

Privacy Policy

SynaptechOne web application, client mobile application and synaptech.in

Synaptech AI Technology Services LLP | LLPIN ACD-2132 | Incorporated 3 October 2023 | Effective 11 October 2026

Effective 11 Oct 2026

This Privacy Policy explains how Synaptech AI Technology Services LLP ("Synaptech", "we", "us") handles personal data when you use SynaptechOne, our website at <https://synaptech.in>, and related support services. It is effective from 11 October 2026.

At a glance

- Your practice controls the client records it creates or maintains in its SynaptechOne workspace. Synaptech processes that workspace data to provide the service and does not acquire ownership of it.
- You retain rights in your personal data under applicable law. For records managed by a practice, contact that practice first; Synaptech assists the practice when appropriate.
- Core SynaptechOne application data, uploaded documents, backups and operational logs are hosted in AWS Mumbai, India. Certain authentication or notification providers may process limited technical data outside India.
- We do not sell personal data or use it to serve targeted advertising.

1. Who is responsible for the data?

For client records entered, uploaded or managed by an accounting or tax practice - including client identities, registrations, documents, tasks, messages, invoices and practice-authorized Tally information - the practice determines the purposes and means of processing and is responsible for its lawful handling. In data-protection terminology, the practice is generally the Data Fiduciary/controller for those records and Synaptech acts as its service provider/Data Processor, following the practice's documented instructions and our agreement.

This does not transfer ownership of personal data to the practice or remove an individual's statutory rights. The practice retains its rights and control in the business

records and content it provides, subject to the rights of the individuals and other rights holders concerned.

Synaptech separately determines how it uses limited data needed to operate SynaptechOne accounts and sign-in, subscriptions and payments owed to Synaptech, Tally-access fees paid to Synaptech, support requests, service security and platform administration. For those activities, Synaptech is responsible for its own processing under applicable law.

2. What information we handle

People / source	Information
Practice owners and staff	Name, business email, contact details, practice/role and permissions, Google Sign-In identifiers and authentication results, session/device/security logs and feature data such as work entries or compensation information where the practice uses those features.
Practice clients and client-app users	Names and contact details; addresses and business details; PAN, GSTIN, TAN and other registration identifiers when supplied; tasks, deadlines, documents, messages, filing artefacts, invoices, payments and content shared with the practice.
Tally-access users	Ledger and report information returned from the practice's authorised Tally company, statement/PDF outputs, access entitlements, payment references and service diagnostics necessary to provide the enabled read-only service.
Google sign-in and device authentication	Limited account/profile information provided by Google Sign-In, such as a provider identifier, name and email address where shared; device/app identifiers and authentication status. Optional Face ID/fingerprint checks are handled locally by the device operating system; Synaptech does not receive raw face scans, fingerprint images or biometric templates.
Payments	For Synaptech payments and practice invoice payments, transaction status, amount, currency, Razorpay

People / source	Information
	payment/reference identifiers, and related refund/reconciliation information. Razorpay handles payment credentials; Synaptech does not ordinarily receive a full card number or UPI PIN.
Referrers and leads	Contact and referral information entered by the practice, including tax or registration details only where the feature requires and the practice is entitled to provide them.
Website visitors and support requesters	Contact details, practice name, support correspondence, IP address, browser/device information and request/security logs reasonably needed to respond and protect the service.
Notifications and operations	Push-notification token, app version, event/request time and technical logs where push notifications or the relevant operational feature is enabled.

Please do not submit passwords, UPI PINs, full card credentials or unnecessary sensitive personal information in support messages or documents.

3. Why we use information

- To provide SynaptechOne features selected by a practice: account access, practice/client workflows, task and document handling, reminders, client communications, authorised Tally ledger/report viewing and PDF statements.
- To administer subscriptions, billing, invoices, payment processing, refunds, reconciliation and customer support.
- To maintain access controls, tenant separation, service reliability, fraud prevention, security monitoring, incident investigation and backups.
- To comply with applicable law, lawful requests, accounting/tax obligations and cybersecurity incident-reporting duties.
- Where enabled, to scan uploads for malware and use limited diagnostic/crash information to detect and fix service failures. We do not use these functions for targeted advertising. Optional analytics/diagnostic providers will not be activated without an appropriate purpose and provider review; this policy or the related provider schedule will be updated where required.

4. Legal grounds and choices

We handle information as needed to provide requested services, perform contracts, follow the practice's instructions for workspace data, meet legal obligations, protect the service and pursue legitimate operational interests permitted by applicable law. Where applicable law requires consent, we will obtain it in an appropriate and specific way and provide a way to withdraw it. A practice is responsible for giving its clients the notices and obtaining permissions it is required to provide or obtain for records it places in SynaptechOne.

Google Sign-In is an authentication service. Google may process information under its own terms and privacy policy. Biometric unlock, if enabled, is performed by the operating system on your device and is not a method by which Synaptech collects biometric templates. Your device may not offer the same biometric options on every platform.

5. Who receives information and where it is processed

Recipient / category	Purpose and information
Amazon Web Services (AWS), Mumbai region	Core application hosting, database, object/document storage and backups, subject to the production configuration.
Google Sign-In	Authentication. Google receives information as described in Google's applicable terms; Synaptech receives the sign-in result and permitted account attributes needed for the account.
Razorpay	Payment checkout, payment confirmation, refunds and reconciliation for Synaptech fees and, where the practice has configured it, practice payments.
Expo and Google Firebase Cloud Messaging, where enabled	Delivery of push notifications. These providers may receive a device push token, routing information and notification text needed to deliver a message. We instruct the platform not to put confidential tax documents or ledger contents in notification text.
Email and operational service providers	Delivering account/support communications and protecting or maintaining the service. Providers are selected and

Recipient / category	Purpose and information
	configured for the task; material provider changes will be reflected in the policy or provider schedule as required.
Practice and its authorised users	Access to workspace information under the practice's permissions and role assignments.
Authorities or professional advisers	Only where required or permitted by law, to establish/defend legal claims, or for a documented compliance or security purpose.
Corporate transaction successor	If a merger, restructuring or sale occurs, subject to confidentiality, appropriate safeguards and applicable law.

