

Data Processing Agreement

Anweshna AI Due Diligence Platform

Version 1.1 — Effective 28 September 2026

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

This DPA is incorporated into and forms part of the [Terms of Service](#) between the Client and the Provider.

1. Scope, Roles & Definitions

1.1 This DPA governs the Provider's processing of Personal Data contained in Engagement Data (documents, extracted text, analysis output, and related metadata) on behalf of the Client. The Client is the **Controller** (GDPR) / **Data Fiduciary** (DPDP Act); the Provider is the **Processor**.

1.2 "Data Protection Laws" means all laws applicable to the processing of Personal Data under this DPA, including the EU GDPR, UK GDPR, the Indian Digital Personal Data Protection Act 2023, and the CCPA/CPRA. Terms not defined here have the meanings in those laws or the Terms of Service.

1.3 Details of processing (subject matter, duration, nature, purpose, data categories, data subjects) are set out in **Annex I**.

2. Instructions

2.1 The Provider processes Personal Data only on the Client's documented instructions, which consist of: (a) the Terms of Service and this DPA; (b) the Client's configuration and use of the Platform (uploading a document is an instruction to analyse it as described in the product); and (c) other written instructions agreed by the parties.

2.2 The Provider will inform the Client if, in its opinion, an instruction infringes Data Protection Laws (without obligation to perform legal review), and may suspend the affected processing until resolved.

2.3 If the Provider is required by law to process beyond instructions, it will inform the Client before processing unless the law prohibits it.

2.4 CCPA: the Provider acts as a "service provider"; it will not sell or share Personal Data, nor retain, use, or disclose it outside the direct business relationship or for any purpose other than performing the Service, and it certifies that it understands these restrictions.

3. Confidentiality of Personnel

Persons authorised to process Personal Data are bound by contractual or statutory confidentiality obligations, receive data-handling instruction appropriate to their role, and access data strictly on a need-to-know basis. Administrative access to client data and metadata is logged.

4. Security

The Provider implements and maintains the technical and organisational measures in **Annex II**, appropriate to the risk of processing highly confidential transaction material. The Provider may update Annex II from time to time, provided the overall level of protection is not materially reduced during a subscription term.

5. Sub-processors

5.1 The Client grants general written authorisation to engage the sub-processors listed in **Annex III**.

5.2 The Provider will give at least **30 days'** notice (email or in-Platform) before adding or replacing a sub-processor that processes Engagement Data. The Client may object on reasonable data-protection grounds within that period; if the parties cannot resolve the objection, the Client may terminate the affected Orders and receive a pro-rata refund of prepaid unused fees.

5.3 The Provider imposes data protection obligations on each sub-processor materially equivalent to this DPA and remains liable for their performance.

6. Assistance

6.1 Data subject requests. Taking into account the nature of processing, the Provider provides reasonable assistance (including the account export and deletion APIs) to help the Client respond to data subject requests. If a data subject contacts the Provider directly about a Client's Engagement Data, the Provider will redirect them to the Client without responding substantively, except as legally required.

6.2 DPIAs and consultations. The Provider will provide reasonable assistance with data protection impact assessments and prior consultations, based on information available to it.

7. Personal Data Breach

The Provider will notify the Client **without undue delay, and in any event within 48 hours**, after becoming aware of a Personal Data breach affecting Engagement Data, providing (as information becomes available): the nature of the breach, categories and approximate volumes of data and data subjects affected, likely consequences, measures taken or proposed, and a contact point. The Provider will document breaches and cooperate with the Client's notification obligations. Notification is not an admission of fault.

8. Deletion & Return

Upon termination or expiry, the Client may export Engagement Data for 30 days (machine-readable via API/report downloads). After that window, the Provider deletes Engagement Data on a reviewed basis — deletion is irreversible and is therefore carried out by an operator rather than automatically on a timer — normally within 30 days of the window closing and in any event within 90 days, except where retention is required by law (see the retention schedule in the [Privacy Policy](#)); retained data remains protected by this DPA and is deleted when the legal ground expires. Deletion covers backups on the backup provider's rotation schedule.

9. Audit & Information

9.1 The Provider will make available information reasonably necessary to demonstrate compliance with this DPA: responses to security questionnaires, summaries of penetration tests or security reviews, and this DPA's annexes.

9.2 Where Data Protection Laws grant the Client a mandatory audit right that cannot be satisfied by documentation, the Client may conduct (itself or via an independent auditor bound to confidentiality) an audit of the Provider's relevant processing, no more than once per 12 months, on 30 days' notice, during business hours, without access to other clients' data, at the Client's cost.

