DATA PROCESSING AGREEMENT

Data Processing Agreement

This Data Processing Agreement (**"DPA"**) forms part of and is incorporated into the Spreeflo Terms of Service or other written agreement between the parties governing Customer's use of the Services (the **"Agreement"**), and is entered into between:

(1) Spreeflo Ltd, a company registered in England and Wales under company number 16068434, whose registered office is at 405 Baltic Quay, 1 Sweden Gate, London, England, SE16 7TJ (**"Spreeflo"**, the **"Processor"**); and

(2) the Customer identified in the Agreement (**"Customer"**, the **"Controller"**).

Each a **"party"** and together the **"parties"**.

Effective date: the date Customer accepts this DPA or the Agreement, whichever is earlier.

---

1. Definitions

1.1 **"Data Protection Law"** means, as applicable to the processing: (a) Regulation (EU) 2016/679 (**"EU GDPR"**); (b) the EU GDPR as incorporated into UK law by the European Union (Withdrawal) Act 2018, together with the Data Protection Act 2018 and the Data (Use and Access) Act 2025 (**"UK GDPR"**); (c) Directive 2002/58/EC and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**"PECR"**); and (d) any other applicable data protection or privacy law, in each case as amended or replaced.

1.2 **"Customer Personal Data"** means personal data contained within Customer Data that Spreeflo processes on Customer's behalf in providing the Services.

1.3 **"Customer Data"** means all data Customer or Customer's end users submit to, or that is collected through, the Services, including contact records, contact attributes, behavioural and web analytics events, form responses, web push subscriptions, and message engagement data.

1.4 **"EU SCCs"** means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914.

1.5 **"Services"** means the Spreeflo marketing automation platform and any related services provided under the Agreement.

1.6 **"Subprocessor"** means any processor engaged by Spreeflo to process Customer Personal Data.

1.7 **"UK Addendum"** means the International Data Transfer Addendum to the EU SCCs issued by the Information Commissioner under s.119A of the Data Protection Act 2018.

1.8 The terms **“controller”**, **“processor”**, **“data subject”**, **“personal data”**, **“personal data breach”**, **“processing”** and **“supervisory authority”** have the meanings given in the EU GDPR.

2. Roles of the parties and scope

2.1 The parties acknowledge that in respect of Customer Personal Data, Customer is the **controller** and Spreeflo is the **processor**.

2.2 Where Customer is itself a processor acting on behalf of a third-party controller, Customer warrants that it has the necessary authority from that controller to enter into this DPA and to instruct Spreeflo, and Spreeflo acts as a subprocessor. In that case, references to Customer’s obligations as controller are to be read as obligations to procure the equivalent from its controller.

2.3 Spreeflo acts as an independent **controller** in respect of: account registration and administration data relating to Customer’s own users; billing and payment data; support correspondence; security and audit logs; and aggregated, de-identified service statistics used to operate, secure and improve the Services. Spreeflo’s processing in that capacity is governed by the Spreeflo Privacy Policy and not by this DPA.

2.4 A description of the processing carried out under this DPA is set out in **Annex I**.

3. Processing instructions

3.1 Spreeflo shall process Customer Personal Data only on Customer’s documented instructions, including with regard to transfers to a third country, unless required to do otherwise by law to which Spreeflo is subject. Where such a legal requirement applies, Spreeflo shall inform Customer of that requirement before processing, unless the law prohibits it on important grounds of public interest.

3.2 The Agreement, this DPA (including Annex I), and Customer’s configuration and use of the Services through the dashboard, API, SDK, in-app AI assistant or MCP server constitute Customer’s complete documented instructions.

3.3 Spreeflo shall inform Customer without undue delay if, in its opinion, an instruction infringes Data Protection Law. Spreeflo may suspend performance of the affected instruction until it is amended or confirmed.

