ReguShield AI
PILOT SUCCESS KIT

PILOT DOCUMENTATION

Data Processing Agreement (DPA) — Template

Part of the ReguShield AI Pilot Success Kit — everything your team needs to run a successful compliance-intelligence pilot.

DRAFT TEMPLATE — for discussion only. Not legal advice. Must be reviewed and adapted by qualified legal counsel before execution.

This template is structured to support the requirements of Article 28 of the EU General Data Protection Regulation (GDPR). It contains placeholders and must be completed, reviewed, and adapted to the specific facts of the engagement and the applicable law before it is used or signed.

---

1. Parties

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

- **[CUSTOMER LEGAL NAME]**, of [CUSTOMER ADDRESS] (the **"Controller"** or **"Customer"**); and
- **ReguShield AI** [INSERT LEGAL ENTITY NAME / NUMBER / ADDRESS] (the **"Processor"** or **"ReguShield AI"**),

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

Effective Date: [EFFECTIVE DATE]

This DPA forms part of, and is subject to, the Terms and Pilot Agreement between the Parties (`11-Terms-and-Pilot-Agreement.md`) (the **"Principal Agreement"**). In the event of a conflict between this DPA and the Principal Agreement in respect of the processing of personal data, this DPA prevails.

---

2. Roles of the Parties

- The Customer is the **data controller** in respect of the personal data processed under this DPA.
- ReguShield AI is the **data processor**, processing personal data only on the documented instructions of the Customer.
- Where the Customer is itself a processor acting on behalf of a third-party controller, the Customer warrants it has the authority to appoint ReguShield AI as a sub-processor and this DPA applies on a back-to-back basis.

---

3. Subject-Matter and Duration

- **Subject-matter:** the processing of personal data by ReguShield AI on behalf of the Customer in connection with the provision of the ReguShield AI compliance decision-support platform during the pilot.
- **Duration:** for the term of the pilot (approximately four (4) weeks, as set out in the Principal Agreement) and any agreed extension, plus the limited period required to return or delete personal data under Section 12.

---

4. Nature and Purpose of Processing

ReguShield AI processes personal data for the purpose of providing compliance decision-support and intelligence to the Customer, including:

- ingesting and storing Customer-provided datasets (for example, transaction and operational records);
- generating risk scores, regulatory mappings, narratives, and recommended actions;
- supporting evaluation of compliance readiness against the frameworks referenced by the platform (AMLA 2027, AMLR, AMLD6, MiCA, DORA, EU AI Act, FATF Travel Rule); and
- providing the pilot workspace, reporting, and related support.

ReguShield AI provides **decision-support only** and does not make regulatory determinations; see `09-Decision-Support-Disclaimer.md` .

---

5. Categories of Personal Data and Data Subjects

The categories below are indicative and must be confirmed and adjusted by the Customer for the specific datasets it provides.

Categories of data subjects (examples — Customer to confirm):

- the Customer's customers / end-users referenced in uploaded records;
- the Customer's authorised platform users (pilot operators).

Categories of personal data (examples — Customer to confirm):

- identifiers contained in uploaded records (e.g. user/account identifiers);
- transaction and operational attributes (e.g. amounts, currencies, origin/destination countries, cross-border flags);
- compliance-related attributes (e.g. KYC status, risk level, PEP flag, sanctions-screening status, source-of-funds status);
- platform-user account data (e.g. email address, role).

Special-category data: the Customer must **not** upload special-category personal data (Article 9 GDPR) or criminal-offence data (Article 10 GDPR) unless it has a lawful basis and has notified ReguShield AI in writing. The platform is not designed to process special-category data by default.

---

6. Processor Obligations

ReguShield AI shall:

1. process personal data only on the Customer's **documented instructions**, including this DPA and the Principal Agreement, unless required to do otherwise by applicable law (in which case it will inform the Customer unless legally prohibited);
2. ensure that persons authorised to process the personal data are bound by an appropriate duty of **confidentiality**;
3. implement appropriate **technical and organisational security measures** (Section 9);
4. respect the conditions for engaging **sub-processors** (Section 7);
5. taking into account the nature of the processing, **assist the Customer** by appropriate measures in fulfilling its obligation to respond to data-subject requests (Section 10);
6. **assist the Customer** in ensuring compliance with its obligations under Articles 32–36 GDPR (security, breach notification, data-protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to ReguShield AI;
7. at the Customer's choice, **delete or return** all personal data after the end of the provision of services (Section 12);
8. make available to the Customer the information necessary to demonstrate compliance with Article 28 and allow for and contribute to **audits** (Section 13); and
9. **inform the Customer** if, in its opinion, an instruction infringes the GDPR or other applicable data-protection law.

