Hatchbox Data Processing Agreement

Signable copy · Last updated October 26, 2026 · The same terms apply to every customer through the Hatchbox Terms of Use at hatchbox.io/dpa.

1. Parties and background

This Data Processing Agreement ("DPA") is entered into between **GoRails, LLC**, a Missouri limited liability company, PO Box 539, Wentzville, MO 63385, USA, operating the Hatchbox service at hatchbox.io ("Hatchbox" or "Processor"), and the customer named on the signature page ("Customer" or "Controller").

This DPA forms part of the Hatchbox Terms of Use (the "Agreement") and applies whenever Hatchbox processes Personal Data on behalf of Customer in the course of providing the Service. It has the same terms as the DPA incorporated into the Agreement at hatchbox.io/dpa, and signing it gives the parties a countersigned copy for their records. It reflects the parties' agreement on the processing of Personal Data in accordance with Article 28 of the GDPR.

Hatchbox provisions, configures and deploys applications to servers that Customer owns or rents from a cloud provider. To do this, Hatchbox holds SSH access to those servers, can read application and system logs, and stores the credentials for databases and environment variables it creates. Hatchbox does not need to view Personal Data to provide the Service, but because this access makes it technically possible, Hatchbox acts as a Processor and the parties enter into this DPA.

2. Definitions

Capitalized terms not defined here have the meaning given in the Agreement or in the GDPR.

- **"Data Protection Law"** means the GDPR, the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and any national law implementing or supplementing them, each as applicable to the processing under this DPA.
- **"GDPR"** means Regulation (EU) 2016/679.
- **"Personal Data"** means any personal data, as defined in Data Protection Law, that Hatchbox processes on behalf of Customer under the Agreement. This includes Personal Data contained in Customer's application databases, environment variables, application and server logs, and backups on Customer Servers, to the extent Hatchbox accesses or stores it.
- **"Customer Servers"** means the servers, databases and related infrastructure that Customer owns or rents from a third-party cloud provider and connects to the Service.
- **"Service"** means the Hatchbox server provisioning, application deployment and management platform at hatchbox.io, including its web dashboard, API and MCP server.
- **"Sub-processor"** means any third party engaged by Hatchbox to process Personal Data on Customer's behalf.
- **"Standard Contractual Clauses"** or **"SCCs"** means the standard contractual clauses for the transfer of personal data to third countries adopted by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
- **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- **"Controller"**, **"Processor"**, **"data subject"**, **"processing"** and **"supervisory authority"** have the meanings given in the GDPR.

3. Scope, roles and instructions

3.1 Roles. Customer is the Controller (or, where Customer acts on behalf of its own customers, a Processor) of the Personal Data, and Hatchbox is the Processor. Where Customer is itself a Processor, Customer warrants that its instructions to Hatchbox are authorized by the relevant Controller.

3.2 Hatchbox as Controller of account data. This DPA does not apply to data Hatchbox processes as a Controller for its own purposes, such as Customer's account registration details, billing information, support correspondence and usage data of the Service. That processing is governed by the Hatchbox Privacy Policy. Stripe, which processes billing information for Hatchbox, is listed in Annex III for completeness.

3.3 Documented instructions. Hatchbox will process Personal Data only on Customer's documented instructions, unless required to do so by EU or Member State law to which Hatchbox is subject. In that case Hatchbox will inform Customer of the legal requirement before processing, unless the law prohibits this on important grounds of public interest. Customer's instructions are:

1. the Agreement and this DPA;
2. Customer's use of the Service, including the configuration of servers, applications, databases, environment variables, cron jobs, backups and deploys through the dashboard, API, MCP server and git provider integrations; and
3. any further written instructions Customer gives, such as a support request asking Hatchbox to investigate an issue on a Customer Server.

3.4 Unlawful instructions. Hatchbox will inform Customer without undue delay if, in its opinion, an instruction infringes Data Protection Law. Hatchbox is not obliged to carry out a legal review of Customer's instructions.

3.5 Nature of access. Customer acknowledges that providing the Service requires Hatchbox to hold root-level SSH access to Customer Servers, to read application and server logs on request through the Service, and to generate and store credentials for databases and environment variables. Hatchbox accesses Customer Servers only to carry out operations Customer initiates through the Service, to resolve support requests Customer raises, or to maintain the security and stability of the Service. Hatchbox does not access the contents of Customer's databases or logs for any other purpose.

