Data Processing Agreement

Last updated: 28 October 2026

This Data Processing Agreement ("DPA") is entered into between you, the customer of Tailride (the "Controller"), and Tailride S.à r.l., a company organised under the laws of Luxembourg, with registered office at 6 rue M. Schnadt, L-2530 Luxembourg, RCS Luxembourg B303779, VAT LU37209474 (the "Processor", "Tailride", "we", "us"). This DPA forms part of the Tailride Terms of Service (the "Agreement") and applies whenever Tailride processes personal data on the Controller's behalf in connection with the service. Capitalised terms not defined here have the meaning given in the Agreement, in Regulation (EU) 2016/679 (the GDPR) and in the UK GDPR. The English version of this DPA is the controlling version; translations are provided for convenience only.

1. Definitions

In addition to terms defined in the Agreement, the following definitions apply:

• "Applicable Data Protection Law" means (i) Regulation (EU) 2016/679 (the GDPR), (ii) the UK Data Protection Act 2018 and the UK GDPR, (iii) the Swiss Federal Act on Data Protection, and (iv) any other privacy or data-protection law applicable to the Processing performed under the Agreement, in each case as amended from time to time.

• "Controller", "Processor", "Sub-processor", "Processing", "Personal Data", "Data Subject", "Special Categories of Personal Data" and "Supervisory Authority" have the meanings given in Applicable Data Protection Law.

• "EU SCCs" means the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, Module Two (controller-to-processor), as updated from time to time.

• "UK Addendum" means the International Data Transfer Addendum to the EU Commission SCCs issued by the UK Information Commissioner's Office (version B.1.0) under section 119A of the UK Data Protection Act 2018.

• "Personal Data Breach" has the meaning given in Article 4(12) GDPR.

• "Customer Personal Data" means Personal Data that Tailride processes on the Controller's behalf under the Agreement, as further described in Appendix 1.

2. Scope and roles

2.1 Roles. For Customer Personal Data, the Controller is the "controller" and Tailride is the "processor" within the meaning of Applicable Data Protection Law. For data Tailride collects independently (for example, the account and billing data described in our Privacy Policy), Tailride acts as an independent controller and that processing is governed by the Privacy Policy, not by this DPA.

2.2 Scope. This DPA applies to all Processing of Customer Personal Data carried out by Tailride and its Sub-processors under the Agreement.

2.3 Compliance. Each party will comply with its respective obligations under Applicable Data Protection Law. The Controller is responsible for the lawfulness of the data it submits to Tailride and for having a valid legal basis to instruct Tailride to process it.

2.4 No special categories without prior agreement. Tailride does not expect to receive special categories of Personal Data (Article 9 GDPR) or data relating to criminal convictions and offences (Article 10 GDPR). The Controller agrees not to upload such data unless expressly agreed in writing in advance.

3. Tailride's processing instructions

3.1 Documented instructions. Tailride will Process Customer Personal Data only on documented instructions from the Controller, including any configuration of the service performed by the Controller. The Agreement (this DPA, the Privacy Policy, the order/checkout, and the Controller's use of the service) constitutes the Controller's complete and final instructions to Tailride.

3.2 Additional instructions. Instructions that go beyond the scope of the service may be charged on a time-and-materials basis, subject to Tailride's prior acceptance.

3.3 Legal obligations. If a law of the European Union or a Member State (or other applicable law) requires Tailride to Process Customer Personal Data otherwise than as instructed, Tailride will notify the Controller of that legal requirement before such Processing, unless that law prohibits such notice on important grounds of public interest.

3.4 Unlawful instructions. If Tailride considers that an instruction infringes Applicable Data Protection Law, it will inform the Controller without undue delay and may suspend the relevant Processing until the Controller modifies its instruction.

4. Confidentiality

4.1 Confidentiality. Tailride ensures that all personnel authorised to Process Customer Personal Data are bound by appropriate confidentiality obligations (contractual or statutory) and receive appropriate data-protection training. Access to Customer Personal Data is limited to personnel who need such access for the purposes of the Agreement.