3.4 **Customer obligations and warranties.** Customer shall:

(a) comply with Data Protection Law in its capacity as controller, including in respect of the collection of Customer Personal Data before it enters the Services;

(b) establish and maintain a valid lawful basis for the processing, and where the processing relies on consent, obtain and be able to demonstrate consent meeting the standard of Articles 4(11) and 7 EU GDPR;

(c) comply with PECR and the ePrivacy Directive in respect of electronic marketing and any storage of or access to information on end users’ terminal equipment, including

obtaining any consent required before deploying the Spreeflo SDK or any tracking, cookies or similar technologies, and before sending marketing email or web push notifications;

(d) provide all notices and information required by Articles 13 and 14 EU GDPR to data subjects;

(e) not upload, submit or instruct the processing of any special category personal data under Article 9 EU GDPR, personal data relating to criminal convictions and offences under Article 10 EU GDPR, or personal data of children below the age of digital consent, without Spreeflo's prior written agreement; and

(f) not use the Services to send unsolicited communications or to process personal data obtained from purchased, rented, scraped or otherwise unlawfully sourced lists.

3.5 Customer is solely responsible for the accuracy, quality and lawfulness of Customer Personal Data and of the means by which it acquired that data.

4. Confidentiality and personnel

4.1 Spreeflo shall ensure that persons authorised to process Customer Personal Data are subject to an appropriate obligation of confidentiality, whether contractual or statutory, that survives termination of their engagement.

4.2 Spreeflo shall take reasonable steps to ensure the reliability of such persons and shall limit access to Customer Personal Data to those personnel who require access to perform Spreeflo's obligations under the Agreement.

5. Security

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk to data subjects, Spreeflo shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex II**.

5.2 Customer is responsible for its own use of the Services, including securing its account credentials, API keys and MCP access tokens, configuring access controls and user roles appropriately, and promptly deactivating access for personnel who no longer require it.

5.3 Spreeflo may update the measures in Annex II from time to time provided that the updated measures do not materially reduce the overall level of security.

6. Subprocessors

6.1 Customer provides Spreeflo with **general written authorisation** to engage Subprocessors, subject to this Clause 6.

6.2 The Subprocessors engaged as at the effective date are listed in **Annex III** and maintained at **https://spreeflo.com/legal/subprocessors**.

6.3 Spreeflo shall give Customer at least **thirty (30) days'** notice before a new Subprocessor begins processing Customer Personal Data, by updating the page referred to in Clause 6.2 and notifying subscribers to its change notification list. Customer may subscribe at that page and is responsible for maintaining a current subscription.

6.4 Customer may object to a new Subprocessor on reasonable grounds relating to data protection by giving written notice within the notice period. The parties shall discuss the objection in good faith. If it cannot be resolved, Customer may terminate the affected Services on written notice, with a pro-rata refund of prepaid fees for the terminated period as Customer's sole remedy.

6.5 Spreeflo shall impose on each Subprocessor, by written contract, data protection obligations that are no less protective than those in this DPA, and shall remain **fully liable** to Customer for the performance of each Subprocessor's obligations.

6.6 **Customer-configured integrations.** Where Customer configures the Services to connect to a third-party service using Customer's own account or API credentials, including an AI provider API key supplied by Customer, that third party is **not** a Subprocessor of Spreeflo. Spreeflo transmits data to that service on Customer's instruction and under Customer's own agreement with that provider. Customer is responsible for entering into any data processing agreement required with that provider, for the lawfulness of the resulting processing, and for the transfer mechanism applying to it. Such services are identified separately in Annex III for transparency.

7. Assistance with data subject rights

7.1 The Services provide Customer with functionality to access, export, rectify, restrict, delete and suppress Customer Personal Data through the dashboard and API. Customer shall use that functionality to respond to data subject requests in the first instance.

7.2 Taking into account the nature of the processing, Spreeflo shall assist Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling Customer's obligation to respond to requests to exercise data subject rights under Chapter III of the EU GDPR.

7.3 If Spreeflo receives a request directly from a data subject in relation to Customer Personal Data, Spreeflo shall not respond substantively other than to direct the data subject to Customer, and shall notify Customer without undue delay.

7.4 Spreeflo may charge a reasonable fee for assistance under Clause 7.2 that goes materially beyond the self-service functionality of the Services, having first notified Customer of the fee.

8. Personal data breach

8.1 Spreeflo shall notify Customer **without undue delay** after becoming aware of a personal data breach affecting Customer Personal Data.