3.6 Customer obligations. Customer is responsible for the lawfulness of the Personal Data it processes using the Service, for providing any required notices and obtaining any required consents from data subjects, and for the configuration and security of Customer Servers and applications beyond the measures described in Annex II.

4. Hatchbox obligations

4.1 Confidentiality. Hatchbox ensures that every person it authorizes to process Personal Data is bound by a contractual or statutory duty of confidentiality and has received appropriate training on their responsibilities.

4.2 Security. Hatchbox implements and maintains the technical and organizational measures described in Annex II, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks to data subjects. Hatchbox may update these measures from time to time provided the overall level of protection is not reduced.

4.3 Assistance with data subject rights. Taking into account the nature of the processing, Hatchbox will assist Customer by appropriate technical and organizational measures, insofar as this is possible, in fulfilling Customer's obligation to respond to requests from data subjects exercising their rights under Chapter III of the GDPR. Because Customer controls its own applications and databases, Customer will normally fulfil such requests directly. Hatchbox will forward to Customer any request it receives that relates to Customer's Personal Data and will not respond to the data subject except on Customer's instruction.

4.4 Assistance with compliance. Hatchbox will assist Customer in ensuring compliance with Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the processing and the information available to Hatchbox. Hatchbox may charge reasonable fees for assistance under Sections 4.3 and 4.4 that goes beyond what Customer can do itself through the Service.

4.5 Deletion and return. Hatchbox will delete the Personal Data it holds relating to Customer, namely stored environment variables, database credentials, SSH keys, server metadata and cached log output, when Customer deletes its Hatchbox account, or within 30 days of Customer's written request (including a request on termination of the Service), unless EU or Member State law requires continued storage. Copies in Hatchbox's control-plane backups are isolated from further processing and expire within 7 days. Personal Data on Customer Servers remains under Customer's control at all times. Deleting a cloud server through the Service deletes it from the cloud provider. For a server Customer connected to the Service itself, Customer should remove the Hatchbox public key from that server after removing it from the Service. Customer is responsible for deleting or retaining Customer Servers and backups with its cloud provider.

4.6 Audits. Hatchbox will make available to Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and will allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer. Customer will first review the information Hatchbox makes available and will request an on-site or remote audit only where that information is insufficient. Audits are limited to once per 12 months unless required by a supervisory authority or following a Personal Data Breach, require at least 30 days' written notice, take place during normal business hours, must not unreasonably disrupt Hatchbox's operations, and are at Customer's expense. The auditor must be bound by confidentiality obligations.

4.7 Records. Hatchbox maintains a record of the categories of processing it carries out on behalf of Customer as required by Article 30(2) of the GDPR.

5. Sub-processors

5.1 General authorization. Customer gives Hatchbox general written authorization to engage the Sub-processors listed in Annex III, and to engage additional or replacement Sub-processors in accordance with this Section 5.

5.2 Notice of changes. Hatchbox will give Customer at least 30 days' prior notice of any intended addition or replacement of a Sub-processor by email to the owner of Customer's Hatchbox account and to any additional contact Customer has given Hatchbox in writing. Where a replacement is needed urgently for the security or continuity of the Service, Hatchbox may make it immediately and will notify Customer as soon as practicable afterwards, and Customer's right to object below still applies. Customer may object on reasonable data protection grounds in writing within that period. If Customer objects, the parties will discuss the concern in good faith. If no resolution is reached, Customer may terminate the affected part of the Service without penalty by written notice, and Hatchbox will refund any prepaid fees for the period after termination.

5.3 Flow-down. Hatchbox will impose on each Sub-processor data protection obligations that are substantially the same as those in this DPA, by way of a written contract, and in particular will ensure that each Sub-processor provides sufficient guarantees to implement appropriate technical and organizational measures.

5.4 Liability for Sub-processors. Hatchbox remains fully liable to Customer for the performance of each Sub-processor's obligations.

5.5 Customer's own providers. The cloud provider on which Customer Servers run (for example DigitalOcean, Hetzner, AWS or Linode), Customer's git hosting provider and Customer's backup storage provider are engaged directly by Customer and are not Sub-processors of Hatchbox. Customer is responsible for its own agreements with those providers.

6. International transfers

6.1 Location of processing. Hatchbox is established in the United States. The Hatchbox control plane (the service that stores Customer's configuration, credentials and cached log output) is hosted by DigitalOcean in the United States, and its database backups are stored in Amazon S3 in the United States. Customer Servers are located wherever Customer chooses to provision them, and Personal Data on Customer Servers is not moved by Hatchbox to any other location.