4.2 Contractors and remote access. Personnel within the meaning of clause 4.1 include individual contractors engaged by Tailride who work under Tailride's instructions, through accounts and systems that Tailride controls. Personnel may access Customer Personal Data remotely from outside the EEA. Where they do, Tailride ensures that the country is covered by an adequacy decision or that the EU SCCs are in place with the individual concerned, and Tailride remains responsible for its personnel as for its own acts.

4.3 Professional secrecy. Where the Controller is subject to a statutory duty of professional secrecy (in particular tax advisers, auditors and lawyers under § 203 of the German Criminal Code (StGB) and § 62a of the German Tax Advisory Act (StBerG), or equivalent rules in other jurisdictions), Tailride additionally ensures that (a) all personnel who may access Customer Personal Data are bound to confidentiality in text form and have been informed of the criminal consequences of unauthorised disclosure or exploitation under §§ 203 and 204 StGB before being granted access; (b) Sub-processors are bound to confidentiality in accordance with clause 6.4, and Tailride documents this and provides evidence to the Controller on justified request; (c) Tailride discloses protected secrets only where lawfully authorised or required by mandatory law and, where legally permitted, informs the Controller beforehand; and (d) these obligations survive termination of the Agreement without time limit. This clause does not by itself constitute client consent under § 62a(5) StBerG or establish comparable protection abroad under § 62a(4) StBerG; the Controller assesses those requirements on the basis of Appendix 3, its chosen AI processing region (clause 7.5) and information Tailride provides on request.

5. Security measures

5.1 Technical and organisational measures. Tailride implements and maintains the technical and organisational measures (TOMs) set out in Appendix 2 to ensure a level of security appropriate to the risk to the rights and freedoms of Data Subjects.

5.2 Assistance with security obligations. Taking into account the nature of the Processing and the information available to it, Tailride will assist the Controller, by appropriate technical and organisational measures and insofar as reasonably possible, in fulfilling its obligations under Articles 32 to 36 GDPR (security of processing, breach notification, data protection impact assessments and prior consultation).

5.3 Updates. Tailride may update its TOMs from time to time, provided that any update does not materially diminish the overall level of protection of Customer Personal Data.

6. Subprocessors

6.1 General authorisation. The Controller grants Tailride a general authorisation to engage Sub-processors to Process Customer Personal Data for the purposes set out in this DPA. The current list of Sub-processors is provided in Appendix 3 of this DPA.

6.2 Notice via the DPA page. Tailride keeps Appendix 3 of this DPA current and publishes any addition or replacement of a Sub-processor on this page. By accepting this DPA, the Controller agrees that publication of an updated Appendix 3 at https://tailride.so/dpa constitutes notice of changes for the purposes of Article 28(2) GDPR. Controllers who wish to receive email notifications of Sub-processor changes may opt in by writing to mikhail@tailride.so.

6.3 Right to object. The Controller may object in writing to a new Sub-processor on reasonable data-protection grounds within thirty (30) days of the change being published on this page. The parties will discuss the objection in good faith. If the parties cannot agree, the Controller may terminate the affected portion of the service at the end of its then-current billing period; Tailride is not obliged to refund fees already due for that billing period.

6.4 Flow-down of obligations. Tailride will impose on each Sub-processor data-protection obligations no less protective than those in this DPA (whether through a separately signed agreement or by accepting the Sub-processor's published Data Processing Agreement), and remains responsible to the Controller for each Sub-processor's compliance with this DPA as if its acts or omissions were Tailride's own.

7. International data transfers

7.1 Processing in the EEA. Tailride primarily Processes Customer Personal Data within the European Economic Area (EEA), including in Germany (Frankfurt), Sweden (Stockholm) and Ireland (Dublin).