8.2 The notification shall include, to the extent then known and insofar as it is within Spreeflo's possession: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed to address it,

and a contact point for further information. Where the information is not all available at once, it may be provided in phases without undue further delay.

8.3 Spreeflo shall provide reasonable assistance to Customer in connection with Customer's obligations under Articles 33 and 34 EU GDPR.

8.4 Spreeflo's notification of, or response to, a personal data breach is not an acknowledgement of fault or liability.

9. Data protection impact assessments

Taking into account the nature of the processing and the information available to Spreeflo, Spreeflo shall provide reasonable assistance to Customer with data protection impact assessments under Article 35 EU GDPR and prior consultations with supervisory authorities under Article 36 EU GDPR, in each case solely in relation to the processing of Customer Personal Data by the Services. Spreeflo may satisfy this obligation by making available its then-current security documentation, this DPA and its published compliance materials.

10. International transfers

10.1 **Transfers from the EEA to Spreeflo.** Spreeflo is established in the United Kingdom. Transfers of Customer Personal Data from the EEA to Spreeflo are made pursuant to the European Commission's adequacy decision in respect of the United Kingdom adopted on 19 December 2025, and no additional transfer mechanism is required for that transfer for so long as that decision remains in force.

10.2 **Onward transfers.** Where Spreeflo transfers Customer Personal Data to a Subprocessor in a country that is not the subject of an adequacy decision, Spreeflo shall ensure that the transfer is subject to an appropriate safeguard under Article 46 EU GDPR and, where applicable, Article 46 UK GDPR. Spreeflo shall achieve this by one or more of: (a) the recipient's active certification under the EU-US Data Privacy Framework and, for UK-origin data, its UK Extension; (b) the EU SCCs (Module Three, processor to processor) together with, for UK-origin data, the UK Addendum; or (c) another lawful transfer mechanism.

10.3 **Fallback.** If the adequacy decision referred to in Clause 10.1 ceases to apply, the parties shall be deemed to have entered into the EU SCCs (Module Two, controller to processor) in respect of transfers from the EEA to Spreeflo, with Annex I, II and III of this DPA populating the corresponding annexes of the EU SCCs, the optional docking clause applying, and the governing law and forum being those of Ireland. For UK-origin data the UK Addendum shall apply with Spreeflo as importer. Acceptance of the Agreement shall have the same effect as signing the EU SCCs and the UK Addendum, and no separate signature is required for them to take effect.

10.4 **Transfer information.** The current location of each Subprocessor and the transfer mechanism relied on is set out in Annex III. Spreeflo shall maintain a transfer risk assessment and make a summary available to Customer on reasonable request.

10.5 As at the effective date, Customer Personal Data is stored and processed in the United States. Spreeflo does not currently offer an EEA storage region.

11. Audit

11.1 Spreeflo shall make available to Customer information reasonably necessary to demonstrate compliance with Article 28 EU GDPR, and shall allow for and contribute to audits, including inspections, conducted by Customer or an auditor mandated by Customer.

11.2 Customer agrees to exercise the right in Clause 11.1 in the first instance by requesting Spreeflo's then-current security documentation, this DPA, Spreeflo's record of processing activities under Article 30(2) EU GDPR, and any third-party audit reports or certifications Spreeflo holds.

11.3 Where that documentation is not sufficient to demonstrate compliance, Customer may request an audit, subject to: not more than **once in any twelve (12) month period** except where required by a supervisory authority or following a personal data breach; **thirty (30) days'** prior written notice; conduct during normal business hours without unreasonably disrupting Spreeflo's operations; the auditor not being a competitor of Spreeflo and being bound by confidentiality; and Customer bearing its own costs and Spreeflo's reasonable costs of the audit.

11.4 Audit rights do not extend to data, systems or facilities of other Spreeflo customers, or to information the disclosure of which would breach Spreeflo's obligations to third parties.

12. Deletion and return

12.1 On termination or expiry of the Agreement, Spreeflo shall, at Customer's election, delete or return Customer Personal Data, and delete existing copies, unless retention is required by law to which Spreeflo is subject.

