

# Privacy Policy

Anweshna AI Due Diligence Platform

Version 1.1 — Effective 28 September 2026

Downloaded from <https://anweshna.com/privacy.html> · the web page is the authoritative version.

## CONTENTS

- |                                        |                                  |
|----------------------------------------|----------------------------------|
| 1. Who we are & our roles              | 9. Security                      |
| 2. Data we collect                     | 10. Your rights                  |
| 3. Lawful bases                        | 11. Automated decision-making    |
| 4. How we use data                     | 12. Cookies, storage & analytics |
| 5. AI processing disclosure            | 13. Children                     |
| 6. Sub-processors & recipients         | 14. Changes                      |
| 7. International transfers & residency | 15. Contact & Grievance Officer  |
| 8. Retention                           |                                  |

## 1. Who We Are & Our Roles

The Anweshna platform is operated by **Anweshna AI Due Diligence**, registered office **E46 Mahadevpur 4, Namsai-792105, Arunachal Pradesh, India** ("Anweshna", "we"). Privacy enquiries: [privacy@anweshna.com](mailto:privacy@anweshna.com).

We act in two distinct roles:

- **Controller / Data Fiduciary** — for account data, billing data, leads and marketing data, website analytics, consent records, and platform telemetry. This policy governs that processing.
- **Processor / Data Processor** — for personal data contained inside documents our clients upload for analysis ("engagement data"). Our clients are the controllers of that data; we process it only on their instructions under our [Data Processing Agreement](#). If your personal data appears in a document uploaded by one of our clients, please direct requests to that client; we will assist them as required by law.

## 2. Data We Collect

### 2.1 Account and contact data

- Name, work email, company name (at signup, team invitation, or demo/contact forms)
- Public demo: the email address you enter on the demo form is also recorded against each document you upload in the demo and each demo analysis you run, so the demo can apply its monthly allowance of analyses per email address
- API key identifiers (hashed for team sub-keys; linked to your account)
- Role assignments for team members (owner, analyst, viewer, clean team), and room roles within clean rooms (lead, counsel, clean team, deal team)

### 2.2 Engagement data (processed as Processor)

- Uploaded documents and their extracted text; AI analysis results and reports — encrypted at rest
- Document metadata: title, filename, type, size, timestamps, deal-room assignment

### 2.3 Technical and security data

- IP address and timestamp of API requests and security-relevant events (auth failures, rate limiting)
- Audit logs: account ID, action type, entity IDs, IP, timestamp for every write and report access
- Error telemetry: error messages, stack traces, and the page URL when the portal or API logs a fault
- Website page-view analytics on our public pages: page path, IP address, browser user-agent, timestamp — collected first-party, without cookies (see Section 12)

## 2.4 Billing data

- Subscription status, plan, Paddle customer/subscription identifiers, payment event history
- Card details are collected and held by Paddle only — we never store card numbers

## 2.5 Consent records

- Each terms/NDA/privacy acceptance: event type, terms version, timestamp, IP address, user agent, account or email identifier — kept in an append-only log as evidence of consent

## 2.6 Communications

- Support requests, feedback, bug reports, sales enquiries, and email delivery logs
- **Kai support assistant:** if you use the in-portal AI assistant (Pro and above), we log each question you send and the answer given, together with your account identifier, plan tier, the model used, and a timestamp. Where a question is escalated to a human, the same content plus the escalation reason and our reviewer's notes are retained for that review. See Section 5 for how these messages are processed, and Section 8 for how long they are kept

## 3. Lawful Bases

| Processing                                                    | GDPR basis                              | Notes                                                                             |
|---------------------------------------------------------------|-----------------------------------------|-----------------------------------------------------------------------------------|
| Account, engagement analysis, billing                         | Contract — Art. 6(1)(b)                 | Needed to deliver the service you purchased                                       |
| Security logging, rate limiting, audit trail, error telemetry | Legitimate interests — Art. 6(1)(f)     | Fraud/abuse prevention, service integrity; assessed as not overriding your rights |
| Consent log retention                                         | Legal obligation / legitimate interests | Evidence of contract formation and consent                                        |
| Tax and accounting records                                    | Legal obligation — Art. 6(1)(c)         | Statutory retention periods                                                       |
| Marketing emails, demo follow-ups                             | Consent — Art. 6(1)(a)                  | Withdrawable at any time; every email has an unsubscribe link                     |
| First-party page-view analytics                               | Legitimate interests — Art. 6(1)(f)     | Cookie-less, first-party, aggregate reporting only                                |

Under India's DPDP Act 2023, we process personal data with consent or for legitimate uses recognised by the Act, and honour Data Principal rights (Section 10). For California residents, see Section 10.3 — **we do not sell or share personal information** as defined by the CCPA/CPRA.