7.2 Transfers outside the EEA / UK / Switzerland. Where Tailride or a Sub-processor transfers Customer Personal Data outside the EEA, the UK or Switzerland to a country that is not covered by an adequacy decision, Tailride will ensure that an appropriate transfer mechanism applies, which may include: (a) the EU SCCs (Module Two), which are incorporated by reference into this DPA and into our contracts with Sub-processors; (b) for transfers subject to the UK GDPR, the UK Addendum to the EU SCCs; (c) for transfers from Switzerland, the EU SCCs as adapted by the Swiss Federal Data Protection and Information Commissioner (FDPIC); and/or (d) any other lawful transfer mechanism, including the EU-US Data Privacy Framework (and its UK and Swiss extensions) where the importer is self-certified.

7.3 Annexes to the SCCs. The data exporter is the Controller; the data importer is Tailride S.à r.l. The information required by Annex I.A (List of Parties), Annex I.B (Description of transfer) and Annex II (Technical and organisational measures) of the EU SCCs is set out in Appendix 1 and Appendix 2 of this DPA. Annex III (List of Sub-processors) corresponds to Appendix 3.

7.4 Transfer impact. Tailride has assessed and will continue to assess the legal frameworks of the destination countries of its Sub-processors and has put in place supplementary measures (encryption, access controls, contractual safeguards, transparency on government requests) where appropriate.

7.5 AI processing region. The Controller chooses in the workspace settings where AI-based extraction of document data takes place: (a) "European Union": Tailride uses only the AI Sub-processors marked for the EU region in Appendix 3, which process data in the EU, and does not fall back to providers outside the EU; or (b) "Global": Tailride may also use the AI Sub-processors marked for the Global region in Appendix 3, which may process data outside the EEA (currently in the United States) under the safeguards in clause 7.2. The selected region is a documented instruction of the Controller under clause 3.1 and applies to documents processed after the setting is saved. During onboarding the region is pre-selected from the Controller's country ("European Union" for EEA countries, "Global" otherwise) and can be changed at any time in Settings; workspaces created before this setting existed use "Global" until it is changed.

8. Data subject requests

8.1 Assistance. Taking into account the nature of the Processing, Tailride will assist the Controller by appropriate technical and organisational measures, insofar as possible, in responding to requests from Data Subjects exercising their rights under Chapter III of the GDPR (right of access, rectification, erasure, restriction, data portability and objection).

8.2 Direct requests. If Tailride receives a request directly from a Data Subject relating to Customer Personal Data, Tailride will not respond to the request on substance unless the Controller has authorised it, and will instead inform the Controller of the request without undue delay.

8.3 Self-service. Many Data Subject requests can be handled directly by the Controller through the Tailride product (for example, deletion of individual records, export of data, or full account deletion from Settings).

9. Personal data breach notification

9.1 Notification. Tailride will notify the Controller of a confirmed Personal Data Breach affecting Customer Personal Data without undue delay after becoming aware of it, and in any event within seventy-two (72) hours.

9.2 Information. The notification will, to the extent reasonably available, describe (a) the nature of the breach, including the categories and approximate number of Data Subjects and records affected; (b) the likely consequences of the breach; and (c) the measures taken or proposed to address the breach and mitigate its possible adverse effects. Tailride will provide further information as it becomes available.

9.3 Cooperation. Tailride will reasonably cooperate with the Controller and provide reasonable assistance in the Controller's communications with Supervisory Authorities and affected Data Subjects.

10. DPIAs and prior consultations

Taking into account the nature of the Processing and the information available to it, Tailride will provide the Controller with reasonable assistance in carrying out data protection impact assessments under Article 35 GDPR and with any prior consultation with a Supervisory Authority under Article 36 GDPR, where required by Applicable Data Protection Law. Tailride will typically satisfy this obligation by making available this DPA, the current Sub-processor list (Appendix 3), the Technical and Organisational Measures (Appendix 2) and its standard security documentation. Bespoke assistance going beyond this — for example, completing a Controller-specific DPIA questionnaire or attending consultations with a Supervisory Authority — may be provided on a time-and-materials basis at Tailride's discretion.

11. Information and audits

11.1 Information. On reasonable written request, Tailride will make available to the Controller all information necessary to demonstrate compliance with this DPA and Article 28 GDPR, including, where applicable, summaries of independent security certifications, audit reports, penetration-test results and questionnaire responses, subject to reasonable confidentiality obligations.

