DataTru Data Processing Addendum

Draft, subject to legal review. This is a draft published for review. It is not a signed agreement and it is not legal advice. It binds neither party until both have agreed the final text and signed it. Each bracketed SIGNING FIELD is completed when a copy is signed.

How this DPA is built

This DPA consists of this Cover Page and the Common Paper Data Processing Agreement Standard Terms Version 1.1 (https://commonpaper.com/standards/data-processing-agreement/1.1), which are incorporated by reference. The Standard Terms are used under the Creative Commons Attribution 4.0 licence, CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/). DataTru has changed them only as listed under "Changes to the Standard Terms" below. Common Paper did not write or review those changes. Where this Cover Page and the Standard Terms conflict, this Cover Page controls, but the EEA SCCs and the UK Addendum control over both, as Standard Terms section 9 provides. Capitalised words have the meaning the Standard Terms give them. "Provider" means the data importer named in Annex I. "Customer" means the Scale or Enterprise customer named in Annex I.

Cover Page: key terms

- **Provider:** Mithyl LLC, a [SIGNING FIELD: Provider state of formation] limited liability company, doing business as DataTru, with its registered address at [SIGNING FIELD: Provider registered address].
- **Agreement:** the DataTru Terms of Service at https://datatru.com/terms/, together with any order form or other written agreement for the Service that both parties sign.
- **Approved Subprocessors:** the list in Annex III.
- **Provider Security Contact:** legal@datatru.com. DataTru has no separate security address. Security questionnaires, Security Incident notices and data subject requests all use this address.
- **Security Policy:** the technical and organisational measures in Annex II. DataTru holds no third-party certification or audit report (such as SOC 2 or ISO 27001), and this DPA claims none. Change C3 replaces the Standard Terms' reliance on one.
- **Special Category Data:** none. Change C5 excludes it.
- **Special Category Data Restrictions or Safeguards:** Customer will not submit Special Category Data without Provider's prior written agreement (change C5). Annex II applies to any that reaches the Service by chance.
- **Liability:** inside the Agreement's limits and capped, as change C4 sets out. This DPA adds no uncapped liability beyond what Standard Terms section 8.3 requires.
- **Governing Member State:** Ireland, for Clauses 17 and 18 of the EEA SCCs.
- **UK transfers:** the UK Addendum applies. Under its Sections 12(c), 15(m), 15(n) and 16, it is governed by the laws of England and Wales and its disputes go to the courts of England and Wales, unless the parties expressly select the laws or courts of Scotland or Northern Ireland.
- **Governing law and courts for this DPA:** except where the EEA SCCs or the UK Addendum name a law or court, this DPA is governed by the laws of [SIGNING FIELD: Provider state of formation], and the state and federal courts located there have exclusive jurisdiction.
- **US state privacy laws (CCPA):** additional term A3 applies.

Processor terms (GDPR Article 28)

A reading aid, not part of the agreement: where it differs from the Standard Terms and the changes below, they apply. Each Article 28(3) requirement and where this DPA meets it:

Draft, subject to legal review.

GDPR Article 28	Where it is met
28(3)(a) Process only on documented instructions	Standard Terms 2.2 and 2.3
28(3)(b) Confidentiality of authorised persons	Additional term A1
28(3)(c) Security measures under Article 32	Security Policy (Annex II); Standard Terms 4
28(2), 28(3)(d), 28(4) Subprocessors	Standard Terms 2.6 as changed by C1 (30 days' notice); Annex III
28(3)(e) Help with data subject requests	Standard Terms 6.1
28(3)(f) Help with Articles 32 to 36	Standard Terms 4 as changed by C2 (notice without undue delay) and 6.2 (impact assessments)
28(3)(g) Delete or return data at the end	Standard Terms 7 as changed by C7; Annex I, Part B
28(3)(h) Information and audits	Standard Terms 5 as changed by C3
28(3), last paragraph: flag an unlawful instruction	Additional term A2