6.2 Standard Contractual Clauses. To the extent Hatchbox's processing involves a transfer of Personal Data from the European Economic Area to a country that has not received an adequacy decision from the European Commission, the parties enter into the Standard Contractual Clauses, Module Two (transfer controller to processor), which are incorporated into this DPA by reference. Where Customer is itself a Processor, Module Three (transfer processor to processor) applies instead. For the purposes of the SCCs:

1. Customer is the "data exporter" and Hatchbox is the "data importer";
2. Clause 7 (the optional docking clause) does not apply;
3. in Clause 9(a), Option 2 (general written authorization) applies, with the notice period in Section 5.2 of this DPA;
4. in Clause 11(a), the optional language on independent dispute resolution bodies does not apply;
5. in Clause 13 and Annex I.C, the competent supervisory authority is the authority of the EU Member State in which Customer is established;
6. in Clause 17 (Option 1), the SCCs are governed by the law of Ireland, unless Customer's Member State law is required by the SCCs, in which case that law applies;
7. in Clause 18(b), disputes will be resolved before the courts of Ireland;
8. Annex I.A of the SCCs is completed by Section 1 and the signature page of this DPA, Annex I.B by Annex I of this DPA, Annex II of the SCCs by Annex II of this DPA, and Annex III of the SCCs by Annex III of this DPA.

6.3 United Kingdom. For transfers of Personal Data subject to the UK GDPR, the SCCs apply as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0, in force 21 March 2022). Table 1 is completed with the parties' details in Section 1, Table 2 refers to the SCCs as completed in Section 6.2, Table 3 refers to Annexes I to III of this DPA, and in Table 4 either party may end the Addendum as set out in its Section 19.

6.4 Switzerland. For transfers subject to the Swiss Federal Act on Data Protection, the SCCs apply with the adaptations required by the Swiss Federal Data Protection and Information Commissioner: references to the GDPR are read as references to the FADP, the competent supervisory authority is the FDPIC, and data subjects in Switzerland may enforce their rights in Switzerland.

6.5 Conflict. If there is any conflict between this DPA and the SCCs, the SCCs prevail.

6.6 Alternative transfer mechanisms. If the European Commission or a supervisory authority invalidates or supersedes the SCCs, or if Hatchbox certifies under a transfer framework recognized by an adequacy decision (such as the EU-US Data Privacy Framework), the parties will cooperate in good faith to rely on that alternative mechanism, and the SCCs will cease to apply to the extent the alternative mechanism covers the transfer.

7. Personal Data Breaches and requests

7.1 Notification. Hatchbox will notify Customer without undue delay and, where feasible, within 72 hours after becoming aware of a Personal Data Breach affecting Customer's Personal Data. Notice will be sent by email to the owner of Customer's Hatchbox account and to any additional security contact Customer has given Hatchbox in writing.

7.2 Content of notice. The notification will, to the extent known at the time and supplemented as information becomes available, describe the nature of the breach including the categories and approximate number of data subjects and

records concerned, the likely consequences, the measures Hatchbox has taken or proposes to take, and a contact point for further information.

7.3 Scope. Hatchbox's notification duty covers breaches of the Hatchbox control plane and of Hatchbox's own access to Customer Servers (for example a compromise of the SSH key Hatchbox holds for Customer's cluster). Customer is responsible for detecting and handling breaches within its own applications and on Customer Servers that do not involve Hatchbox's systems or credentials. Hatchbox will nonetheless provide reasonable assistance on request.

7.4 Cooperation. Hatchbox will cooperate with Customer and take reasonable steps as directed by Customer to investigate, mitigate and remediate a Personal Data Breach. Hatchbox will not notify a supervisory authority or data subjects of a breach affecting Customer's Personal Data unless required by law, and will inform Customer before doing so where legally permitted.

7.5 Government and third-party requests. If Hatchbox receives a legally binding request from a public authority or a third party for access to Customer's Personal Data, Hatchbox will, unless legally prohibited, promptly notify Customer, review the legality of the request, challenge it where there are reasonable grounds to do so, and disclose only the minimum information required.

8. Term, liability and general terms

8.1 Term. This DPA takes effect on the date it is signed by both parties or, if earlier, the date it took effect under the Agreement, and remains in force for as long as Hatchbox processes Personal Data on behalf of Customer.