12.2 Customer may export Customer Personal Data through the Services at any time during the term and for **thirty (30) days** after termination. After that period Spreeflo shall delete Customer Personal Data from its live production systems within **thirty (30) days**, and from encrypted backups within **ninety (90) days** in accordance with its backup rotation cycle. Data held in backups remains subject to Clause 4 and 5 until deleted.

13. Liability

13.1 Each party's liability arising out of or in connection with this DPA is subject to the exclusions and limitations of liability set out in the Agreement.

13.2 Nothing in this DPA limits either party's liability to a data subject under Article 82 EU GDPR, or any liability that cannot lawfully be limited.

14. General

14.1 In the event of conflict, the order of precedence is: (1) the EU SCCs or UK Addendum where they apply; (2) this DPA; (3) the Agreement.

14.2 This DPA takes effect on the effective date and continues until Spreeflo ceases to process Customer Personal Data. Clauses 4, 12 and 13 survive termination.

14.3 Spreeflo may amend this DPA on **thirty (30) days'** notice where necessary to comply with Data Protection Law, to reflect a change in the transfer mechanisms relied on, or where the amendment does not materially reduce Customer's protections. Any other amendment requires the written agreement of both parties.

14.4 This DPA is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction, save where the EU SCCs apply and specify otherwise.

14.5 If any provision is held invalid or unenforceable, the remainder continues in full force.

Execution

This DPA is incorporated into the Agreement and takes effect automatically when Customer accepts the Agreement or uses the Services. **No signature is required for this DPA to be binding**, and Article 28(9) EU GDPR is satisfied by this DPA being recorded in electronic form.

Where Customer's internal procedures require a countersigned copy for its records, Customer may request one from privacy@spreeflo.com and Spreeflo will provide an executed version. A countersigned copy does not alter the terms below and is provided solely as a record.

Signed for and on behalf of Spreeflo Ltd *(completed only where a countersigned copy is requested)*

Name: _____ Title: _____

Signature: _____ Date: _____

Signed for and on behalf of the Customer

Name: _____ Title: _____

Signature: _____ Date: _____

ANNEX I — Description of the processing

A. Parties

Data exporter / Controller: the Customer identified in the Agreement. Contact: as recorded in Customer's Spreeflo account. Role: controller.

Data importer / Processor: Spreeflo Ltd, 405 Baltic Quay, 1 Sweden Gate, London, England, SE16 7TJ. Contact: privacy@spreeflo.com. Role: processor.

B. Description of the processing

Categories of data subjects

- Customer's contacts, subscribers and leads
- Visitors to Customer's website or application, including visitors not yet identified
- Respondents to Customer's forms and surveys
- Recipients of Customer's email campaigns and web push notifications
- Customer's own personnel who use the Services

Categories of personal data

Category	Examples
Contact identifiers	Email address, name, phone number, company, postal address
Custom contact attributes	Any field Customer chooses to store, e.g. plan, country, job title, lifecycle stage, numeric counters
Behavioural and analytics data	Page views, sessions, custom events and event properties, entry and exit pages, referrer and UTM parameters, session duration
Technical data	Visitor identifier, IP address, browser, operating system, device type, approximate geolocation derived from IP (country, region, city)
Form responses	Any answer submitted through a Spreeflo form, including free text and uploaded files where those question types are used
Messaging data	Web push subscription endpoints and keys, message send, delivery, open, click, bounce, dismissal and unsubscribe records
Consent records	Subscription status, opt-in source, timestamp, double opt-in confirmation
Content submitted for AI generation	Contact attributes and prompt content that Customer configures the AI features to use

Special category data: Not requested by Spreeflo and not permitted without prior written agreement (Clause 3.4(e)).

Frequency of transfer: Continuous, for the duration of the Agreement.

Nature and purpose of the processing

Provision of the Spreeflo marketing automation platform, comprising: storage and management of contact records and attributes; audience segmentation; collection of website and application behavioural events; web analytics reporting; creation and delivery of email campaigns and journeys; creation and delivery of browser push notifications; hosting and processing of forms and form responses; generation of personalised message content using AI inference services where Customer enables those features; provision of an in-app AI assistant

and a hosted MCP server through which Customer may operate the Services; reporting and analytics on the foregoing; and technical support.