10. International Transfers

10.1 Processing locations are listed in Annex III. Where Personal Data protected by EU/UK GDPR is transferred to a country without adequacy, the parties rely on the EU Standard Contractual Clauses (Module 2: controller→processor, and Module 3 where the Client is itself a processor), which are incorporated by reference, completed with the details in Annex I–III; for UK transfers, the UK IDTA Addendum applies; for Swiss transfers, the Swiss adaptations apply.

10.2 The Provider will notify the Client if it receives a legally binding request from a public authority for the Client's Engagement Data unless prohibited by law, and will challenge disproportionate or unlawful requests where reasonably possible.

11. Liability & Order of Precedence

Liability under this DPA is subject to the limitations and exclusions in the Terms of Service, except where Data Protection Laws prohibit such limitation. In conflict, this DPA prevails over the Terms for data protection matters.

Annex I — Details of Processing

Item	Description
Subject matter	AI-assisted risk analysis of documents uploaded by the Client for due diligence purposes (such analysis constitutes document-level risk screening, not comprehensive due diligence, and does not replace independent legal, financial, or expert review; see Terms Section 11)
Duration	Term of the Client's subscription or per-deal purchase, plus the 30-day export window and legally required retention
Nature & purpose	Storage (encrypted), text extraction, AI scoring and findings generation, report generation and export, cross-document comparison, access control and audit logging

Categories of data	Any personal data contained in deal documents, typically: names, roles, contact details, employment and compensation information, contractual relationships, litigation and compliance history of individuals connected to a target business; account data of the Client's Authorised Users (name, email, role)
Special categories	Not intended; prohibited without prior written agreement (Terms §7.3). Incidental occurrences within deal documents are processed under the same protections
Data subjects	Employees, officers, directors, shareholders, customers, suppliers, and counterparties of businesses referenced in uploaded documents; the Client's Authorised Users
Frequency	Continuous, as initiated by Client uploads and analysis requests

Annex II — Technical & Organisational Measures

- **Encryption at rest:** document text and analysis results encrypted at the application layer (Fernet: AES-128-CBC + HMAC-SHA256) with per-client keys derived via HKDF-SHA256 from a root secret held only in the deployment environment; documented key-rotation procedure with dual-key re-encryption support.
- **Encryption in transit:** TLS for all client, database, and sub-processor connections.
- **Tenant isolation:** every query is scoped to the authenticated client's identifier at the application layer; database row-level-security policies (fail-closed) provide an independent backstop; isolation is covered by an automated regression test suite.
- **Access control:** API-key authentication with constant-time comparison; hashed team sub-keys with role-based permissions (owner/analyst/viewer/clean-team); viewer role cannot upload; clean-team-restricted deal rooms; clean rooms (Clean Rooms add-on) held in a separate database schema accessible only to a dedicated database role, encrypted with a separate key, with per-room roles, human-approved releases and an append-only, hash-chained audit log; administrative endpoints separately gated.
- **Abuse resistance:** IP-based rate limiting and auth-failure lockouts; upload type/size validation; OTP attempt limits on signup verification.
- **Auditability:** append-only consent log; audit log of write and report-access operations (actor, action, entity, IP, timestamp); report provenance watermarking (who downloaded, when).
- **Data minimisation:** original uploaded files are not retained after text extraction; only extracted text and derived analysis are stored; document content is never written to application logs.
- **Personnel & organisation:** confidentiality obligations for all personnel with access; least-privilege administrative access, logged; documented incident-response and breach-notification procedure (internal runbook, available to clients on request).
- **Resilience:** managed database platform with automated backups; fail-fast startup checks refusing insecure configuration (e.g. missing encryption key) in production.

Annex III — Authorised Sub-processors

Sub-processor	Role	Data	Location
Anthropic, PBC	AI inference (risk scoring, findings, emerging-risk detection)	Extracted document text; no original files	United States
Supabase, Inc.	Managed Postgres database	All platform data; document content and analyses stored application-layer-encrypted	United States (us-east-1, N. Virginia)
Paddle.com Market Ltd.	Payment processing	Billing contact and payment data (card data held by Paddle only)	United States
FastAPIcloud.com	Application compute	All data in transit through the application	us-east-1
Namecheap.com	Transactional email	Recipient name, email address, account lifecycle content	United States

Current version of this list is always published at this URL; changes are notified per Section 5.

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

Legal: legal@anweshna.com · Privacy: privacy@anweshna.com · General: info@anweshna.com

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