INTAI LIMITED

Data Processing Agreement

INTAI portal | Business customers
Version 1.0 | Document date: 6 October 2026

The parties

Processor: INTAI LIMITED, registered in England and Wales, company number 16850074, VAT number GB 516 1732 10, whose registered office is Boxwood Farm, Station Road, Old Bursledon, Southampton, SO31 8AA, United Kingdom (INTAI).

Controller: the customer organisation identified in the applicable order, subscription record or signed Services Agreement (Customer). The person accepting on its behalf must have authority to bind that organisation.

Contact

Data protection instructions, security enquiries and notices to INTAI: enquiries@intai.co.uk.
INTAI incident decision owner: Jamie Randall, Managing Director.
Notices to the Customer: its designated administrative or privacy contact recorded in the service or order.

Effective date and acceptance

This agreement takes effect when INTAI adopts this version and the Customer accepts it through a recorded electronic acceptance or signature. Its document date alone does not establish adoption or acceptance. The applicable order or acceptance record identifies the Customer and effective date; no handwritten fields are required for electronic acceptance.

Service activation

Acceptance of this agreement does not authorise unapproved AI routes or enable real client data automatically. INTAI will enable real-client processing only after the applicable contractual, transfer, security, retention and service-closure safeguards are implemented and verified. Synthetic-data demonstrations must not contain real client information.

Contents

1. Scope, roles and instructions
2. Security, assistance and incidents
3. Providers, transfers and termination
Schedule 1: Processing description
Schedule 2: Security measures
Schedule 3: Providers and routes
Schedule 4: Retention, return and deletion

1. Scope, roles and instructions

1.1 Contract and priority

This Data Processing Agreement (DPA) forms part of the order, subscription terms or other services agreement between INTAI and the Customer (Services Agreement), on its effective date. It governs INTAI's processing of Customer Personal Data on the Customer's behalf. For that processing, this DPA prevails over inconsistent provisions of the Services Agreement. Applicable mandatory transfer terms take priority where required.

1.2 Definitions

Data Protection Law means the UK GDPR, the Data Protection Act 2018 and other applicable UK data protection legislation, as amended. Controller, Processor, Personal Data, Processing, Personal Data Breach and Supervisory Authority have their statutory meanings. Customer Personal Data means personal data processed by INTAI on the Customer's behalf in delivering the portal. A Sub-processor is another processor engaged by INTAI for that processing.

1.3 Roles and duration

The Customer acts as Controller and INTAI acts as Processor for Customer Personal Data. Where the Customer is itself a processor, it warrants that it has the relevant controller's authority for these instructions and appointments. Processing is described in Schedule 1 and continues during service delivery and any necessary, lawful return or deletion period. INTAI's own-controller processing is governed by its applicable privacy notice, not by instructions under this DPA.

1.4 Documented instructions

INTAI will process Customer Personal Data only on the Customer's documented instructions, including instructions about international transfers. These comprise the final Services Agreement, this DPA, authorised configurations and requests submitted by authorised Customer users. INTAI will notify the Customer immediately if it considers an instruction infringes Data Protection Law and may suspend the affected processing pending clarification.

1.5 Required disclosures

If applicable UK law requires processing beyond those instructions, INTAI will inform the Customer of the legal requirement before processing unless the law prohibits that information on important grounds of public interest. INTAI will limit the processing to what the law requires.

1.6 Customer responsibilities

The Customer determines purposes, lawful bases and any conditions for special-category or criminal-offence data; provides required notices; checks that submitted data is necessary, accurate and lawfully obtained; manages its users and permissions; and issues lawful instructions. It must not upload unnecessary identification documents or unsupported categories of information. Human review remains the Customer's responsibility before an output is used or written to another system.

1.7 AI restrictions

INTAI will not use Customer Personal Data to train general-purpose AI models or authorise providers to do so. AI processing is limited to approved providers and routes in Schedule 3. Identifier replacement is pseudonymisation, not a guarantee of anonymity: contextual information may still identify a person. The Customer must minimise sensitive information in prompts and uploads.

2. Security, assistance and incidents

2.1 Confidentiality and access

INTAI will ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty. Access will be limited to what is necessary for their duties and subject to appropriate authorisation. INTAI will maintain and review access controls and withdraw access when no longer required.

2.2 Technical and organisational measures

INTAI will implement measures appropriate to the risk, taking account of the nature, scope, context and purposes of processing and the risks to individuals. The baseline measures are described in Schedule 2. INTAI will maintain processes for restoring availability and access after incidents, and regularly assess the effectiveness of its safeguards. Changes must not materially reduce the overall protection of Customer Personal Data.

