



ReguShield AI

PILOT SUCCESS KIT

PILOT DOCUMENTATION

GDPR Privacy Notice

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

This document describes ReguShield AI's pilot environment as currently implemented. It is provided for customer due diligence and is not a warranty or certification.

1. Purpose & Scope

This notice explains how ReguShield AI handles personal data in connection with its pilot environment, for the benefit of prospective customers and their data protection teams. It complements the Data Processing Agreement (DPA) template available in this pilot kit.

A full, published privacy policy is in preparation (target Q3 2026). This notice reflects the current pilot.

2. Controller & Processor Roles

- For **customer-uploaded operational records**, the **customer is the controller** and **ReguShield AI is the processor**, processing data on the customer's documented instructions to provide compliance analysis.
 - For limited **account and pilot-administration data** (e.g. the email used to authenticate, invitation and activation records, support correspondence), ReguShield AI acts as **controller** for the purpose of operating and securing the service.
-

3. Lawful Basis

- **Contract performance** — processing necessary to deliver the pilot under the pilot agreement.
- **Legitimate interest** — operating, securing and improving the compliance-analytics service, and managing pilot access, balanced against the rights of data subjects.

For customer-uploaded records, the lawful basis for the underlying personal data rests with the **customer as controller**; ReguShield AI processes that data on the customer's instructions.

4. Data Categories

ReguShield AI processes:

- **Customer-uploaded operational records** — transaction, KYC and risk-signal fields ingested for compliance analysis. Only fields required for the analysis are ingested (data minimisation).
- **Account / administration data** — authentication email, invitation/activation records, workspace and organisation profile, support correspondence.
- **Evidence and document uploads** — files a customer chooses to upload.

Special-category data: Customers should **avoid uploading special-category personal data** (as defined in GDPR Article 9) and should upload only the fields necessary for compliance analysis. Case analysis outputs are designed to reference anonymised transaction fields. If a customer's intended processing involves special-category data, this should be raised before the pilot so it can be assessed and documented.

5. Where Data Is Processed

All data is processed and stored **within the European Union** — PostgreSQL via Supabase in the Dublin / Amsterdam region. Case data, analysis logs and audit records are stored within the EU. Data is encrypted at rest (AES-256) and in transit (TLS), and isolated per workspace by Postgres Row-Level Security keyed to the verified session email.

6. Sub-Processors

ReguShield AI uses the following sub-processors:

SUB-PROCESSOR	PURPOSE	LOCATION
Supabase	Managed PostgreSQL database, authentication and file storage	EU (Dublin / Amsterdam)
Vercel	Application hosting and delivery	Global edge network with EU-accessible points of presence
Resend	Transactional / invitation email delivery	Email service provider

The current list of sub-processors is available on request. Material changes will be communicated to pilot customers.

Note: transactional email delivery is provider-ready. Where email is not yet wired to a live provider for a given pilot, invitation and notification messages may be logged rather than delivered until the provider is configured.

7. Data-Subject Rights

Data subjects have the rights afforded by the GDPR, including the right to **access, rectification, erasure, restriction, objection and portability**.

- Where ReguShield AI is **processor**, requests are routed through the **customer (controller)**, and ReguShield AI will assist the controller in responding.
- Where ReguShield AI is **controller** (account/administration data), requests can be made directly to **hello@regushield.ai**.

We aim to respond to data-subject and deletion requests promptly. (See the Data Retention & Deletion document in this kit for the deletion process.)

8. Data Sharing

Case data is **not** shared with third-party analytics, advertising or data-broker services. Data is shared only with the sub-processors listed in Section 6 strictly to operate the service.

9. Retention

Pilot workspace data is retained for the pilot with a **90-day default**; enterprise retention is configurable per the DPA. Deletion can be requested at any time (see the Data Retention & Deletion document). Residual copies may persist temporarily in the managed platform's backups until they age out on the normal cycle.

10. EU Representative

An EU GDPR representative has been **identified; formal appointment is planned for Q3 2026**. Until that appointment is formalised, data protection enquiries should be directed to the contact below.

11. Current Limitations / Roadmap

- Published privacy policy: in preparation (target Q3 2026).
- EU representative: identified; formal appointment planned Q3 2026.
- Data Protection Impact Assessment (DPIA) for high-risk processing: in progress.

These items are tracked and will be updated as the programme matures. Nothing in this notice should be read as asserting a certification or formal appointment that is not yet in place.

12. Contact

For privacy enquiries, data-subject requests or the DPA:

hello@regushield.ai