DERROS

LEGAL

LEGAL · FOR TRELLIS CLIENTS

Data Processing Agreement

The terms on which we process personal data for organisations that use Trellis.

VERSION	IN EFFECT FROM	SUB-PROCESSORS UPDATED
1.0	15 March 2026	18 September 2026

derros.com/legal/data-processing-agreement

IN THIS DOCUMENT

01

About this agreement

This Data Processing Agreement ("**DPA**") is between **Derros Ltd**, a company registered in Jersey with company number 159837 and its registered office at 3 Pinewood Close, La Rue Du Pont Marquet, St. Brelade, JE3 8DT, Jersey ("**Derros**", "we", "us"), and the organisation that uses the Trellis platform under terms or an engagement letter that refers to this DPA (the "**Client**", "you").

It forms part of that agreement (the "**Main Agreement**") and applies whenever we process personal data on your behalf in providing Trellis. If this DPA and the Main Agreement conflict on the processing of personal data, this DPA takes precedence.

This DPA covers Trellis wherever Derros hosts it, in our multi-tenant service or as a dedicated instance. If you run Trellis on premise, on your own infrastructure, the Client Personal Data stays with you, and this DPA applies only to personal data we access when we install, support or maintain that installation.

You accept this DPA by entering into the Main Agreement. You do not need to sign it separately, but we will provide a signed copy if you would like one (see section 16).

02

Definitions

- **Data Protection Law** means the Data Protection (Jersey) Law 2018 and, where they apply to the processing, the EU General Data Protection Regulation and the UK GDPR, together with any law that replaces them.
- **Client Personal Data** means personal data that you, your users or people you invite put into Trellis, or that we otherwise process on your behalf in providing Trellis.

- **Sub-processor** means a third party we engage that processes Client Personal Data.
- **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data.
- *Controller*, *processor*, *data subject*, *personal data* and *processing* have the meanings given to them in Data Protection Law.

03

Roles and responsibilities

For Client Personal Data, you are the controller and we are your processor. You decide why and how that data is processed, and we act on your behalf.

We are a controller in our own right for the business information we need to run our relationship with you, such as contact details for invoicing and correspondence. Our Privacy & Data Protection notice covers that information, not this DPA.

You are responsible for having a lawful basis for the Client Personal Data you put into Trellis, and for giving the people it concerns any information Data Protection Law requires. Trellis is designed to work with aggregated, de-identified impact data. You should not upload special category data about identifiable individuals, such as health information, unless we have agreed it with you in writing first.

04

Details of the processing

- **Subject matter:** providing the Trellis impact-management platform and the consulting and support services around it.
- **Duration:** the term of the Main Agreement, plus the period in section 13 during which data is returned and deleted.
- **Nature and purpose:** hosting, storing, organising, analysing and reporting on your data in Trellis; generating summaries and insights with AI features you use; sending notification emails; and support, maintenance and backup.
- **Types of personal data:** names, email addresses, job titles and organisations of users and contacts; account and sign-in data; the content of documents, form responses, survey answers and notes that you or your users add; and technical records of how Trellis is used.
- **Data subjects:** your staff and other users you give access to Trellis; contacts at organisations you fund or work with; and people who respond to forms or requests you send through Trellis.

05

Our obligations

We will:

- process Client Personal Data only on your documented instructions, which are the Main Agreement, this DPA, your use and configuration of Trellis, and any further written instructions you give us, unless the law requires otherwise, in which case we will tell you first unless the law forbids it;
- tell you promptly if we think an instruction breaks Data Protection Law;
- make sure everyone who can access Client Personal Data is bound by a duty of confidentiality;
- keep in place the security measures described in section 9;
- engage sub-processors only as set out in section 7;
- help you respond to requests from data subjects, as set out in section 11;
- help you meet your obligations on security, breach notification, data protection impact assessments and consultation with the regulator, taking into account the nature of the processing and the information available to us;
- return or delete Client Personal Data when the Main Agreement ends, as set out in section 13; and
- make available the information you need to show that these obligations are met, as set out in section 12.

We will not sell Client Personal Data or use it for our own purposes. We may use aggregated, anonymised statistics derived from it to benchmark and improve our methods, provided no individual or organisation can be identified from them.

