FillWright — Data Processing Agreement

Version 18 July 2026

This Data Processing Agreement ("**DPA**") is entered into between:

1. **Redbit S.r.l.s.**, Viale della Grande Muraglia 494, 00144 Roma, Italy — VAT IT15237911001, REA RM-1576999, PEC redbitsrls@legalmail.it (the "**Processor**"); and
2. _____ (legal name), _____ (registered address), VAT / Tax ID _____ (the "**Controller**"),

each a "Party" and together the "Parties".

This DPA forms part of the FillWright Terms of Service between the Parties and applies whenever the Processor processes personal data on behalf of the Controller in providing FillWright (the "**Lead Data**" — the data the Controller uploads and submits through the service). It gives effect to Article 28 GDPR and, as applicable, the UK GDPR, and includes a CCPA/CPRA service-provider addendum. On data-protection matters this DPA prevails over the Terms.

1. Definitions

"Applicable Data Protection Law" means the EU GDPR, the UK GDPR, and any other privacy law applicable to the processing, including the CCPA/CPRA. "Controller", "Processor", "Processing", "Personal Data", "Data Subject", and "Personal Data Breach" have the meanings given in the GDPR. "Sub-processor" means any processor engaged by the Processor to process Lead Data. "SCCs" means the European Commission's Standard Contractual Clauses (Decision 2021/914) and, for UK data, the UK International Data Transfer Addendum. Details of the processing are in Annex 1; the security measures in Annex 2; the sub-processors in Annex 3.

2. Roles and scope

For the Lead Data the Controller is the controller (or a processor acting for a third-party controller) and the Processor is the processor. The Processor processes Lead Data only to provide the service and only on the Controller's documented instructions, which are set out in the Terms, this DPA, and the Controller's configuration of the service (recipes, runs, and targets). The Processor will inform the Controller if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law.

3. Processor obligations (Art. 28(3))

The Processor shall:

(a) process Lead Data only on the Controller's documented instructions, including for transfers, unless required by law (in which case the Processor informs the Controller first, unless the law prohibits it);

(b) ensure that persons authorised to process Lead Data are bound by confidentiality;

(c) implement the technical and organisational security measures set out in Annex 2 (Art. 32);

(d) engage Sub-processors only under Section 5;

(e) assist the Controller, by appropriate technical and organisational measures, to respond to Data Subject requests (Section 6);

(f) assist the Controller with security, breach notification, data protection impact assessments, and prior consultation (Art. 32–36), taking into account the nature of processing and the information available to the Processor;

(g) delete or return Lead Data at the end of the service (Section 10); and

(h) make available the information necessary to demonstrate compliance and allow for audits (Section 11).

4. Confidentiality

The Processor keeps Lead Data confidential and grants access only to personnel who need it to provide the service and who are subject to binding confidentiality obligations.

5. Sub-processors

The Controller grants general written authorisation for the Processor to engage the Sub-processors listed in Annex 3. The Processor imposes on each Sub-processor data-protection obligations that are no less protective than this DPA and remains fully liable for their performance. The Processor will give the Controller at least 30 days' notice of any intended addition or replacement of a Sub-processor; the Controller may object on reasonable data-protection grounds within that period, and if the Processor cannot address the objection the Controller may terminate the affected part of the service.

6. Data-subject rights

Taking into account the nature of the processing, the Processor assists the Controller with appropriate technical and organisational measures — and the self-service tools in the application — to fulfil the Controller's obligation to respond to Data Subject requests (access, rectification, erasure, restriction, portability, objection). If a Data Subject contacts the Processor directly regarding the Controller's Lead Data, the Processor will refer them to the Controller and will not respond to the substance without the Controller's instruction.

7. Personal data breach

The Processor notifies the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Lead Data, and provides the information reasonably available to help the Controller meet its notification obligations (Art. 33–34), including the nature of the breach, likely consequences, and measures taken or proposed.

8. Impact assessments

The Processor provides reasonable assistance with the Controller's data protection impact assessments and any prior consultation with a supervisory authority, to the extent they relate to the Processor's processing of Lead Data and taking into account the information available to the Processor.