Changes to the Standard Terms

- **C1. Subprocessor changes (section 2.6).** "At least 10 business days in advance" becomes "at least 30 days in advance". Customer may object in writing, on reasonable data protection grounds, within those 30 days. If the parties cannot resolve the objection in good faith before the new Subprocessor starts, Customer's sole and exclusive remedy is to terminate the part of the Service that depends on that Subprocessor, by written notice to Provider. Where Provider must replace a Subprocessor urgently to protect the security or availability of the Service, it may give shorter notice, to the extent the EEA SCCs allow, and will give notice as soon as it can. The minimum notice under Clause 9 of the EEA SCCs stays at 10 business days, as section 3.2.3 sets.
- **C2. Security Incident notice (section 4).** In clause (a), "without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident" becomes "without undue delay after becoming aware of the Security Incident". Provider sends the notice to Customer's contact in Annex I, from legal@datatru.com.
- **C3. Audits and reports (section 5).** Section 5.2 is replaced with: "Provider is not audited by independent third-party auditors and holds no Report. On written request, Provider will give Customer Annex II and answer Customer's security questionnaire under section 5.3." Customer first exercises its audit rights through section 5.3. If that information is not reasonably enough to show Provider's compliance with this DPA, or a supervisory authority requires it, Customer may inspect Provider's Processing of Customer Personal Data on these conditions:
  - at most once in any 12 months, unless a Security Incident affecting Customer or a supervisory authority requires another;
  - on at least 30 days' written notice to the Provider Security Contact;
  - during business hours, without unreasonable disruption to the Service, and without access to other customers' data or to Subprocessors' facilities;
  - at Customer's own cost, by Customer or an independent auditor bound by confidentiality who is not a competitor of Provider. Customer will give Provider a copy of any audit report.
- **C4. Liability (section 8.1).** Added at the end: "To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability arising out of or related to this DPA and the Agreement together will not exceed the lower of any limit in the Agreement and the fees Customer paid or owed for the Service in the 12 months before the event giving rise to the liability. Liability under this DPA counts toward that limit and is not in addition to it." Section 8.3 still applies.
- **C5. Special Category Data.** Customer will not upload, connect or otherwise submit Special Category Data, or personal data relating to criminal convictions and offences, to the Service unless Provider has first agreed in writing. Review text is free text, so it can contain such data by chance. Customer is responsible for the content it submits, and Provider applies Annex II to whatever it receives.

Draft, subject to legal review

- **C6. Assignment.** Provider may assign this DPA, together with the Agreement, to an Affiliate or to a successor to all or substantially all of the business of the Service, including a company formed to run DataTru on its own, by written notice to Customer. The assignee takes on Provider's obligations under this DPA.
- **C7. Return and deletion (section 7).** Provider meets an instruction to return Customer Personal Data by letting Customer export its reviews, action items and topics as CSV files through the Service until the Agreement ends. Deletion follows the schedule in Annex I, Part B. Until backups expire, they stay encrypted and are used only to restore the Service.

Additional terms

These terms supplement the Standard Terms.

- **A1. Confidentiality.** Provider ensures that every person it authorises to process Customer Personal Data has committed to confidentiality or is under an appropriate statutory obligation of confidentiality.
- **A2. Unlawful instructions.** Provider will inform Customer immediately if, in its opinion, an instruction infringes Applicable Data Protection Laws.
- **A3. US state privacy laws.** Where Customer Personal Data is personal information under the California Consumer Privacy Act or a similar US state law, Provider acts as Customer's service provider or processor. Provider will not sell or share it, as those laws define these words. It will not retain, use or disclose it outside the direct business relationship with Customer, or for any purpose other than providing the Service, except as those laws permit a service provider. It will not combine it with personal information from other sources except as those laws permit. It will tell Customer if it can no longer meet these obligations.

International transfers

Customer Personal Data is stored and processed in the United States, and transactional email is sent through servers in the European Union (see Annex III). Transfers are governed by Standard Terms section 3:

- **EEA:** where the GDPR applies and no adequacy decision covers the transfer, the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) are incorporated. Module Two (controller to processor) applies when Customer is a Controller. Module Three (processor to processor) applies when Customer is a Processor. The options chosen for each clause are those in Standard Terms 3.2.3. Annexes I, II and III below complete the SCC annexes.
- **United Kingdom:** where the UK GDPR applies and no adequacy regulation covers the transfer, the UK Addendum (the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the Information Commissioner under S119A(1) of the Data Protection Act 2018) is incorporated, as Standard Terms 3.3 sets out.
- **Switzerland:** the SCCs apply with the changes in Standard Terms 3.4.