Documents uploaded by clients may contain personal data of third parties (e.g. employees or directors of a target company). The uploading client, as controller, is responsible for its lawful basis; we process such data solely as processor per Section 1.

## 4. How We Use Data

- Providing the platform: document analysis, reports, deal rooms, team management
- Delivering your API key and account lifecycle emails (welcome, renewal, cancellation)
- Billing and subscription management via Paddle
- Security monitoring, abuse prevention, and incident response
- Diagnosing faults via error telemetry and support requests
- Understanding aggregate usage of our public pages (first-party analytics)

We do not use your documents or analysis results to train AI models, and we do not permit our AI sub-processor to do so. We do not sell personal data, and we do not run third-party advertising or tracking.

## 5. AI Processing Disclosure

When a document is analysed, its extracted text (not the original file) is transmitted over encrypted channels to our AI inference provider, **Anthropic, PBC (US)**, to generate risk scores and findings. This processing is governed by Anthropic's commercial API terms and data processing addendum, under which API inputs and outputs are **not used to train Anthropic's models** and are retained by Anthropic only for limited abuse-monitoring periods. Analysis output is stored encrypted in our database, attributed to your account.

Reports are labelled as AI-generated and carry provenance metadata identifying who downloaded them and when.

## 5.1 Kai support assistant

The in-portal Kai assistant (Pro and above) answers product questions. Your message is sent to the same AI inference provider, **Anthropic, PBC (US)**, under the same commercial API terms as above — **not used to train Anthropic's models**, retained by them only for limited abuse-monitoring periods. Kai answers only from our own published product documentation. It has no access to your documents, analyses, or reports, and this is enforced rather than assumed: the assistant runs on a separate, restricted database role granted access to two tables — its own chat log and its escalation queue — and to nothing else.

**Please do not paste confidential deal content into the assistant.** Unlike your uploaded documents, chat messages are **not encrypted at rest**, and a message escalated to a human is read by our staff. We are the Controller for these messages — they are support communications, not Engagement Data — so the processor protections in the [DPA](#) do not apply to them. They are deleted on the schedule in Section 8. If you need to discuss a specific document, use the analysis and report features, where content is encrypted per-client and covered by the DPA.

## 6. Sub-processors & Recipients

The authoritative, maintained list of sub-processors (with locations and roles) is **Annex III of our [DPA](#)**. As of this version it comprises:

- **Anthropic, PBC (USA)** — AI inference on extracted document text
- **Supabase, Inc.** (database hosted in the **us-east-1 region, N. Virginia, United States**) — managed Postgres database holding all platform data (documents encrypted at application level before storage)
- **Paddle.com Market Ltd.** (USA) — payment processing
- **FastAPIcloud.com** — application compute; all data transits this infrastructure
- **Namecheap.com** — transactional email delivery (recipient address and email content only)

We may also disclose data to professional advisers, and to authorities where legally compelled — in which case we will notify the affected client where the law permits.

## 7. International Transfers & Data Residency

- **Database:** United States (Supabase us-east-1).
- **AI inference & payments:** United States (Anthropic, Paddle).
- **Application hosting:** us-east-1.

Where personal data protected by the EU/UK GDPR is transferred to countries without an adequacy decision, we rely on the European Commission's Standard Contractual Clauses (and the UK Addendum / IDTA), plus supplementary measures including application-level encryption. Details and copies are available on request via [privacy@anweshna.com](mailto:privacy@anweshna.com).

## 8. Retention

| Data                                                   | Retention                                                                                                                                                                                                                   |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Engagement documents & analyses                        | Duration of subscription (or deal-room life for per-deal purchases) + 30-day export window after termination, then deleted on a reviewed basis — normally within 30 days of the window closing, in any event within 90 days |
| Extracted text of analysed documents                   | Deleted 30–31 days after the document's analysis completes. The analysis and its reports are kept for the period above; asking questions about the document or re-analysing it after that requires uploading it again       |
| Cross-Doc comparison results (file names and findings) | Until you delete them, or until Engagement Data is deleted after termination (above). Files uploaded for a comparison are deleted when you leave Cross-Doc, and in any event within 6 hours                                 |
| Account data (name, email, keys)                       | Subscription + up to 12 months (billing/legal defence)                                                                                                                                                                      |
| Server/security logs & error telemetry                 | 90 days, then deleted or anonymised                                                                                                                                                                                         |
| Kai support assistant chat logs and escalations        | 90 days, then deleted                                                                                                                                                                                                       |
| Audit logs (uploads, analyses, report access)          | 7 years (regulatory defensibility)                                                                                                                                                                                          |
| Consent records (clickwrap log)                        | 7 years                                                                                                                                                                                                                     |
| Billing & tax records                                  | 7 years or as required by tax law                                                                                                                                                                                           |

|                                                                                |                                                                                           |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Demo/sales leads                                                               | 12 months from collection unless converted or consent renewed                             |
| Public demo uploads and reports                                                | Deleted when you start a new analysis or close the page, and in any event within 48 hours |
| Public demo usage records (the demo email recorded against each demo analysis) | 7 years, with the audit logs above                                                        |
| Page-view analytics                                                            | Raw entries 12 months; aggregates indefinitely                                            |

