Nordath Data Processing Agreement

Version 2.0 - November 2026

1. Parties and scope

This Data Processing Agreement ("DPA") is between the customer that uses Steward (the "Controller") and Nordath, the trade name of Romain Compagnon, an individual entrepreneur (EI) whose business address is a domiciliation address at 173 rue de Courcelles, 75017 Paris, France (the "Processor"). Contact: dpo@nordath.com.

It forms part of the Terms of Use and Sale and applies from the moment the Controller sends files to Steward, through the API or by upload. It implements Article 28 of Regulation (EU) 2016/679 (GDPR). For Nordath's own processing of website, account, billing and support data, Nordath is a controller, as set out on the GDPR Compliance page, and this DPA does not apply.

2. Subject matter, nature and purpose

The Processor provides Steward, which checks whether images, audio and video files carry valid machine-readable labels (C2PA manifests) and produces per-file verdicts and an Evidence File. On the Controller's behalf, the Processor receives the files the Controller sends, reads each file's label, checks its signature and the file's integrity, and records the verdict and what the label claims.

Files are checked and released: the Processor does not modify them and does not keep them beyond processing. The Processor processes this data only to deliver those functions and not for its own purposes, and does not use the files or their content to train models.

3. Duration

This DPA lasts as long as the Controller has an account and the Processor holds the Controller's personal data, including the deletion period in section 11.

4. Categories of data and data subjects

Data subjects: people whose likeness or voice appears in the files the Controller sends, and people named in a label (for example a creator or an author).

Data: the content of the files during processing (images, audio, video and their metadata, including the label), and, in the Evidence File and the verdicts, the verdict per file and the claims the label makes. No special categories of data are intended; the Controller should not send files that reveal them.

5. Instructions

The Processor processes personal data only on the Controller's documented instructions, which are these Terms, this DPA and the Controller's use of Steward's features, unless Union or Member State law requires otherwise, in which case it informs the Controller beforehand unless the law forbids it. The Processor informs the Controller if it considers an instruction to infringe data protection law.

The Controller decides what to send and why, and is responsible for having a lawful basis for sending it.

6. Confidentiality

The Processor ensures that everyone authorised to process the data is bound by a duty of confidentiality and accesses it only as needed to run and support Steward.

7. Security

The Processor applies the technical and organisational measures in Annex II, appropriate to the risk, and reviews them as the service changes.

8. Sub-processors

The Controller gives general authorisation for the sub-processors in Annex III. The Processor publishes the current list on its GDPR Compliance page and updates it there before a new sub-processor starts processing the Controller's data. The Controller may object on reasonable data protection grounds within 30 days by writing to dpo@nordath.com; if the parties cannot resolve the objection, the Controller may terminate the affected subscription.

The Processor imposes on each sub-processor data protection obligations no less protective than this DPA and remains liable to the Controller for the sub-processor's performance.

9. Assistance

Taking into account the nature of the processing, the Processor assists the Controller by appropriate measures in answering data subject requests (access, rectification, erasure, restriction, portability, objection), and in meeting its obligations on security, breach notification, impact assessments and prior consultation. A person who writes to the Processor directly about the Controller's data is told which Controller to contact, and the Processor passes the request or objection on to that Controller.

10. Personal data breaches

The Processor notifies the Controller without undue delay, and where feasible within 72 hours, after becoming aware of a personal data breach affecting the Controller's data, with the information it then has: the nature of the breach, the data and approximate number of data subjects concerned, likely consequences, and measures taken or proposed.

11. Return and deletion

Files are released as soon as they are checked. Evidence Files and verification results are kept for the retention period of the Controller's offer and then deleted; the Controller can download its Evidence Files at any time during that period. The Processor deletes or anonymises the rest of the Controller's account data after the account is closed, within 90 days, unless Union or Member State law requires it to keep it. Backups are overwritten in the normal course of their rotation, within 6 months.

12. Audits

The Processor makes available the information necessary to show compliance with Article 28 and allows for audits by the Controller or an auditor it appoints, on at least 30 days' written notice, during business hours, no more than once a year unless a breach or a supervisory authority requires otherwise, subject to confidentiality and without access to other customers' data. The Controller bears the cost of the audit.

13. International transfers

The Processor's database is hosted in the EU. Where a sub-processor processes personal data outside the EEA, the transfer relies on an adequacy decision (for example the EU-US Data Privacy Framework where the sub-processor is certified) or on the European Commission's Standard Contractual Clauses, with the UK and Swiss addenda where relevant.

14. Liability, governing law

Each party's liability under this DPA is subject to the limitations in the Terms, without prejudice to data subjects' rights and to liability that cannot be limited by law. This DPA is governed by French law and the jurisdiction clause of the Terms applies.

Annex I - Processing details

Controller: the Steward customer named on its account. Processor: Nordath (see section 1). Data protection contact: dpo@nordath.com.

Frequency: continuous while the account is active. Retention: as in section 11. Competent supervisory authority: the Controller's own; for the Processor, the CNIL (France).

Annex II - Technical and organisational measures

- Files checked and released, never modified, not kept beyond processing.
- Encryption of data in transit; storage in the EU.
- Role-based access inside each customer organisation; staff tools sit behind Cloudflare Access.
- API keys managed and revocable by the Controller.
- Analytics only with consent, without cookies, with form inputs masked.
- Bot protection and rate limiting on public forms and APIs.
- Responsible disclosure policy (Security Policy page) and a security contact at security@nordath.com.

Annex III - Sub-processors (November 2026)

- Railway: application hosting and database (EU region).
- Cloudflare: network delivery, security, bot protection and staff access control (global network).
- Stripe: payments (Ireland).
- Resend: transactional email (Ireland).
- PostHog: analytics (EU hosting), only with consent.
- Google: Gemini model for the chat assistant; Google sign-in (United States).
- Microsoft: Microsoft sign-in (United States).
- The email provider hosting the mailbox that receives contact-form messages.