9. International transfers

Lead Data is hosted in the European Union (Germany). Where the Processor or a Sub-processor transfers Lead Data to a country outside the EEA or the UK that is not covered by an adequacy decision, the SCCs apply and are incorporated into this DPA by reference — the EU SCCs (Module Two, controller-to-processor, or Module Three, processor-to-processor, as applicable) and, for UK data, the UK International Data Transfer Addendum. The Controller instructs and authorises these transfers for the purpose of providing the service.

10. Deletion and return

The Controller may delete Lead Data (and everything derived from it) at any time from the dashboard. On termination of the service, at the Controller's choice the Processor returns or deletes the Lead Data and existing copies within 30 days, and residual copies in encrypted backups are overwritten within 30 days, unless retention is required by law.

11. Audits and information

The Processor makes available the information necessary to demonstrate compliance with Article 28 and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor it mandates. Audits take place no more than once every 12 months (or following a Personal Data Breach or where required by a supervisory authority), on at least 30 days' written notice, during business hours, subject to confidentiality, and without unreasonably disrupting the Processor's operations. The Processor may satisfy an audit request by providing relevant third-party audit reports or certifications where available.

12. CCPA / CPRA addendum (service provider)

For Lead Data relating to California residents, the Processor acts as the Controller's "service provider". The Processor processes such data solely to perform the service and on the Controller's instructions, and does not: (a) sell or share it; (b) retain, use, or disclose it for any purpose other than performing the service or as permitted by the CCPA; (c) retain, use, or disclose it outside the direct business relationship with the Controller; or (d) combine it with personal information from other sources except as the CCPA permits. The Processor certifies that it understands and will comply with these restrictions.

13. Liability

Each Party's liability under this DPA is subject to the limitations and exclusions set out in the FillWright Terms of Service.

14. Term

This DPA takes effect on the effective date below (or, if earlier, when the Controller accepts the Terms) and continues for as long as the Processor processes Lead Data on the Controller's behalf. Provisions that by their nature should survive (including confidentiality, deletion, and audit) survive termination.

15. Governing law and order of precedence

This DPA is governed by Italian law, with the courts of Rome having jurisdiction, consistent with the Terms. In case of conflict: the SCCs prevail over this DPA on matters of international transfer; this DPA prevails over the rest of the Terms on data-protection matters.

Annex 1 — Details of the processing

- **Subject matter:** provision of FillWright (authorized data entry on the Controller's behalf).
- **Duration:** the term of the Controller's account and until deletion of the Lead Data.
- **Nature and purpose:** storage and structuring of the Lead Data and its automated submission to the web forms (Targets) the Controller configures, including optional AI-assisted suggestion of field mappings.
- **Categories of data subjects:** as determined by the Controller — for example its leads, applicants, customers, or contacts.
- **Types of personal data:** as determined by the Controller and contained in the CSV it uploads (for example names and contact details, and any fields it includes). The Controller must not upload special-category data unless it has a lawful basis and instructs the Processor accordingly.

Annex 2 — Technical and organisational measures (Art. 32)

- Encryption in transit (TLS); credentials hashed with Argon2id.
- Mandatory two-factor authentication for financial actions; login lockout; rate limiting.
- Strict per-target authorization; SSRF protection on outbound requests; honeypots respected and never filled.
- Role-based access controls and least privilege; audit logging; environment segregation.
- Hosting in the EU (Germany); encrypted backups overwritten within 30 days.
- Breach detection and response procedures; secure development practices.

Annex 3 — Sub-processors

Sub-processor	Role	Location	Transfer safeguard
Revolut (Revolut Bank UAB)	Payment processing	European Union (Lithuania)	Intra-EEA — no transfer
Anthropic	Optional AI form-field mapping	United States	SCCs

Sub-processor	Role	Location	Transfer safeguard
LangChain (LangSmith)	LLM observability — token/cost/latency only; prompt/response content redacted and not sent	EU	—
Smartproxy / Decodo	Regional network egress (only when enabled)	Varies by region	SCCs where applicable
IONOS	Hosting infrastructure	EU (Germany)	—
Redbit self-managed email (mail.redbitapp.com)	Transactional email	EU	—

Signatures

Agreed by the Parties:

For the Processor — Redbit S.r.l.s.

Name: _____

Title: _____

Signature: _____

Date: _____

For the Controller

Name: _____

Title: _____

Signature: _____

Date: _____

Effective date: _____