11.2 Audits. Without prejudice to clause 11.1, the Controller (or an independent auditor mandated by it, subject to confidentiality and provided that the auditor is not a competitor of Tailride) may conduct on-site audits of Tailride's processing facilities no more than once per calendar year (save where required by a Supervisory Authority), on at least thirty (30) days' written notice, during regular business hours and without unreasonably disrupting Tailride's operations. The Controller bears its own costs for any audit; Tailride bears the cost of reasonable assistance up to a maximum of one (1) business day per calendar year per Controller, and may charge on a time-and-materials basis beyond that.

11.3 Cooperation with Supervisory Authority. Tailride will cooperate with any audit or investigation by a competent Supervisory Authority.

12. Return or deletion of personal data

12.1 Active-account retention. While the Controller's account remains active — including on a paused subscription, a free plan or an otherwise dormant state — Tailride retains Customer Personal Data so that the Controller can continue to access and use the service. The Controller may trigger deletion at any time from Settings > Delete account in the Tailride product.

12.2 Return or deletion on closure or termination. On closure of the Controller's account, or on termination or expiry of the Agreement (each, the "End Date"), and at the Controller's choice, Tailride will return or delete Customer Personal Data held on the Controller's behalf within ninety (90) days of the End Date. The default is deletion. For the avoidance of doubt, pausing a subscription, downgrading a plan or moving to a free plan does not constitute an End Date.

12.3 Self-service export. Before deletion, the Controller may export its data using the available product features. The Controller has at least thirty (30) days from the End Date to perform a self-service export.

12.4 Backups and legal retention. Tailride may retain Customer Personal Data (a) in encrypted backups, which are kept isolated from production systems and used solely for disaster-recovery purposes, for a limited period until the

backup is overwritten on the normal rolling backup retention cycle (currently up to twelve (12) months); and (b) where required to comply with applicable law (for example, accounting, tax or anti-fraud obligations). If Tailride restores from a backup that contains Customer Personal Data which had previously been deleted in accordance with this Section 12, Tailride will, without undue delay after the restore, re-apply the relevant deletion to the restored data. Any retained data remains subject to this DPA.

13. Liability

The aggregate liability of each party arising out of or relating to this DPA is subject to the limitations and exclusions of liability set out in the Agreement. Nothing in this DPA limits any rights or remedies that Data Subjects may have directly against the Controller or the Processor under Applicable Data Protection Law.

14. Governing law and jurisdiction

This DPA is governed by the laws of the Grand Duchy of Luxembourg, without prejudice to mandatory consumer-protection laws of the Controller's country of residence. The competent courts of the City of Luxembourg have exclusive jurisdiction, except where Applicable Data Protection Law provides otherwise (in particular for Data Subjects' rights, where the courts of the Data Subject's habitual residence may also have jurisdiction). For transfers governed by the EU SCCs or the UK Addendum, the governing law and forum set out in those clauses prevail for any matter falling within their scope.

15. Changes to this DPA

Tailride may update this DPA from time to time to reflect changes in Applicable Data Protection Law, changes to our services, or changes to our Sub-processor list. Material updates will be announced on this page with a new "Last updated" date, and any change that materially reduces the level of protection of Customer Personal Data will not take effect for an existing Controller for at least thirty (30) days after notice (unless required to take effect sooner by Applicable Data Protection Law). Previous versions of this DPA are archived at https://tailride.so/dpa/versions.

Appendix 1 — Details of processing (Annex I.B of the EU SCCs)

Data exporter (Controller). The Customer of Tailride, as identified by the account details, billing information and order/checkout submitted to Tailride. Role: controller.

Data importer (Processor). Tailride S.à r.l., 6 rue M. Schnadt, L-2530 Luxembourg, RCS Luxembourg B303779, VAT LU37209474. Privacy contact: mikhail@tailride.so. Role: processor.

Subject matter. The provision of the Tailride service as described in the Agreement: capture, OCR, AI-based structured extraction, organisation, storage, search, sharing and onward export of invoices, receipts and related business documents, plus related customer support.