## 9. Security

Measures include: application-level encryption of document content and analysis results at rest with per-client derived keys and a key-rotation procedure; TLS in transit; per-tenant isolation enforced on every query with database-level row security policies as a backstop; role-based team access; authenticated, rate-limited APIs with brute-force lockouts; append-only consent logging; audit logging of writes and report access; and report provenance watermarking. Full technical and organisational measures are in Annex II of the [DPA](#). We notify affected clients of personal data breaches without undue delay, and in any event within 48 hours of becoming aware (see DPA §7).

## 10. Your Rights

### 10.1 EU/UK GDPR

Access, rectification, erasure, restriction, objection, portability, and withdrawal of consent. Self-serve:

GET `/api/v1/account/export` (portability) and DELETE `/api/v1/account` (erasure request), or email [privacy@anweshna.com](mailto:privacy@anweshna.com). We respond within 30 days. You may complain to your supervisory authority (UK: ICO; EU: your national DPA).

### 10.2 India DPDP Act 2023

Data Principals may access a summary of processing, request correction and erasure, nominate a representative, and raise grievances with our Grievance Officer (Section 15), escalating to the Data Protection Board of India if unresolved.

### 10.3 California (CCPA/CPRA)

Rights to know, delete, correct, and to non-discrimination. We do not sell or share personal information for cross-context behavioural advertising, and we do not use sensitive personal information beyond permitted service purposes. Submit requests to [privacy@anweshna.com](mailto:privacy@anweshna.com); we verify via your account email.

### 10.4 Other jurisdictions

We honour equivalent statutory rights (e.g. Brazil LGPD, Canada PIPEDA, Australia Privacy Act) on request.

Note: erasure requests cannot override retention we are legally required to keep (tax, consent evidence, audit integrity); those records are retained per Section 8 and then deleted.

## 11. Automated Decision-Making

The platform produces AI-generated risk analyses of documents for professional review. We do not make automated decisions producing legal or similarly significant effects about natural persons (GDPR Art. 22). Our terms require clients to keep a qualified human in the loop before acting on any output.

## 12. Cookies, Storage & Analytics

- **No tracking cookies, no third-party analytics or advertising scripts.**
- **sessionStorage:** by default, your API key is held in browser sessionStorage for the session and cleared when the tab closes; never sent to third parties.
- **localStorage:** minor UI preferences. In the public demo, also a flag that you completed the demo form, a random session identifier, and the email address you entered on it. These let the demo recognise you on this browser, keep your uploads separate from other visitors', and apply its monthly allowance; they are sent with your demo requests to our servers and stay until you clear this site's data in your browser. If you opt in to "Remember me" at sign-in, your API key is instead held in browser localStorage so you stay signed in across browser restarts, until you sign out or clear it yourself.
- **First-party page-view beacon:** our public pages send a single beacon per page load containing the page path; our server records it with your IP address and user-agent for aggregate traffic statistics and abuse prevention. No cookie or persistent identifier is set, and no cross-site tracking occurs.

### 13. Children

---

The platform is a business tool and is not directed at anyone under 18. We do not knowingly collect children's data; if you believe we hold any, contact us and we will delete it.

### 14. Changes

---

We will notify registered users of material changes by email or in-platform notice at least 30 days before they take effect, and update the version and date below. Prior versions are available on request.

### 15. Contact & Grievance Officer

---

**Anweshna AI Due Diligence** — E46 Mahadevpur 4, Namsai-792105, Arunachal Pradesh, India

Privacy requests: [privacy@anweshna.com](mailto:privacy@anweshna.com) (acknowledged within 72 hours; substantive reply within 30 days)

Grievance Officer (DPDP Act): Compliance Team Lead [grievance@anweshna.com](mailto:grievance@anweshna.com)

EU/UK representative: **Not applicable** — Anweshna does not regularly offer services to, or monitor the behaviour of, data subjects in the EU/UK and has not appointed a representative there

---

**Anweshna AI Due Diligence · E46 Mahadevpur 4, Namsai-792105, Arunachal Pradesh, India**

Legal: [legal@anweshna.com](mailto:legal@anweshna.com) · Privacy: [privacy@anweshna.com](mailto:privacy@anweshna.com) · General: [info@anweshna.com](mailto:info@anweshna.com)

Anweshna scores documents for risk signals. It does not replace legal review, independent verification, or expert due diligence.