06

People with access

Derros consultants have administrative access to client workspaces in Trellis so they can deliver our services and support you. Engineers at our development partner, Blue Flame Digital Solutions Limited, can access Trellis systems to build, maintain and support the platform. Access is limited to people who need it for those purposes, and all of them are bound by confidentiality obligations.

07

Sub-processors

You authorise us to use the sub-processors listed below. We have a written agreement with each one that requires it to protect Client Personal Data to the standard Data Protection Law requires, and we remain responsible to you for its performance.

Hetzner Online GmbH / Hetzner Finland Oy

WHAT IT DOES WITH CLIENT DATA
Hosts the servers that run Trellis, including its database and search index, in Hetzner's ISO/IEC 27001 certified data centre in Helsinki.

LOCATION
Finland (EU)

Cloudflare, Inc.

WHAT IT DOES WITH CLIENT DATA
Routes and protects traffic to Trellis, and stores uploaded documents and encrypted database backups in its EU storage region.

LOCATION
Global network; storage in the EU

Blue Flame Digital Solutions Limited

WHAT IT DOES WITH CLIENT DATA
Our development partner. Builds, maintains and supports Trellis, and may access Client data when support or maintenance needs it.

LOCATION
Jersey

Google LLC

WHAT IT DOES WITH CLIENT DATA
Displays maps in Trellis (Google Maps, loaded in your browser), and holds our email and documents (Google Workspace) when you correspond with us.

LOCATION
USA / global

Postmark (Wildbit / ActiveCampaign)

WHAT IT DOES WITH CLIENT DATA
Sends the notification and account emails that Trellis generates.

LOCATION
USA

Anthropic, PBC

WHAT IT DOES WITH CLIENT DATA
Provides the Claude AI models behind Trellis's AI features, such as automatic document summaries. Content we send is not used to train its models.

LOCATION
USA

Functional Software, Inc. (Sentry)

WHAT IT DOES WITH CLIENT DATA
Records errors in Trellis so we can fix them. It is set up not to collect IP addresses or account details, although an error report can occasionally include data from the request that failed.

LOCATION
USA

List last updated: 18 September 2026.

We review our hosting and security providers regularly and may replace one when another offers stronger security. When we add or replace a sub-processor, we will update this list, and the date above, before the new sub-processor starts processing Client Personal Data. It is your responsibility to check this page for changes. If you have reasonable data protection grounds to object to a change, email us at hello@derros.com within 30 days of the update. We will discuss your concerns in good faith, and if we cannot resolve them you may end the part of the service that depends on that sub-processor.

08

Where data is held and transfers

Trellis runs on servers in Hetzner's data centre in Helsinki, Finland, and uploaded documents and database backups are stored in Cloudflare's EU storage region. Client Personal Data held in Trellis is therefore stored inside the European Union. Our Privacy & Data Protection notice describes the hosting in more detail.

Some sub-processors in the table above process data outside Jersey, the United Kingdom and the European Economic Area, for example when an AI feature sends a document to Anthropic for summarising. Where that happens, we rely on a transfer mechanism recognised by Data Protection Law, such as an adequacy decision, standard contractual clauses or an equivalent safeguard.

09

Security measures

We keep in place technical and organisational measures appropriate to the risk, which currently include the following. We may change them over time, but not in a way that lowers the overall level of protection.

HOSTING AND INFRASTRUCTURE

- Servers in an ISO/IEC 27001:2022 certified data centre in Helsinki, with controlled physical access, around-the-clock video surveillance and on-site staff.
- A network firewall and a host firewall that block all inbound connections from the internet, so the live service is reachable only through Cloudflare.
- Administrative access to the servers restricted to named Derros employees and development partners, using SSH keys over a private, encrypted network.
- A staging environment on the same server, under the same access controls, which may hold a copy of production data so that changes can be tested before release.

ENCRYPTION

- All traffic to the live Trellis service is encrypted with HTTPS, and it reaches our servers through an encrypted Cloudflare tunnel.
- Selected sensitive fields are encrypted in the database at application level.
- Uploaded documents are held in Cloudflare storage, which encrypts data at rest.
- Database backups are encrypted before they leave the server.