Duration. The duration of the Agreement, plus any retention period required for backup rotation or legal obligations (see clause 12).

Nature and purpose of processing. Hosting, OCR and AI-based extraction, indexing, search, deduplication, sharing, exporting and integration of financial documents on the Controller's instructions; provision of related customer support and account/billing operations.

Categories of Data Subjects.
• The Controller's authorised users (admins, accountants, team members);
• The Controller's customers, suppliers and counterparties whose names appear on invoices, receipts and related documents;
• Any other natural persons whose Personal Data appears in documents the Controller chooses to upload or connect.

Categories of Personal Data.
• Identification data: full name, business email address, postal address, VAT/tax IDs, phone numbers where present in documents.
• Account data: name, email, hashed authentication credentials, language preference, role.
• Transaction data: invoice numbers, dates, line items, amounts, currencies, payment status.

• Connection data: OAuth tokens for connected mailboxes, cloud-storage providers and accounting systems (stored encrypted at rest).
• Technical data: IP address, browser/device identifiers, time stamps, application logs.
• Content data: text and images contained in uploaded or fetched documents.

Special categories of Personal Data. None expected. The Controller agrees not to upload special categories of Personal Data unless agreed in writing in advance.

Frequency of transfer. On a continuous basis for the duration of the Agreement.

Competent supervisory authority. The Commission nationale pour la protection des données (CNPD), Luxembourg, for transfers governed by the EU SCCs where Tailride is the data importer.

Appendix 2 — Technical and organisational measures (Annex II of the EU SCCs)

Tailride implements the following technical and organisational measures to ensure a level of security appropriate to the risk. The measures may be updated from time to time, provided that the overall level of protection is not reduced.

A. Organisational measures
• Documented information-security policies covering acceptable use, access management, incident response, change management and vendor management.
• Annual review of security policies and roles.
• Personnel are subject to written confidentiality obligations.
• Access to production systems is granted on a need-to-know, least-privilege basis and reviewed at least annually.
• Documented incident-response plan including roles, communication paths and post-mortem requirements.

B. Access control
• Single sign-on for internal systems where possible.
• Multi-factor authentication required for production access and for privileged developer accounts.
• Personal accounts for production access; no shared credentials.
• Time-bound access tokens; revocation on role change or departure.

C. Encryption
• TLS 1.2 or above for data in transit between client and Tailride and between Tailride and its Sub-processors.
• Encryption at rest for the production database and object storage (AES-256 or equivalent).
• Encryption at rest of OAuth tokens for connected third-party accounts.

D. Network and hosting
• Production hosted on Vercel (EU compute region: Frankfurt) and on managed cloud services (AWS EU regions, MongoDB Atlas EU region, Upstash EU region).
• Logical segregation of customer data via tenant identifiers.
• WAF/CDN-level protections at the edge.
• Sub-processors with industry-standard certifications (ISO 27001, SOC 2 Type II) preferred for critical infrastructure.

E. Operations
• Centralised logging for security-relevant events; logs retained for at least 30 days.
• Vulnerability management programme (dependency scanning, automated patch rollouts).
• Daily encrypted backups of the production database, with point-in-time recovery on a rolling 7- to 35-day window and full snapshot retention of up to twelve (12) months; backups are kept isolated from production systems and used solely for disaster recovery.
• Recovery testing on a periodic basis.

F. Software development
• Source code stored in private repositories with mandatory code review for production branches.
• Separation of development, staging and production environments.
• Secrets stored in a managed secret store; no secrets in source code.
• Automated tests as part of the CI pipeline.

G. Vendor management

• Sub-processors selected on the basis of security, compliance and business criticality.
• Data-processing agreements with all Sub-processors that Process Customer Personal Data.
• Transfer mechanisms (EU SCCs / UK Addendum / DPF) in place where required.

H. Data subject support
• Built-in self-service deletion of accounts and individual records.
• Documented process for handling Data Subject requests received indirectly via the Controller.

