and org ids	Data stored in Frankfurt, Germany. PostHog, Inc. is a United States company; any access from there relies on PostHog's Standard Contractual Clauses or Data Privacy Framework certification.

Of these, only DigitalOcean and Resend handle Customer Data in the ordinary course: DigitalOcean hosts everything, and Resend delivers the alert and invitation emails the Customer configures. Stripe sees the Customer's billing data, Vercel sees visits to this website, and PostHog sees the dashboard analytics described in the Privacy Policy; they are listed so that the list here and the one in the Privacy Policy are the same. Changes to this list are notified under Section 5.2 of the DPA.