2.3 Rights requests

Taking account of the nature of processing, INTAI will assist the Customer through appropriate technical and organisational measures, insofar as possible, in responding to individuals exercising their data protection rights. INTAI will promptly forward requests relating to Customer Personal Data to the Customer and will not independently decide the response except on instructions or as legally required.

2.4 Compliance assistance

Taking account of the nature of processing and information available to it, INTAI will assist the Customer with security obligations, breach assessments and notifications, data protection impact assessments and prior consultation with the Supervisory Authority. INTAI will provide information reasonably needed to assess the service's processing risks and safeguards.

2.5 Personal Data Breaches

INTAI will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. Available information will include the nature of the breach, affected data and individuals, approximate numbers where known, a contact for further information, likely consequences and measures taken or proposed. Information may be supplied in stages without undue further delay.

2.6 Incident cooperation

INTAI will take reasonable steps to contain, investigate and mitigate the breach, preserve relevant evidence and cooperate with the Customer. The Customer determines its notifications to individuals and regulators, unless INTAI has an independent legal duty. Notification is not an admission of liability. The initial notification will be made without undue delay and in any event within 24 hours of INTAI becoming aware of the breach, even if the investigation is continuing.

2.7 Evidence and audits

INTAI will make available information necessary to demonstrate compliance with its processor obligations and allow and contribute to audits, including inspections, conducted by the Customer or its mandated auditor. The parties will coordinate reasonable notice, confidentiality, scope and security arrangements. These arrangements must not prevent an urgent or legally necessary audit or restrict statutory regulatory powers. INTAI will notify the Customer immediately if an audit instruction appears unlawful.

3. Providers, transfers and termination

3.1 Sub-processor authorisation

The Customer gives general written authorisation for the Sub-processors listed in Schedule 3, subject to the route restrictions and activation conditions in that schedule. INTAI will notify the Customer in advance of intended additions or replacements and provide information sufficient for a data protection assessment. INTAI will give at least 15 calendar days of advance notice before introducing a new Sub-processor or replacement for Customer Personal Data. The Customer may object on reasonable data protection grounds before the change takes effect.

3.2 Objections and safeguards

INTAI and the Customer will seek a reasonable alternative or mitigation for a justified objection. Until resolved, INTAI will not route the affected Customer Personal Data to the disputed new provider. If no solution is available, the parties will agree how to end the affected service and address fees under the Services Agreement. INTAI will impose equivalent applicable data protection obligations by written contract and remains responsible to the Customer for its Sub-processors' performance of those obligations.

3.3 International transfers

INTAI will make a restricted transfer only on documented instructions and with a lawful mechanism under applicable Data Protection Law. Before use, INTAI will verify relevant recipients, access locations, onward transfers and any applicable adequacy decision or contractual safeguards. Where needed, the parties will complete the UK IDTA or UK Addendum and the applicable data protection test / transfer risk assessment. This agreement does not itself execute the provider transfer instruments.

3.4 AI routes

Customer Personal Data may be sent to an AI route only when its provider contract, account/model retention settings, processing locations and any necessary transfer safeguards and assessment have been verified and recorded by INTAI. Amazon Bedrock is the intended primary route. Anthropic is subject to the same activation conditions. xAI is excluded from real-client processing under this agreement; introducing it requires the Sub-processor change process and satisfaction of these conditions. Until activation conditions are met, affected routes must remain limited to synthetic data.

3.5 End of processing

At the Customer's choice, INTAI will return or delete Customer Personal Data after the end of the relevant processing services and delete existing copies unless applicable UK law requires retention. Return will use a reasonably accessible format. Legally retained data will be identified, isolated where appropriate and processed only for the relevant legal purpose. A subscription cancellation does not remove these obligations.

3.6 Completion and backups

Return, deletion and recovery-copy arrangements are specified in Schedule 4. Inaccessible backup copies must remain protected, be excluded from ordinary use and expire under an agreed deletion cycle; restoration must reapply deletion instructions. INTAI will provide confirmation of completion on request. The absence of an automated firm-wide deletion tool is not an exception to the obligation to return or delete data.

3.7 General provisions

This DPA creates no new commercial liability cap. Any applicable allocation under the approved Services Agreement must preserve mandatory statutory obligations and individuals' rights. Changes must be documented and accepted by authorised parties. This DPA is governed by the law of England and Wales. Its courts have jurisdiction, subject to mandatory law and any applicable transfer instrument.