Provider is not certified under the EU-US Data Privacy Framework and relies on the SCCs and the UK Addendum above. Annex III shows which Subprocessors state that they participate in the Data Privacy Framework. Provider has not prepared a written transfer impact assessment. Under Standard Terms 6.2 it will give Customer the information Customer reasonably needs for its own assessment, including the facts in Annexes II and III.

Annex I: List of parties and details of processing

A. List of parties

Data exporter (Customer). Name, address, contact person and role (Controller or Processor) are completed when the parties agree the final text. Activities: using the DataTru Service.

Data importer (Provider). Mithyl LLC, a [SIGNING FIELD: Provider state of formation] limited liability company, doing business as DataTru. Address: [SIGNING FIELD: Provider registered address]. Contact person: [SIGNING FIELD: Provider contact person and title], legal@datatru.com. Role: Processor, or Subprocessor where Customer is a Processor. Activities: providing the Service described in Part B.

Draft, subject to legal review

B. Description of processing

- **Service:** DataTru, a hosted service that ingests customer reviews, analyses them (sentiment, topics, summaries) and reports the results.
- **Categories of data subjects:**
  - Customer's authorised users: workspace members and people invited to a workspace.
  - Authors of the reviews Customer uploads or connects.
  - People named or described in review text.
- **Categories of personal data:**
  - Authorised users: name, email address, password (stored only as an Argon2 hash), multi-factor authentication settings, organisation and workspace membership and role, and activity in the Service.
  - Reviews: review text and title, rating, date, source, product, external identifier, language, and any other field in an uploaded file, which may include a reviewer's name or handle.
  - Derived data: sentiment scores, topics and summaries produced from reviews.
  - Technical data: IP address and browser details in server and error logs.
- **Special category data:** none intended, and excluded by change C5. Free-text reviews may contain it by chance. Annex II applies to it, and no further safeguards apply.
- **Frequency of transfer:** continuous, for the term of the Agreement.
- **Nature and purpose of processing:** receiving, storing, analysing, displaying, exporting and erasing Customer Personal Data to provide the Service under the Agreement. Reviews are analysed by language models that DataTru runs on its own servers. DataTru does not use Customer's review content to train third-party models without Customer's consent.
- **Duration of processing:** as Standard Terms 2.1 and 7 provide, with this deletion schedule:
  - Deleted records are first soft-deleted. A scheduled job runs every day and permanently removes records soft-deleted more than 30 days earlier, so removal from the live database takes about 30 days (between 30 and 31).
  - Database backups keep 28 daily, 12 weekly and 12 monthly snapshots, so deleted data can remain in encrypted backups for up to about 12 months. Backups of uploaded files are kept for up to about 8 months, and backups of logs for up to about 4 months.

C. Competent supervisory authority

As Standard Terms section 3 and the Cover Page provide: the supervisory authority of the data exporter under Clause 13 of the EEA SCCs, or the Information Commissioner for UK transfers.

Annex II: Technical and organisational measures

Only measures found in DataTru's code, configuration and accounts are listed. Where a common control is not in place, this Annex says so.

Encryption in transit

- All public traffic is HTTPS. The reverse proxy (Traefik) serves Let's Encrypt certificates and HTTP requests redirect to HTTPS.
- HTTP Strict Transport Security is set for one year, including subdomains.
- Session and CSRF cookies are Secure-only and use the `__Secure-` prefix.
- A Content Security Policy, a strict referrer policy and a same-origin opener policy are set on responses.
- Calls to subprocessors (email, payments, error reports) use HTTPS.

Draft, subject to legal review

Encryption at rest and pseudonymisation

- Oracle Cloud Infrastructure encrypts the production server's boot and block volumes at rest with AES-256, using Oracle-managed keys. The database and uploaded files are stored on those volumes. DataTru adds no separate disk or database encryption of its own.
- Backups are encrypted by restic on DataTru's server before they are sent off site. The off-site provider stores only encrypted data.
- User passwords are stored only as Argon2 hashes.

User identification and authorisation

- Email verification is mandatory before an account can be used.
- Users can turn on multi-factor authentication (authenticator app codes, with recovery codes).
- The API requires an authenticated user by default.
- Rate limits apply to sign-in and API requests.
- Data is scoped to organisations and workspaces, and members see only the workspaces they belong to.