ACCESS CONTROL

- Each client's data is kept in its own workspace, and users see only the workspaces they belong to.
- Passwords are stored as salted hashes using a modern algorithm, must be at least 12 characters, and are checked against lists of common and breached passwords. Repeated failed sign-in attempts are slowed and then blocked.

- Two-factor authentication is available to every user and required for Derros staff and development partners, in Trellis and in every cloud service we use to run it.
- Staff and partner accounts are removed promptly when someone leaves, and administrator access is reviewed regularly.
- Changes to important records are logged, and the log is kept for 90 days.

RESILIENCE AND MONITORING

- Database backups every six hours and before every release, stored in Cloudflare's EU storage region and kept on a rolling schedule for up to 12 months.
- Uploaded documents are copied to the same backup store.
- Security updates that fix high-risk or critical vulnerabilities are installed within 14 days of release.
- Devices used for Derros work run supported software, are protected against malware and lock automatically when not in use.
- Error monitoring, set up not to collect IP addresses or account details, so that faults are found and fixed quickly.

10

Personal data breaches

If we become aware of a Personal Data Breach, we will tell you without undue delay and in any case within 48 hours. We will give you the information you need to meet your own obligations, as far as it is available to us: what happened, the categories and approximate number of data subjects and records affected, the likely consequences, and what we have done or propose to do about it. Where not all of that is available at once, we will send it as we learn it.

We will take reasonable steps to contain the breach and reduce its effects, and help you with any notification you make to the regulator or to the people affected. Telling you about a breach is not an admission of fault.

11

Data subject requests

If someone contacts us to exercise their rights over Client Personal Data, we will pass the request to you promptly and will not respond to it ourselves unless you ask us to. Trellis lets users export their own personal data and ask for their account to be deleted. Where you need more help to answer a request, we will provide it, taking into account the nature of the processing.

12

Information and audits

We will give you the information reasonably needed to show that we meet this DPA, including answers to reasonable security questionnaires and evidence of our hosting provider's certification.

If that information is not enough, you or an independent auditor you appoint may audit our compliance with this DPA. You must give us at least 30 days' written notice, carry out the audit during business hours in a way that does not disrupt our services or breach our confidentiality obligations to other clients, and bear its costs. Audits are limited to one a year, unless a regulator requires one or it follows a Personal Data Breach.

13

When the agreement ends

When the Main Agreement ends, you can ask us to return Client Personal Data to you in a commonly used format. Within 30 days of the end date, we will return or delete it, at your choice, and delete remaining copies from our live systems.

Copies in our encrypted database backups are deleted as those backups expire on their rolling schedule, within 12 months. Until then they stay encrypted, and we will not restore them except to recover from an incident. Copies of documents in our backup store are removed at the next backup run after the originals are deleted. We may keep Client Personal Data for longer only where the law requires us to, and this DPA continues to apply to it while we do.

14

Liability and governing law

Each party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability in the Main Agreement.

This DPA is governed by the law of Jersey, and the courts of Jersey have exclusive jurisdiction over any dispute arising from it.

15

Changes to this agreement

If we change this DPA, we will publish the new text here with a new version number and date. The version your Main Agreement refers to continues to apply to you until you agree to a newer one. Previous versions are available on request. Updates to the sub-processor list follow section 7 and do not create a new version.

16

Getting a signed copy

If your organisation needs a copy of this DPA signed by Derros, for your records or a supplier review, email hello@derros.com with your organisation's legal name and address and we will send one back.

NOTES

Questions about this document?

We would rather talk things through than hide behind small print. Get in touch and we will answer you directly.

hello@derros.com

OUR OTHER LEGAL DOCUMENTS

- Privacy & Data Protection
- Terms of Service
- Service Level Agreement
- Security

This handout reproduces the version published at derros.com/legal/data-processing-agreement on 18 September 2026. If the two differ, the online version applies. All our legal documents are at derros.com/legal.

Derros Ltd · registered in Jersey, company number 159837 · 3 Pinewood Close, La Rue Du Pont Marquet, St. Brelade, JE3 8DT, Jersey