Duration of processing: For the term of the Agreement, plus the deletion periods in Clause 12.

Retention: Customer Personal Data is retained until deleted by Customer, until deleted under Customer's configured retention settings, or until deletion under Clause 12, whichever is earliest.

C. Competent supervisory authority

The supervisory authority of the EEA Member State in which Customer is established, or in which Customer's EU representative is established.

ANNEX II — Technical and organisational measures

Encryption. All data in transit is encrypted using TLS 1.2 or above. All data at rest is encrypted using AES-256 at the storage layer. Secrets and credentials are held in a managed secrets store.

Access control. Role-based, workspace-scoped access control within the application. Multi-factor authentication is enforced on all administrative and infrastructure accounts. Production access follows least privilege, is limited to named personnel, and is logged. API keys and MCP tokens are workspace-scoped and revocable by Customer.

Pseudonymisation and minimisation. Contacts are separable from behavioural events by identifier. Anonymous visitor data is stored against a rotating visitor identifier until the visitor is identified, and the identifier is rotated on logout.

Availability and resilience. Automated encrypted backups are taken on a documented cycle, and restore procedures are tested periodically. Infrastructure is hosted with a major cloud provider offering redundancy at the platform level.

Integrity and logging. An application audit trail records assets created and modified, including those created through the AI assistant and the MCP server. Infrastructure and application logs are retained for 12 months.

Segregation. Customer data is logically separated by workspace and enforced at the data access layer. Production, staging and development environments are separated, and production personal data is not used in development.

Secure development. Changes are managed through version control and an automated deployment pipeline. Dependencies are scanned for known vulnerabilities.

Personnel. All employment and contractor agreements include confidentiality obligations. Access is revoked as part of offboarding.

Sub-processor management. Written data protection terms are in place with each Sub-processor. Security posture and transfer mechanism are reviewed before engagement. The Sub-processor list is published with change notification.

Deletion. Deleting a contact removes the contact record and its associated events, engagement records and form responses from production systems. Suppression records are retained after deletion for the purpose of honouring objections to direct marketing, as permitted by Article 17(3)(b) EU GDPR.

ANNEX III — Sub-processors

Sub-processor	Registered address	Service provided	Location of processing	Transfer mechanism
Amazon Web Services, Inc.	410 Terry Avenue North, Seattle, WA 98109, USA	Cloud infrastructure, application hosting, database storage and backups	United States	AWS GDPR Data Processing Addendum; EU SCCs; UK Addendum
Amazon Web Services, Inc.	As above	Outbound email delivery	United States	As above
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA	DNS and proxy for Customer-branded link domains used in email	Global anycast edge	Cloudflare Data Processing Addendum; EU-US Data Privacy Framework including the UK Extension; EU SCCs; UK Addendum
Fireworks.ai, Inc.	Redwood City, California, USA	AI model inference supporting the in-app AI assistant	United States, and such other locations as set out in Fireworks' own sub-processor schedule	Fireworks Data Processing Addendum: EU SCCs Module Two, the UK Approved Addendum, and a Swiss addendum

Fireworks is contractually prohibited from using Customer Personal Data to train, fine-tune or otherwise improve any model, and does not retain prompt inputs or model outputs beyond the lifecycle of the request under the configuration Spreeflo uses. Fireworks undergoes annual SOC

2 Type II audits and holds ISO 27001, ISO 27701 and ISO 42001 certifications. Its own sub-processor list is available to Customer on request.

Customer-configured integrations — not Sub-processors (Clause 6.6)

Where Customer supplies its own credentials for a third-party AI provider, that provider processes data under Customer's own agreement with it and is not a Sub-processor of Spreeflo. Customer is responsible for the data processing agreement and transfer mechanism applying to that provider. Spreeflo determines which fields are included in the prompt; that selection is described in Annex I and falls within Spreeflo's processing under this DPA.

Not Sub-processors under this DPA

- **Stripe, Inc.** processes Customer's billing and payment data, in respect of which Spreeflo is a controller. Stripe does not process Customer Personal Data as defined in this DPA and is addressed in the Spreeflo Privacy Policy.

Version 1.0 — 19 August 2026. Maintained at https://spreeflo.com/legal/dpa