Data Processing Addendum

EmailFlow AI — emailflow.ai — the authoritative current version of this document lives at https://emailflow.ai/legal/dpa

Version 1.0 — July 6, 2026

This Data Processing Addendum ("DPA") forms part of the agreement between EmailFlow AI ("Processor", "we", "us") and the customer identified in the applicable account or order ("Customer", "Controller", "you") governing the Customer's use of the EmailFlow AI services (the "Agreement"). It reflects the parties' agreement on the processing of personal data under the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR, and comparable data protection laws (together, "Data Protection Laws").

1. Definitions

- "Personal Data", "processing", "controller", "processor", "data subject", and "supervisory authority" have the meanings given in the GDPR.
- "Customer Data" means the personal data the Customer submits to the service for processing — in particular subscriber and contact records (email addresses, names, custom fields, tags, segmentation attributes) and the email engagement data generated by sending to them.
- "Sub-processor" means a third party engaged by the Processor to process Customer Data on the Customer's behalf.
- "Standard Contractual Clauses" or "SCCs" means the clauses approved by European Commission Implementing Decision (EU) 2021/914, and, for UK transfers, the UK International Data Transfer Addendum.

2. Roles and scope

For Customer Data, the Customer is the controller and EmailFlow AI is the processor. For the Customer's own account data (registration, billing, usage), EmailFlow AI is an independent controller and its Privacy Policy applies; that processing is outside the scope of this DPA. This DPA applies to all processing of Customer Data by the Processor for the duration of the Agreement.

3. Details of processing (Annex I)

- **Subject matter:** provision of the EmailFlow AI email marketing platform — contact storage and management, campaign and automation sending, analytics, and related AI-assisted features.
- **Duration:** the term of the Agreement, plus the deletion period in Section 10.
- **Nature and purpose:** hosting, storage, transmission (email delivery), verification, analytics computation, and display of Customer Data as configured by the Customer through the service and its APIs.
- **Categories of data subjects:** the Customer's subscribers, contacts, and email recipients; the Customer's own team members using the account.
- **Categories of personal data:** email addresses; names; any custom fields, tags, and attributes the Customer chooses to store; IP-derived and device-derived engagement data (opens, clicks, bounces, unsubscribes, complaints).
- **Special categories:** the service is not designed for and must not be used to process special categories of data (Article 9 GDPR).

4. Processor obligations

The Processor shall:

- process Customer Data only on the Customer's documented instructions — given through the service's settings, features, and APIs, and through the Agreement — unless required to do otherwise by law, in which case the Processor will inform the Customer unless legally prohibited;
- ensure that persons authorized to process Customer Data are bound by confidentiality obligations;
- implement and maintain the technical and organizational measures described in Annex II;
- not sell Customer Data, and not use it for advertising, profiling, or its own purposes;
- not use Customer Data to train third-party AI foundation models, and contractually require its AI sub-processors not to use inputs or outputs for model training except as necessary to provide the requested feature;
- inform the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Laws.

5. Sub-processors

The Customer grants the Processor general written authorization to engage Sub-processors for the processing activities described in Annex I. The current complete list — with each Sub-processor's purpose, location, and data protection terms — is published at emailflow.ai/legal/subprocessors and is kept accurate by an automated check against the Processor's codebase. The Processor will update that page before engaging a new Sub-processor. The Customer may object on reasonable data-protection grounds within 30 days of a change by contacting privacy@emailflow.ai; if the objection cannot be resolved, the Customer may terminate the affected services. The Processor imposes data protection obligations on each Sub-processor materially equivalent to those in this DPA and remains liable for their performance.

6. Assistance to the Controller

Taking into account the nature of the processing, the Processor shall assist the Customer by appropriate technical and organizational measures in fulfilling data subject requests (access, rectification, erasure, restriction, portability, objection) — primarily through the service's built-in export, edit, delete, and unsubscribe features — and shall assist the Customer in ensuring compliance with Articles 32 to 36 GDPR (security, breach notification, impact assessments, prior consultation), taking into account the information available to the Processor. If a data subject contacts the Processor directly regarding Customer Data, the Processor will refer the request to the Customer without undue delay.

7. Personal data breach

The Processor shall notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Data, and shall provide the information reasonably required for the Customer to meet its own breach notification obligations, including the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed.

8. Security (Annex II)

The Processor implements and maintains, as a minimum, the following technical and organizational measures:

- **Encryption in transit:** all application traffic over HTTPS/TLS; automatically issued and renewed certificates for customer tracking domains.
- **Encryption and hashing at rest:** integration and connected-account credentials encrypted with AES-256 application-level encryption; passwords stored as salted bcrypt hashes; API keys stored as SHA-256 digests only.
- **Hosting:** application and database on a dedicated server in an ISO 27001-certified data center region operated by Hetzner Online GmbH in Falkenstein, Germany (EU); email delivery via Amazon SES.

- **Access control:** two-factor authentication available on all accounts; scoped API keys with per-key revocation and rate limits; the application runs as an unprivileged service user; production access restricted to the operations team.
- **Payment isolation:** card data is collected and stored exclusively by the PCI-DSS Level 1 payment processor and never touches the Processor's servers.
- **Integrity of deployment:** automated multi-layer test suites gate every release; atomic deploys with retained previous releases and immediate rollback.
- **Monitoring:** continuous health snapshots (services, queues, failed jobs, host resources) with alerting; automated processing of bounce and complaint feedback streams.
- **Retention hygiene:** scheduled purges of operational logs (API idempotency records after 24 hours; webhook delivery and raw API usage logs after 30 days; trigger event fire logs after 90 days; transactional message records after 13 months).

9. International transfers

Customer Data is hosted in the EU. Where processing by a Sub-processor involves a transfer of personal data outside the EEA or UK to a country without an adequacy decision, the Processor ensures the transfer is protected by appropriate safeguards under Data Protection Laws — the Standard Contractual Clauses (and UK Addendum) incorporated into the Sub-processor's data protection terms, or the Sub-processor's certification under the EU-U.S. Data Privacy Framework, where applicable. The per-vendor terms are linked from the subprocessors page.

10. Deletion and return

The Customer can delete Customer Data at any time through the service and its APIs; deletion is immediate in the live database. Upon termination of the Agreement, the Processor shall, at the Customer's choice, delete or return all Customer Data within a commercially reasonable period, and delete existing copies unless storage is required by law. Data held by Sub-processors is deleted through the same instruction chain.

11. Audit and information

The Processor shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA — including this document, the published subprocessors page, and the published security description — and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, on reasonable notice, no more than once annually unless required by a supervisory authority, and subject to reasonable confidentiality obligations.

12. Liability and order of precedence

Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement. In case of conflict between this DPA and the Agreement regarding the processing of Customer Data, this DPA prevails; in case of conflict between this DPA and the Standard Contractual Clauses, the SCCs prevail.

13. Contact

Data protection questions, signature requests for a countersigned copy, and Sub-processor objections: privacy@emailflow.ai (data protection contact: dpo@emailflow.ai).