Appendix 3 — List of Sub-processors (Annex III of the EU SCCs)

Tailride engages the following Sub-processors to provide the service. This page is the authoritative list of Sub-processors and is kept current; any addition or replacement is published here in accordance with clause 6. Entries marked as user-enabled are only used if the Controller activates the relevant integration. Entries marked "Planned" are not yet active and are listed for transparency; they will start Processing Customer Personal Data only when the relevant feature is enabled.

Vercel Inc.
Purpose: Web hosting, edge compute, cron jobs and CDN.
Legal entity: Vercel Inc., 340 S Lemon Ave #4133, Walnut, CA 91789, USA
Region of processing: EU (Frankfurt / fra1) compute, global CDN
Transfer safeguards: EU SCCs + EU-U.S. DPF

Amazon Web Services EMEA SARL
Purpose: Object storage of uploaded documents (Amazon S3) and OCR extraction (Amazon Textract).
Legal entity: AWS EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg
Region of processing: EU (eu-central-1 Frankfurt / eu-north-1 Stockholm)
Transfer safeguards: EU SCCs (AWS DPA) + EU-U.S. DPF

MongoDB, Inc.
Purpose: Managed application database (MongoDB Atlas).
Legal entity: MongoDB, Inc., 1633 Broadway 38th Fl, New York, NY 10019, USA
Region of processing: EU (Atlas EU region)
Transfer safeguards: EU SCCs + EU-U.S. DPF

Upstash, Inc.
Purpose: Asynchronous job queue (QStash) for OCR, sync and export tasks.
Legal entity: Upstash, Inc., 350 California Street, Suite 600, San Francisco, CA 94104, USA
Region of processing: EU (eu-central-1)
Transfer safeguards: EU SCCs

Google Ireland Limited (Cloud Run)
Purpose: Internal backend microservice hosted on Google Cloud Run.
Legal entity: Google Ireland Ltd, Gordon House, Barrow Street, Dublin 4, Ireland
Region of processing: EU (europe-west3 Frankfurt)
Transfer safeguards: Within EEA + EU SCCs / DPF for onward US transfers

Hetzner Online GmbH
Purpose: Cloud hosting for the background worker and the Gotenberg PDF rendering service.
Legal entity: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany
Region of processing: EU (eu-central, Helsinki, Finland)
Transfer safeguards: Within EEA + Hetzner DPA

Resend, Inc.
Purpose: Transactional email (sign-up, password reset, receipts, product notifications).
Legal entity: Resend, Inc., 2261 Market Street #5039, San Francisco, CA 94114, USA
Region of processing: US
Transfer safeguards: EU SCCs

Crisp IM SAS
Purpose: Live chat support — Controllers may share screenshots and details of their workspace data when contacting support.
Legal entity: Crisp IM SAS, 2 boulevard de Launay, 44100 Nantes, France
Region of processing: EU (France)
Transfer safeguards: Within EEA

OpenAI, LLC
Purpose: Invoice text extraction.
Legal entity: OpenAI, LLC, 3180 18th Street, San Francisco, CA 94110, USA
Region of processing: US. AI region: Global only (fallback provider)
Transfer safeguards: EU SCCs (OpenAI EU DPA); zero-retention API mode

Microsoft Ireland Operations Ltd (Azure OpenAI / AI Vision)
Purpose: OCR and document understanding via Azure OpenAI / Azure AI Vision.
Legal entity: Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
Region of processing: EU (Azure EU Data Zone). AI region: EU (fallback provider)
Transfer safeguards: Within EEA + EU SCCs / DPF for onward US transfers

Google Ireland Limited (Gemini API / Vertex AI)
Purpose: Invoice extraction via the Google Gemini API.
Legal entity: Google Ireland Ltd, Gordon House, Barrow Street, Dublin 4, Ireland
Region of processing: AI region EU: Gemini on Vertex AI, EU multi-region. AI region Global: Gemini API on global Google AI infrastructure, including the US
Transfer safeguards: AI region EU: within EEA. AI region Global: EU SCCs + EU-U.S. DPF

This list covers Sub-processors that Process Customer Personal Data on Tailride's behalf within the meaning of Article 28 GDPR. The following categories of third parties are intentionally not included in this list because Tailride does not engage them as Article 28 Sub-processors:

(i) Payment partners (for example Stripe, and where applicable Paddle as planned future Merchant of Record): these providers act as independent data controllers for the payment data they process under their own legal and regulatory obligations (PCI-DSS, anti-money-laundering, fraud prevention). They are described in the Privacy Policy.