Schedule 1 | Processing description

Subject matter and purpose

Provision of a governed AI workspace for financial advisers and their supporting staff: client summaries, document analysis, meeting preparation, notes, research and communications, draft advice based on the adviser's own recommendation, workflow administration, human review and governance evidence. Customer content must not be processed for unrelated advertising or general-purpose model training.

Nature of operations

Authorised reading of client records from the Customer's CRM; receiving adviser notes and uploaded materials; malware scanning and text extraction; working-content storage; replacing direct identifiers with tokens before approved AI requests; generation and human review of drafts; authorised CRM write-back; recording governance metadata; export and deletion. CRM write permission is separate from read access and off by default.

Individuals

The Customer's current and prospective clients; family members, dependants, beneficiaries and representatives named in permitted records; advisers and supporting staff; and other individuals whose information is lawfully included in authorised processing.

Personal data

Identity and contact information, including names, addresses, email, phone, dates of birth and NI numbers; financial circumstances, holdings, pensions, income, expenditure, protection and risk information; meeting notes, fact finds, statement text, correspondence and draft outputs. Identity documents are not requested by workflows and must not be uploaded unless necessary, lawful and within the authorised service scope.

Special-category information

Health and vulnerability information may be included where necessary for an authorised client task. The Customer must establish the applicable lawful basis and special-category condition and minimise what it supplies. Other special-category information or criminal-offence data requires INTAI's prior written agreement to support that processing and appropriate safeguards.

Duration

During the relevant processing services and the necessary return/deletion period, subject to configured working-content retention and Schedule 4. Any legal retention must be limited to the data, purpose and duration actually required by law.

Separate-controller processing

INTAI determines purposes for its own account administration, sign-in, security and billing records and must explain those activities in its applicable privacy notice. Stripe acts as an independent controller for its own purposes. The Customer's CRM arrangements remain its responsibility. These boundaries do not exempt personal data processed on the Customer's behalf from this DPA.

Schedule 2 | Technical and organisational measures

Firm separation and permissions

Tenant separation is enforced in database queries. Cross-firm attempts are blocked and logged. Access is permission-based across adviser, paraplanner, compliance, firm administrator, network and platform roles. Network and platform views expose aggregates rather than routine access to client content. Any exceptional support access must be authorised, necessary, logged and subject to confidentiality.

Authentication

Users sign in using a password and authenticator-app code. Access to Client files and firm exports requires fresh authentication. INTAI will control privileged access, manage recovery securely, review access rights and remove access when no longer required.

Encryption and secrets

HTTPS protects data in transit. Google Cloud and Neon provide encryption at rest. Token maps and CRM connection tokens receive additional application-level encryption. Optional Client files use private storage with a customer-managed encryption key. Secrets are held in Google Secret Manager. INTAI will protect keys and restrict access to them.

Privacy and human review

Direct identifiers are replaced by tokens before AI processing. Wrong-client and absent-client checks stop affected runs before AI calls. Token maps are encrypted and removed when no longer needed for the run. Human review is required before an output is used or written; a record check precedes client-record write-back. These controls reduce risk but do not guarantee anonymous prompts or error-free outputs.

Uploads and records

Uploads are scanned for malware before reading; scanning fails closed. Run-form files are processed for text extraction rather than retained as original files. Optional Client files are stored separately. A tamper-evident, exportable evidence log records decisions and workflow steps without client content. Governance metadata may nevertheless be personal data and remains protected.

Resilience and review

INTAI will maintain appropriate recovery arrangements, protect recovery copies, reapply deletion following restoration and regularly assess the effectiveness of its safeguards. The agreement does not represent that the service holds an independent penetration-test report, external certification or a specified recovery-time guarantee.

Incident handling

INTAI maintains an incident and breach procedure covering logging, containment, investigation, assessment, customer notification, supplier incidents and root-cause review. Containment may include disabling real data or a provider, revoking integrations and restricting accounts. Initial customer notice is due within 24 hours under clause 2.5; material updates follow without undue delay. INTAI will maintain response cover and exercise its response arrangements.

Schedule 3 | Providers and AI route conditions

The appointments below are subject to clauses 3.1-3.4. INTAI must maintain equivalent processor contracts, verify relevant access and onward-transfer locations and provide current recipient and safeguard information on request. Regional hosting descriptions are not a guarantee that all supplier support access occurs in that region.

Google Cloud

Infrastructure for hosting, malware scanning, secrets, service logs and optional Client files. App and Client files infrastructure: Belgium, europe-west1. Log bucket locations must be verified independently of the app region. Google supplies infrastructure logging subject to the periods in Schedule 4.