---

7. Sub-Processors

The Customer provides **general written authorisation** for ReguShield AI to engage sub-processors, subject to the conditions in this Section.

ReguShield AI shall impose on each sub-processor data-protection obligations that are, in substance, equivalent to those set out in this DPA (in particular, appropriate technical and organisational measures), and ReguShield AI remains fully liable to the Customer for the performance of each sub-processor's obligations.

Current sub-processors:

SUB-PROCESSOR	PURPOSE	LOCATION
Supabase	Application hosting and PostgreSQL database	EU region
Resend	Transactional email delivery (e.g. invitations, notifications)	[CONFIRM REGION]

ReguShield AI shall give the Customer reasonable prior notice of any intended addition or replacement of a sub-processor, and the Customer may **object** on reasonable, data-protection grounds. If the Parties cannot resolve the objection, the Customer may terminate the affected services as set out in the Principal Agreement.

---

8. International Transfers

Personal data is processed and stored in the **EU region** (Supabase, EU region). ReguShield AI shall not transfer personal data outside the European Economic Area (EEA) without (a) the Customer's prior written authorisation and (b) an appropriate transfer mechanism under Chapter V GDPR (for example, an adequacy decision or Standard Contractual Clauses). Where transactional email delivery (Resend) involves processing outside the EEA, the Parties shall ensure an appropriate transfer mechanism is in place; the Customer must confirm and document this before relying on the service.

---

9. Security Measures

ReguShield AI implements appropriate technical and organisational measures designed to protect personal data, including:

- **Encryption at rest** using AES-256.
- **Tenant isolation** via row-level security (RLS) keyed on the verified account email, designed to **fail closed** (access is denied if the email claim is absent or does not match).
- Hosting on **Supabase (PostgreSQL), EU region**.
- Access controls and the principle of least privilege for the small operating team.

Full details of the technical and organisational measures are set out in the **ReguShield AI Security Whitepaper**, which is incorporated into this DPA by reference and forms the description of measures for the purposes of Article 28(3)(c) and Article 32 GDPR.

Certifications: ReguShield AI does **not** currently hold ISO 27001 or SOC 2 certification. These are on the roadmap and are not represented as held. This DPA does not imply any certification.

---

10. Assistance with Data-Subject Requests

Taking into account the nature of the processing, ReguShield AI shall provide reasonable assistance to the Customer, by appropriate technical and organisational measures and insofar as possible, in responding to requests by data subjects to exercise their rights under Chapter III GDPR (including access, rectification, erasure, restriction, portability, and objection). If ReguShield AI receives a request directly from a data subject, it shall, unless legally prohibited, promptly notify the Customer and not respond to the request itself except on the Customer's documented instructions.

---

11. Personal Data Breach Notification

ReguShield AI shall notify the Customer **without undue delay** after becoming aware of a personal data breach affecting the Customer's personal data, and shall provide the Customer with reasonably available information to help the Customer meet its own breach-notification obligations under Articles 33 and 34 GDPR, including (to the extent known): the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, and the measures taken or proposed.

---

12. Return or Deletion on Termination

On termination or expiry of the provision of services, and at the Customer's choice, ReguShield AI shall **delete or return** all personal data processed on the Customer's behalf and delete existing copies, unless applicable law requires storage of the personal data. The Customer should make any request for return within [RETENTION / RETURN WINDOW] of termination; thereafter ReguShield AI may delete the personal data in accordance with its standard deletion practices.

---

13. Audit Rights

ReguShield AI shall make available to the Customer information reasonably necessary to demonstrate compliance with Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. The Parties agree that audits shall be conducted on reasonable prior written notice, no more than once per twelve (12) month period (save where required by a supervisory authority or following a personal data breach), during business hours, in a manner that does not unreasonably disrupt ReguShield AI's operations, and subject to confidentiality. ReguShield AI may satisfy audit requests by providing relevant documentation (including the Security Whitepaper and, when available, third-party reports).

---

14. Liability

The liability of each Party under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement, to the extent permitted by applicable law.

15. Governing Law

This DPA is governed by the laws of **[JURISDICTION]**, and is subject to the dispute-resolution and governing-law provisions of the Principal Agreement, save where mandatory data-protection law requires otherwise.

16. Signatures

CONTROLLER — [CUSTOMER LEGAL NAME]	PROCESSOR — REGUSHIELD AI
Name: _____	Name: _____
Title: _____	Title: _____
Date: [EFFECTIVE DATE]	Date: [EFFECTIVE DATE]
Signature: _____	Signature: _____

DRAFT TEMPLATE — for discussion only. Not legal advice. Must be reviewed and adapted by qualified legal counsel before execution.

Contact: hello@regushield.ai