8.2 Liability. Each party's liability arising out of or related to this DPA, including the SCCs, is subject to the exclusions and limitations of liability set out in the Agreement, except to the extent that Data Protection Law or the SCCs do not permit liability to be limited. Nothing in this Section limits a party's liability to data subjects under the SCCs or Article 82 of the GDPR.

8.3 Order of precedence. In the event of a conflict, the following order of precedence applies: (1) the SCCs; (2) this DPA; (3) the Agreement; (4) the Hatchbox Privacy Policy.

8.4 Changes in law. If Data Protection Law changes in a way that makes this DPA inadequate, the parties will negotiate in good faith to amend it. Hatchbox may update this DPA on notice to Customer where the update is required by law or does not reduce the protection afforded to Personal Data.

8.5 Governing law. This DPA is governed by the law governing the Agreement, except that the SCCs are governed by the law stated in Section 6.2.

8.6 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in effect and the invalid provision will be replaced by a valid one that achieves the same purpose as closely as possible.

8.7 Counterparts and electronic signature. This DPA may be signed electronically and in counterparts, each of which is an original and which together form one instrument.

Annex I. Description of the processing

This Annex also serves as Annex I.B of the Standard Contractual Clauses.

Item	Description
Subject matter	Provisioning and management of Customer Servers and deployment of Customer's applications through the Service
Nature of processing	Storage of server configuration and credentials; execution of commands on Customer Servers over SSH to provision, deploy, restart, back up and maintain applications; retrieval and display of application and server log output at Customer's request; transmission of Customer-configured notifications

Item	Description
Purpose of processing	Providing the Service to Customer as described in the Agreement and responding to Customer's support requests
Categories of data subjects	Customer's employees and contractors who use the Service; end users of the applications Customer deploys on Customer Servers; any other individuals whose data Customer stores in those applications
Categories of Personal Data	Data Customer chooses to store in environment variables (for example third-party API keys and database URLs); database connection credentials; hostnames and IP addresses of Customer Servers; and any Personal Data contained in application and server logs or application databases that Hatchbox can technically access on Customer Servers, which may include names, email addresses, IP addresses, user identifiers and any other data Customer's applications process
Special categories of data	None intended. Customer must not instruct Hatchbox to process special categories of data (Article 9 GDPR) beyond incidental presence in logs or databases on Customer Servers, and is responsible for applying additional safeguards in its applications if such data is stored there
Frequency of transfer	Continuous for the duration of the Service, with access to Customer Servers occurring on each operation Customer initiates and on each support request
Duration of processing	The term of the Agreement, plus the deletion period in Section 4.5
Retention	Configuration and credentials are retained until Customer deletes the resource or the account. The output of deploy and other operation logs is automatically purged from the Hatchbox control plane 7 days after the operation (30 days for web server configuration logs) by a nightly job; only the record of the operation and its status remain. Hatchbox holds no copies of Customer's application databases
Transfers to Sub-processors	As listed in Annex III, for the purposes stated there

Annex II. Technical and organizational measures

This Annex also serves as Annex II of the Standard Contractual Clauses. Hatchbox maintains the following measures to protect Personal Data.

Access to Customer Servers

- Hatchbox connects to Customer Servers only over SSH with public key authentication. Password authentication is never used by Hatchbox.
- A separate SSH key pair (Ed25519, or RSA 4096 where the cloud provider requires it) is generated for each Customer cluster. A key is never shared between customers.
- SSH private keys are stored encrypted at rest in the Hatchbox control plane using application-level encryption, in addition to disk encryption by the hosting provider.
- Hatchbox staff do not hold copies of Customer SSH keys on their own devices. Operations Customer starts through the Service are recorded with their output in a log visible to Customer. When resolving a support request, Hatchbox staff may also open a terminal session on a Customer Server through the Hatchbox application, as described under Staff access and auditing.
- Customer can revoke Hatchbox's access at any time by removing the Hatchbox public key from a server, or for a cloud server, by deleting it through the Service.

- Optional jump hosts allow Customer to keep Customer Servers off the public internet while retaining Hatchbox management.

Credentials and secrets

- Environment variable values, database backup storage credentials, API tokens and git provider OAuth tokens are encrypted at rest with application-level encryption (Rails Active Record Encryption) and decrypted only when needed to perform an operation Customer has requested.
- Database passwords are generated by the Service using a cryptographically secure random generator and are never sent by email or displayed in logs.
- Secrets are redacted from deploy and operation logs where they appear in command output.