(ii) Web and product analytics partners (for example Google Tag Manager, Google Analytics 4, DataFast): Tailride determines what to measure on its public website and product, so Tailride acts as a controller (and, with the analytics provider, in a joint or independent-controller arrangement). These tools are loaded subject to cookie consent and are described in the Privacy Policy.

(iii) Advertising partners (for example Meta Pixel and Conversions API, and Google Ads as a planned future addition): Tailride and the advertising platform act as joint or independent controllers for ad measurement and conversion data. They are loaded subject to cookie consent and described in the Privacy Policy.

(iv) Affiliate-marketing partners (for example Affonso): Tailride uses affiliate-attribution events for its own marketing; the affiliate provider acts as an independent controller for the data it receives. Described in the Privacy Policy.

(v) Anti-fraud and account-creation checks (for example UserCheck disposable-email-domain check): Tailride performs these checks for its own legitimate interest in fraud prevention; the check provider acts as a controller for the email-domain data it receives. Described in the Privacy Policy.

(vi) Ancillary service providers that do not Process Customer Personal Data (for example currency-rate APIs and vendor-logo lookup services such as Brandfetch, which only receive a vendor domain name).

(vii) User-enabled integrations, communication channels and destinations. If the Controller connects or uses Google Drive / Gmail / Sheets, Microsoft 365 / OneDrive / Outlook, QuickBooks Online, Xero, Microsoft Dynamics 365 Business Central, Odoo, IMAP/SMTP servers, WhatsApp Cloud API, Telegram Bot API, or custom webhooks, or if documents are submitted through browser upload or email chosen by the Controller or Data Subject, Tailride transmits or receives Customer Personal Data through that channel only on the Controller's instruction or the relevant Data Subject's action. The third-party account, browser, email service, messaging channel or destination is

selected, configured or used by the Controller or the relevant Data Subject and operates under that party's separate relationship with the relevant provider. These channels and destinations are not Tailride Article 28 Sub-processors.

How this DPA becomes binding

This DPA forms part of the Tailride Terms of Service. By accepting the Terms of Service (for example, when registering for the service or maintaining an active subscription), the Controller agrees to be bound by this DPA and incorporates by reference the EU SCCs (Module Two, controller-to-processor) and, where applicable, the UK Addendum, with Tailride S.à r.l. as the data importer and the Controller as the data exporter.

Customers requiring a counter-signed copy of this DPA on Tailride's letterhead — for example for procurement records — can request one at mikhail@tailride.so. Tailride may sign a substantially similar DPA proposed by the Controller subject to commercial review.

Contact

Privacy and data-protection contact: mikhail@tailride.so

Postal address:
Tailride S.à r.l.
6 rue M. Schnadt
L-2530 Luxembourg
Grand Duchy of Luxembourg

Competent supervisory authority (where Tailride acts as data importer under the EU SCCs):
Commission nationale pour la protection des données (CNPD)
15, boulevard du Jazz
L-4370 Belvaux
Grand Duchy of Luxembourg
https://cnpd.public.lu

Signatures

This DPA is binding on acceptance of the Tailride Terms of Service. Tailride has signed this copy in advance. The Customer does not need to sign or return it; the Customer block below may be completed for the Customer's own records.

For Tailride S.à r.l. (Processor)

Name	Mikhail Erman
Title	Gérant (Managing Director)
Date	28 October 2026
Signature	Signed electronically by Mikhail Erman

For the Customer (Controller), optional

Company	_____
Name	_____
Title	_____
Date	_____
Signature	_____