Data Processing Agreement

For organizations that use Missa. It is part of the Terms, so you don't need to sign anything. Version of 10 November 2026.

1. Who this agreement is between

This Data Processing Agreement ("DPA") is between Content Systems Lab, Inc. ("Missa", "we") and the organization that uses Missa to run calls, read submissions, pay writers or send a newsletter (the "organization", "you").

It forms part of the Missa Terms. It applies from the day the organization starts using Missa and lasts as long as Missa processes organization data. No signature is needed. If this DPA and the Terms disagree about personal data, this DPA wins.

2. Roles

For organization data, the organization is the controller and Missa is its processor (a "service provider" under the CCPA). In this DPA, organization data means the personal data the organization collects or keeps through Missa: submissions and the details sent with them, readers' notes and decisions, contracts and payout details, messages, members of its team, and its newsletter subscribers.

Missa is a controller of its own account data, such as a writer's Missa account, saved calls and portfolio. The Privacy notice covers that data, not this DPA.

3. What Missa does with organization data

Missa processes organization data only to provide Missa to the organization, following the organization's documented instructions. The Terms, this DPA and the organization's own use of Missa's features are those instructions. If an instruction would break data protection law, Missa will tell the organization.

Missa does not sell organization data, share it for advertising, or use it for any purpose of its own. Missa does not use AI to read or change writers' submissions or other writing.

4. Details of the processing

- Subject matter and duration: providing Missa, for as long as the organization uses it, then until deletion under section 10.
- Nature and purpose: storing, organizing, showing, sending and deleting data so the organization can take submissions, read and decide on them, sign contracts, pay writers, and email its subscribers.
- People the data is about: people who submit or apply, the organization's readers, editors and other team members, writers it pays, and its newsletter subscribers.
- Kinds of data: names, email addresses, the details in a submission form, uploaded files and writing, notes and decisions, contract and payment status, payout details, and newsletter sign-up and consent records. Card numbers are handled by the payment provider, never by Missa.
- Special category data: only what a person chooses to include in a submission or an organization chooses to ask for. The organization is responsible for having a lawful basis for it.

5. Confidentiality and security

Everyone at Missa who can reach organization data is bound to keep it confidential and reaches it only as their work needs.

Missa keeps the measures in Annex 2 in place and may improve them, but will not make them weaker overall.

6. Sub-processors

The organization allows Missa to use the sub-processors listed in Annex 1. Missa puts each one under written terms that protect organization data at least as well as this DPA, and stays responsible for them.

Before adding or replacing a sub-processor, Missa will update Annex 1 and tell the organization's owners by email at least 30 days ahead. The organization may object for a reasonable data protection reason by writing to hello@usemissa.com within that time. We will then work in good faith on a fix. If there isn't one, the organization may stop using the affected feature, or cancel its plan and get a refund of any prepaid amount for the time left.

7. Helping the organization

Missa's features let the organization find, export, correct and delete organization data, so it can answer people who ask to access, correct, delete or move their data. If a person asks Missa directly about organization data, Missa will pass the request on and will not answer it without the organization's say.

Missa will also give reasonable help with data protection impact assessments and with questions from a data protection authority, as far as they concern Missa's processing.

8. Personal data breaches

If Missa becomes aware of a breach of security that leads to organization data being lost, changed, disclosed or reached without permission, Missa will tell the organization's owners without undue delay, and within 48 hours. Missa will share what it knows, what it is doing about it, and updates as it learns more, and will take reasonable steps to limit the harm.

9. International transfers

Missa and its sub-processors may process organization data outside the country where the organization or the people concerned are, including in the United States.

Where the GDPR applies to such a transfer, the European Commission's Standard Contractual Clauses (2021/914), Module 2 or Module 3 as fits, form part of this DPA,

with the organization as data exporter and Missa as data importer, the optional clause 7 left out, option 2 (general authorization) in clause 9 with the notice period in section 6, the Irish law and courts in clauses 17 and 18, and the Annexes of this DPA as their Annexes. Where the UK GDPR applies, the UK Addendum to those Clauses also applies. For Switzerland, the Clauses apply with references to the Swiss law. Where Nigeria's NDPA applies, these same safeguards are the adequate protection it asks for.

10. When the organization leaves

The organization can export its submissions at any time from Settings. When it asks Missa to delete its organization, by writing to hello@usemissa.com, Missa deletes organization data within 30 days, except where the law requires Missa to keep it, such as billing records. Copies in backups are deleted as those backups expire on their normal cycle and are not used in the meantime.

11. Checks

Missa will give the organization the information needed to show it meets this DPA. If that isn't enough, the organization may ask for an audit with 30 days' written notice to hello@usemissa.com, at most once a year unless a breach or an authority calls for more. Audits happen in working hours, keep other customers' data confidential, and are at the organization's cost.

12. Liability and changes

Each party's liability under this DPA follows the limits in the Terms, except where the law does not allow it.

Missa may update this DPA to follow changes in the law or in its sub-processors. It will not lower the protection of organization data without the organization's agreement. Missa will tell the organization's owners about a material change before it takes effect.

Annex 1. Sub-processors

- Amazon Web Services: Hosting, background jobs, file storage with malware scanning, and sending newsletters.

- Neon: The database.
- Cloudflare: Delivering Missa quickly and protecting it from attacks.
- Resend: Sending account and submission emails.
- Stripe: Plan payments, and entry fees taken into the organization's own Stripe account.
- Bachs: Entry fees and payouts, where the organization chooses it.
- Upstash: Rate limits and short-lived usage counts.
- Sentry: Error reports, with personal details removed where possible.
- PostHog: Product analytics, only for people who accept them.

Annex 2. Security measures

- Data is encrypted in transit with TLS, and stored data is encrypted at rest by the hosting and database providers.
- Uploaded files are kept in private storage, reached only through short-lived links for people allowed to see them, and scanned for malware before anyone can open them.
- Passwords are stored only as hashes. Credentials for connected services are encrypted.
- Every request is checked against the person's role in the organization, and reads are limited to the organization's own data.
- Production access is limited to the people who run Missa and protected with two-step verification.
- The database is backed up, and backups can be restored to a point in time.
- Logging in and signing up are rate limited, and errors are reported with personal details removed where possible.

Questions about this agreement: hello@usemissa.com. See also the Privacy notice.