Control plane security

- The Hatchbox control plane is hosted by DigitalOcean with encrypted storage, managed firewalls and network isolation.
- All traffic between Customer's browser or API client and the Service, and between the Service and Sub-processors, is encrypted with TLS.
- Customer accounts support two-factor authentication (TOTP). Team access to Customer's account is role-based and managed by Customer.
- API access is by per-user tokens that Customer can revoke at any time.

Staff access and auditing

- Access to the production control plane is limited to a small number of authorized Hatchbox staff and is protected by multi-factor authentication.
- Production console sessions are logged and audited (console1984 and audits1984). Encrypted values such as environment variables and SSH keys remain encrypted in the console unless an engineer explicitly decrypts them, and each decryption is recorded with a stated reason.
- Hatchbox staff access a Customer account only to provide support Customer has requested, to investigate a security incident or service problem, or where required by law. Staff may view the account as a Customer user sees it to diagnose a problem. Hatchbox does not change Customer's Servers or applications during this access without Customer's instruction or permission. Support communications are recorded under the staff member's own identity.
- Staff are bound by confidentiality obligations.

Availability and resilience

- The control plane database is backed up hourly to Amazon S3, where backups are encrypted at rest (AES-256) and deleted after 7 days.
- Customer application database backups configured through the Service are written directly from Customer Servers to storage Customer controls (for example Customer's own S3 bucket). Hatchbox does not store copies of Customer's application data or backups.

Software security

- Hatchbox applies security updates to the control plane promptly and runs automated static analysis (Brakeman) and dependency vulnerability checks (bundler-audit) in its CI pipeline.
- Servers provisioned by the Service are configured with a firewall, unattended security updates and SSH hardening at provisioning time.

Data minimization and deletion

- Hatchbox stores only the configuration and credentials required to operate Customer Servers. It does not copy the contents of Customer databases.
- Log output retrieved from Customer Servers is streamed to Customer's browser and is not stored by Hatchbox except as part of deploy and operation logs, whose output is purged automatically after 7 days (30 days for web server configuration logs).
- Data is deleted as described in Section 4.5.

Annex III. Sub-processors

This Annex also serves as Annex III of the Standard Contractual Clauses. Hatchbox uses the following Sub-processors to provide the Service.

Sub-processor	Purpose	Data processed	Location	Transfer mechanism
DigitalOcean, LLC	Hosting of the Hatchbox control plane (web application, database, background workers)	All data stored in the control plane, including server configuration, encrypted credentials and operation logs	United States	EU-US Data Privacy Framework; SCCs
Amazon Web Services, Inc. (Amazon SES and Amazon S3)	Delivery of transactional email (deploy notifications, alerts, account email); storage of control plane database backups	Email addresses of Customer's users and the contents of notification emails, which may include short excerpts of deploy or error output; encrypted backups of all data stored in the control plane, kept for 7 days	United States	EU-US Data Privacy Framework; SCCs
AppSignal B.V.	Error and performance monitoring of the Hatchbox control plane	Technical error data from the control plane, which may incidentally include request parameters or identifiers relating to Customer's account	Netherlands	Processing within the EEA
Honeybadger Industries LLC	Error monitoring of the Hatchbox control plane	Technical error data from the control plane, which may incidentally include request parameters or identifiers relating to Customer's account	United States	SCCs
Stripe, Inc.	Payment processing and subscription billing for Hatchbox plans (see Section 3.2)	Billing contact name, email address and billing address; payment card details are collected directly by Stripe and not stored by Hatchbox	United States	EU-US Data Privacy Framework; SCCs

The cloud provider on which Customer Servers run, Customer's git hosting provider and Customer's backup storage provider are engaged by Customer directly and are not Sub-processors of Hatchbox (see Section 5.5).

The current list is published at hatchbox.io/dpa. Changes are announced by email as described in Section 5.2.

Signature page

By signing below, the parties agree to this Data Processing Agreement, including the Standard Contractual Clauses incorporated in Section 6. Fill in the fields, sign, and email the completed copy to support@gorails.com.

Customer (Controller / data exporter)

Customer legal name

Registered address

Company registration number

Contact email for notices under this DPA

For GoRails, LLC (Processor / data importer)

Name

Chris Oliver

Title

Owner

Date

Signature

For Customer

Name

Title

Date

Signature