Neon

Database service on AWS eu-west-2, London, United Kingdom. Current point-in-time history: six hours on the configured plan. INTAI must assess and communicate any material change to recovery-copy retention affecting Customer Personal Data.

AWS / Amazon Bedrock

Intended primary AI route. Processing in London, eu-west-2, or specified EEA regions where an approved EU cross-region profile is required. Before real-client use, INTAI must verify the exact model and API route, account/project retention settings, invocation logging, applicable provider terms and all destination regions. A no-training statement alone is not evidence of zero retention.

Anthropic, PBC

Additional direct AI drafting and research route, United States. Before real-client use, INTAI must verify commercial-account retention arrangements and any safety/legal exceptions, relevant feature coverage and search recipients. Restricted transfers must be covered by applicable contractual safeguards, including the EU SCCs with UK Addendum where used, and the required transfer assessment. No UK-US Data Bridge certification is represented by this agreement.

Brevo / Sendinblue SAS

Service email delivery, including invitations and password resets, with no client content included. Reported processing location: France/EU. Account/service email metadata may concern INTAI's own-controller activities. INTAI must minimise email content and set and document an appropriate retention period; this schedule does not promise an account setting not yet applied.

Excluded and separately controlled services

xAI/Grok is restricted to synthetic testing and is not authorised to receive real Customer Personal Data under this version. Introducing real-client use requires prior notice, an opportunity to object and verified contractual, retention and transfer safeguards. OpenAI and Google Gemini are not appointed. Stripe's independent-controller billing activities and the Customer's CRM suppliers are outside these appointments.

International safeguards

UK-to-EEA adequacy arrangements may be used where applicable to the actual transfer. US and other restricted transfers require a lawful mechanism and applicable assessment before activation. INTAI must verify onward transfers and avoid sending Customer Personal Data to an unapproved route, including during fallback or failover.

Schedule 4 | Retention and service closure

Working content

Inputs, extracted document text, drafts and edits follow the Customer's 30, 90 or 180-day setting, default 90 days, then automatic expiry. The applicable timer rules must be disclosed in the service. Any extension for an outstanding check or incident must be necessary, documented, regularly reviewed and limited; it must not become indefinite retention by default.

Uploads and Client files

Run-form originals are malware-scanned and text-extracted without retaining the original file. Extracted form text may be held encrypted for up to two hours while the form is open, then follows working-content retention. Optional Client files are kept until deletion is instructed; ordinary file deletion follows the configured purge window, default 30 days, then a seven-day storage recovery period. At service closure, files are deleted without waiting for the ordinary purge window. A file-retention label must not be represented as automatically enforced where it is not.

Governance evidence

Evidence excludes client content but may contain identifiers, times, decisions and references. The Customer's documented default instruction is to retain its governance evidence for the subscription duration plus six years, with deletion available at closure or on a further lawful instruction. INTAI must not treat absence of client content as proof that the record is anonymous. Any separate-controller retention requires an appropriate basis and disclosure.

Export and closure instructions

At the Customer's choice INTAI will return or delete Customer Personal Data after processing services end. Secure export includes organisation and people records, runs and content, review decisions, stored files, exceptions, incidents and evidence, with file fingerprints. Sign-in secrets and CRM tokens are excluded. Export access must remain available for the agreed closure process; if self-service is unavailable, INTAI will provide an authorised alternative. The Customer may withdraw an unexecuted deletion request.

Active deletion and recovery copies

INTAI will execute an actionable closure-deletion request within five working days, revoke CRM connections, delete active operational content and stored files, and irreversibly anonymise or remove affected user credentials and identifying fields where not lawfully retained. Database history currently expires after six hours, storage recovery copies after seven days and application logs after 30 days. Recovery copies are protected and excluded from ordinary use; deletion is reapplied after restoration.

Confirmation

INTAI will provide written confirmation of return/deletion and the status of recovery-copy expiry within 60 days after processing services end, provided the Customer's choice is recorded by that date. For a later instruction, confirmation is due within 60 days of receipt. Confirmation must identify its scope and retained categories; it must not claim that every supplier or independently controlled record has expired. INTAI may retain a minimised closure certificate for accountability.

Lawful exceptions and Google infrastructure logs

A subscription or open incident alone does not establish a legal hold. Any legally required retention must identify its basis, scope, safeguards and review/end point, with customer notice unless prohibited. Google _Required infrastructure audit logs have a 400-day period; some other audit logs fall in _Default. INTAI must assess any Customer Personal Data in those records and lawfully address it rather than assume a provider policy overrides deletion duties. Billing, contract and sign-up records processed by INTAI as controller follow its separately disclosed lawful periods. Records in the Customer's own CRM remain under its control.