ChitiShield™ Data Processing Agreement

Version 1.0 — 22 November 2026

This Data Processing Agreement ("DPA") forms part of the order form, proposal or pilot agreement and the Terms of Service (together, the "Agreement") between the customer named in the Agreement ("Customer") and **AnantaQuanta Consulting Pvt Ltd**, Padmaraonagar, Secunderabad, Hyderabad, Telangana 500025, India ("AnantaQuanta").

1. Definitions

"Data Protection Laws" means all laws applicable to the processing of Customer Personal Data under the Agreement, including, where applicable, India's Digital Personal Data Protection Act 2023 and Rules 2025 ("DPDP"), the EU General Data Protection Regulation ("GDPR"), the UK GDPR, the UAE Federal Decree-Law No. 45 of 2021, and the Saudi Personal Data Protection Law. "Customer Personal Data" means personal data within content that Customer or its users upload to, or create in, the ChitiShield™ platform. Terms such as "Controller", "Processor", "Data Fiduciary", "Data Processor", "personal data breach" and "data subject" or "Data Principal" have the meanings given in the applicable Data Protection Laws.

2. Roles

Customer is the Controller / Data Fiduciary of Customer Personal Data. AnantaQuanta is the Processor / Data Processor and processes Customer Personal Data only on Customer's documented instructions, which are given in the Agreement, this DPA and through Customer's configuration and use of the platform. AnantaQuanta will tell Customer if it believes an instruction breaches Data Protection Laws.

3. Details of processing

The subject matter, duration, nature and purpose of processing, and the categories of data and data subjects, are described in **Annex 1**.

4. Confidentiality

AnantaQuanta ensures that everyone authorised to process Customer Personal Data is bound by confidentiality obligations.

5. Security

AnantaQuanta implements the technical and organisational measures described in **Annex 2**, appropriate to the risk. AnantaQuanta may update these measures provided the overall level of protection is not reduced.

6. Subprocessors

6.1 Customer gives general authorisation for AnantaQuanta to engage subprocessors. AnantaQuanta provides Customer with its current subprocessor list (names, purposes and processing locations) before Customer Personal Data is uploaded, and on request at any time.

6.2 AnantaQuanta will give Customer at least 30 days' notice of any new subprocessor. Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, Customer may terminate the affected services and receive a pro-rata refund of prepaid fees for them.

6.3 AnantaQuanta imposes data protection obligations on each subprocessor no less protective than this DPA and remains responsible for its subprocessors' performance.

7. Assistance

Taking into account the nature of the processing, AnantaQuanta will assist Customer, by appropriate technical and organisational measures, to respond to requests from data subjects / Data Principals, and with security, breach notification, data protection impact assessments and consultations with regulators. AnantaQuanta will promptly forward to Customer any request it receives directly from a data subject about Customer Personal Data and will not respond except on Customer's instructions.

8. Personal data breaches

AnantaQuanta will notify Customer **without undue delay, and in any event within 48 hours**, after becoming aware of a personal data breach affecting Customer Personal Data. The notice will include, as far as then known, the nature of the breach, the categories and approximate volume of data and individuals affected, likely consequences and the measures taken or proposed. AnantaQuanta will provide further information as it becomes available, so Customer can meet its own notification obligations (including DPDP's requirement to inform the Data Protection Board and affected Data Principals, and GDPR's 72-hour regulator notification).

9. International transfers

AnantaQuanta will transfer Customer Personal Data outside the country in which it was collected only in compliance with Data Protection Laws. Where GDPR or UK GDPR applies to a transfer to a country without an adequacy decision, the parties agree that the European Commission's Standard Contractual Clauses (Module 2 or Module 3, as applicable) and, for the UK, the International Data Transfer Addendum, are incorporated into this DPA by reference. Transfers from India comply with any restrictions notified under the DPDP Act.

10. Return and deletion

At the end of the services, AnantaQuanta will, at Customer’s choice, return Customer Personal Data in a commonly used format or delete it, within 30 days, unless the law requires AnantaQuanta to keep it. Backups are deleted on their normal rotation cycle and remain protected under this DPA until deleted. Security logs are retained for the period required by the DPDP Rules 2025.

11. Audits

AnantaQuanta will make available the information reasonably necessary to demonstrate compliance with this DPA, including completed security questionnaires and, when available, third-party audit reports. Where that information is not sufficient, Customer may conduct an audit once a year, on 30 days’ written notice, during business hours, at its own cost and subject to confidentiality, or more often where required by a regulator or following a personal data breach.

12. Liability and precedence

Each party’s liability under this DPA is subject to the limitations in the Agreement, except where Data Protection Laws do not allow limitation. If this DPA conflicts with the Agreement on the processing of Customer Personal Data, this DPA prevails. If the Standard Contractual Clauses apply and conflict with this DPA, the Standard Contractual Clauses prevail.

13. Term

This DPA lasts for as long as AnantaQuanta processes Customer Personal Data under the Agreement.

Annex 1 — Details of processing

Item	Detail
Subject matter	Provision of the ChitiShield™ platform
Duration	The subscription or pilot term, plus the return/deletion period in clause 10
Nature of processing	Hosting, storage, retrieval, AI-assisted analysis of documents, drafting of answers for human review, mapping to frameworks, logging, export
Purpose	Enabling Customer to map controls to evidence, answer questionnaires, maintain an audit log and export Trust Packs

Item	Detail
Data subjects	Customer’s users; individuals named in documents Customer uploads (e.g. employees, control owners, approvers, vendor contacts)
Categories of personal data	Names, work contact details, job titles, user IDs, approval and activity records, and any personal data contained in uploaded documents
Sensitive data	Not required for the service. Customer should not upload sensitive or special-category personal data unless agreed in writing.

Annex 2 — Technical and organisational measures

- Encryption of data in transit and at rest
- Role-based access control on a least-privilege basis for Customer users and AnantaQuanta personnel
- Logging of user and administrator actions in an audit log; security logs retained for at least one year
- Logical separation of each Customer’s workspace
- Human approval required before AI-drafted answers are finalised
- Customer Personal Data not used to train AI models
- Backups and recovery procedures to maintain availability
- Confidentiality obligations and data protection training for personnel with access
- Incident response procedure supporting the breach-notification timeline in clause 8

Annex 3 — Subprocessors

The current subprocessor list, including each subprocessor’s name, purpose and processing location, is provided to Customer before Customer Personal Data is uploaded and is available on request from engage@anantaquantaconsulting.com.