Operational access

- Only the web ports (80 and 443) are open to the internet.
- Internal tools (metrics dashboards, the task monitor, the backup console, the job scheduler) listen only on the server itself and are reached through an SSH tunnel.
- One person, DataTru's founder, holds administrative access to the production server (SSH, with a key) and to DataTru's private source repository.
- Production changes are deployed from the repository's protected main branch by a CI runner on the production server. Only the founder's account and automation tokens the founder controls can push to that branch.
- There is no formal process for issuing and revoking access keys, because no one else holds access.

Event logging and monitoring

- Container logs are collected centrally (Promtail and Loki) on DataTru's own server and kept for 7 days.
- Metrics (Prometheus) are kept for 7 days, and request traces (Tempo) for 24 hours.
- Copies of the log, metric and trace stores are included in the encrypted backups, which keep them for up to about 4 months.
- Application errors are reported to Sentry, which keeps them for the retention period of DataTru's Sentry plan. The integration leaves Sentry's "send default personal data" option off, but an error report can still contain data from the failing request.

Availability, resilience and restoration

- Backrest runs restic backups on a schedule. The database is dumped nightly at 01:30 UTC, and the cache store at 01:50 UTC.
- Database backups keep 28 daily, 12 weekly and 12 monthly snapshots.
- A weekly integrity check reads back 10% of the backup data.
- Backups are stored off site with Dropbox (Annex III).
- Every change's CI pipeline backs up and restores a disposable copy of the backup system as a test.
- No restore of production backups has been rehearsed and logged yet. DataTru plans quarterly restore drills.

Data minimisation and retention

Draft, subject to legal review

- Review analysis runs on language models hosted on DataTru's own servers. Review content is not sent to a third-party AI provider.
- Customers can delete review content from their workspace settings. Deletion follows the schedule in Annex I, Part B.

Testing and configuration

- Every change runs an automated test suite and lint checks in continuous integration before it is deployed.
- No penetration test has been carried out.

Physical security

- The servers sit in Oracle Cloud Infrastructure data centres (region us-phoenix-1), and their physical security is Oracle's. DataTru runs no data centre or server room of its own.

Personnel and governance

- DataTru is run by one person, its founder, who is the only person with access to Customer Personal Data. DataTru has no employees or contractors with such access.
- Before anyone else is given access, DataTru will bind them to confidentiality (additional term A1) and brief them on these measures. There is no formal security training programme.
- Certifications: none. DataTru holds no SOC 2 report, ISO 27001 certificate or other security certification.

Annex III: Approved subprocessors

Subprocessor	Purpose	Personal data involved	Location	Transfer safeguards it states
Oracle Cloud Infrastructure: the Oracle Corporation affiliate named in DataTru's Oracle cloud order	Hosting: servers and storage for the application, database and files	All Customer Personal Data	United States, region us-phoenix-1	EU-US Data Privacy Framework; EU SCCs
Brevo: Brevo, Inc. (United States), part of the Brevo group led by Brevo SAS (France)	Sending transactional email (verification, invitations, password resets, billing notices)	Authorised users' names, email addresses and the email content	European Union: France and Belgium	Hosted in the EU; EU-US Data Privacy Framework for Brevo, Inc.; EU SCCs
Sentry: Functional Software, Inc., doing business as Sentry (United States)	Error monitoring	Error reports, which may contain data from the failing request	United States	EU-US Data Privacy Framework; EU SCCs (Modules Two and Three)
Dropbox: Dropbox, Inc. (United States)	Off-site backup storage	Encrypted backups of the database, files and logs; Dropbox holds no key	United States	EU-US Data Privacy Framework

Not a subprocessor: Stripe. Stripe, LLC (United States) processes the billing contact and payment details DataTru collects to bill Customer. DataTru decides that processing as a controller for its own billing, and Stripe also acts as an independent controller for some of it. It is not processing Customer Personal Data on Customer's behalf, so it is not listed above.

Checked and not used as subprocessors today: product analytics (PostHog code is present but not enabled in production), third-party object storage, third-party AI providers, and a content delivery network. Adding any of them is a subprocessor change under Standard Terms 2.6, as changed by C1.

Draft, subject to legal review

Signatures

Signature blocks are added once both parties agree the final text. This draft carries none.

Draft, subject to legal review