Core SynaptechOne data is intended to remain in AWS Mumbai, India. Google identity services, push-notification services and some other third-party systems may process limited account or technical data in other jurisdictions under their global infrastructure. Accordingly, we do not claim that every item of information remains in India. Tally source data may remain on a practice-hosted server or on a Synaptech-hosted server, depending on the practice's arrangement. Data copied into SynaptechOne is handled under this Policy.

We do not sell or rent personal data. We do not share practice records for advertising. We limit provider access to what is needed to deliver the relevant function.

6. Ownership and instructions for practice data

The practice and/or relevant client retains rights in the records, files, messages, business information and other content it supplies or generates, subject to the rights of individuals and other rights holders. Synaptech receives only the limited right to host, transmit, store, back up, display, retrieve and otherwise process that content for the purposes of delivering, securing, supporting and improving the contracted service in line with the practice's instructions and applicable law. We do not sell, license for advertising, or independently exploit practice client records.

The practice is responsible for its account users, role assignments, legal basis and notices for client data, accuracy of source records, professional advice and filings, and

responding to its clients' data requests. Synaptech will reasonably assist where a request relates to our processing systems.

7. Retention and deletion

- Active practice records: retained while the practice uses the service and for the period directed by the practice or needed to provide the contracted service, subject to legal obligations and valid requests.
- When a practice leaves: the practice can export its data for at least 90 days after the subscription ends. After that window, Synaptech may begin deleting or anonymising data that is no longer needed and that Synaptech is not legally required or otherwise entitled to retain. We may retain records longer where required by tax/accounting law, for security/audit purposes, to handle a dispute or chargeback, to establish or defend legal claims, or to comply with a lawful direction.
- Tally-derived data and statements: retained for the period needed to provide the enabled Tally service and in accordance with the practice's document-retention choices and applicable legal requirements. A statement saved into a client's document file follows the applicable document-retention policy.
- Payment, tax and billing records: retained for applicable statutory/accounting periods and to handle refunds, chargebacks, audits and disputes.
- ICT/system logs: maintained for a rolling period of at least 180 days within India where required by applicable CERT-In directions, and longer where required for incident investigation, legal compliance or dispute handling.
- Backups: backup copies are access-restricted and retained under a controlled rotation schedule. A deleted record may remain temporarily in a backup until that backup expires; backup deletion is not necessarily simultaneous with deletion from live systems. After a restore, deletion requests will be reapplied through the operational process where applicable.
- Support requests and demo leads: retained for the time needed to respond, manage follow-up, keep necessary business records and protect against misuse; they are deleted or anonymised when no longer needed, except for a lawful retention basis.

We do not promise that every record is erased exactly on day 90. The 90-day period is the minimum export window, not a universal statutory retention limit. Data that law requires us to keep is not erased merely because a practice or user asks to close an account.

8. Security

We apply technical and organisational safeguards appropriate to the sensitivity of the information and the service, which may include encrypted network connections, access controls and least-privilege permissions, practice-level access boundaries, security logging, protected cloud infrastructure, backups and incident response. The controls applicable to a particular feature depend on its implementation and configuration. No internet service can be guaranteed perfectly secure. Practices must maintain suitable access permissions and safeguard their own devices, credentials and Tally environments.

If an incident affects practice data, Synaptech will notify the affected practice without undue delay and cooperate on investigation and any notifications required by applicable law. We may also notify affected individuals or authorities where we are legally required to do so.

9. Your requests and rights

For client records held on a practice's instructions, contact the practice first. The practice determines how to respond and may ask Synaptech to assist. For your Synaptech account, sign-in information, payments made to Synaptech or this website, contact privacy@synaptech.in. You may request access to information, correction, completion, update or deletion where available under applicable law; object or withdraw consent where the applicable processing depends on consent; and raise a grievance. Legal, tax, security and record-retention obligations can limit deletion or other requests.

We aim to acknowledge a grievance within 48 hours and resolve it within 30 days, unless a shorter legal deadline applies or the issue requires a reasonable additional period, in which case we will explain the status. You may approach the Data Protection Board of India or another competent authority where permitted by applicable law.

10. Cookies, app storage and diagnostics

The website and web application may use essential cookies or similar local storage required for sign-in, session security and core functionality. The mobile app may store a session credential in platform-protected storage to support sign-in and, if enabled, local biometric unlocking. We do not use advertising cookies or targeted-advertising trackers. Where crash reporting, service diagnostics, malware scanning or analytics is enabled, we limit it to a documented operational purpose and update the relevant provider information

where required. External webpage resources, if loaded, may receive standard request information such as an IP address and browser metadata.

11. Children and records relating to minors

The client app is designed for adult users. A practice must not use SynaptechOne to process a child's personal data unless it has the authority and verifiable parent/guardian consent or other lawful basis required by applicable law. The practice must configure and use the service consistently with its professional and legal duties.

12. Changes to this Policy

We may update this Policy when the service, providers or law changes. We will publish a new effective date and give notice of material changes through the service or by email where appropriate. Where a new consent or acknowledgement is legally required, we will request it separately and record it.

Contact details

Synaptech AI Technology Services LLP (LLPIN ACD-2132)

Privacy concerns: privacy@synaptech.in

General support: care@synaptech.in | 10:00-20:00 IST on working days