

JOHN THOMAS FINTECH PRIVATE LIMITED

PRIVACY POLICY AND INFORMATION SECURITY NOTICE

Prepared with reference to the Digital Personal Data Protection Act, 2023 and Rules, 2025; ISO/IEC 27001:2022; and Indian laws and RBI requirements applicable to accounting, SaaS, ERP, NBFC and financial-institution software

Effective date: [date of publication 22 October 2026] | Version 2.0 (Draft)

CIN: U62099KL2026PTC106017 | Ernakulam (Kochi), Kerala, India



Table of Contents

1. Introduction, Scope and Our Roles
2. Key Terms
3. Who We Are and How to Reach Us
4. Personal Data We Collect
5. Why We Process Personal Data and On What Basis
6. Notice, Consent and Consent Managers
7. Artificial Intelligence Features
8. Sharing and Disclosure
9. Data Location and Cross-Border Transfers
10. Data Retention and Deletion
11. Information Security (ISO/IEC 27001:2022)
12. Personal Data Breach and Incident Response
13. Your Rights as a Data Principal
14. Our Role as Data Processor for Customers
15. Our Role as a Technology Provider to NBFCs, Banks and Financial Institutions
16. Indian Laws and Regulations We Design For
17. Cookies and Tracking Technologies
18. Children's Data
19. Your Responsibilities as a Customer or User
20. Significant Data Fiduciary Obligations
21. Changes to This Policy
22. Grievance Redressal
23. Governing Law and Jurisdiction
24. Contact Us
- Annex A: Sub-processor Register
- Annex B: Pre-publication Checklist (delete before publishing)

1. Introduction, Scope and Our Roles

John Thomas Fintech Private Limited ("**we**", "**us**", "**our**", "**the Company**") develops and provides cloud software for businesses and the financial services industry. Our products include **John Thomas Fin Accounting (AI Powered)**, the **Unify Suite** (Accounting, CRM, HRM and related modules), our websites, mobile and web applications, and application programming interfaces (together, the "**Services**").

This Policy explains what personal data we collect, why, how we protect it, who we share it with, how long we keep it, and what rights you have. It also explains the security framework we follow and how we support customers that are regulated entities, such as NBFCs, banks and other financial institutions.

1.1 The three roles we play

Role	When it applies	Who decides how data is used
Data Fiduciary (DPDP Act)	Personal data we collect for ourselves: website visitors, people who sign up, account owners and authorised users, billing contacts, support requests, job applicants, marketing leads.	We do.
Data Processor (DPDP Act)	Personal data our customers put into the Services: employee and payroll records, customer and vendor records, invoices, ledgers, borrower or client records and uploaded documents.	The customer, who is the Data Fiduciary. We act only on its documented instructions (Section 14).
Technology service provider to a regulated entity	Where the customer is an NBFC, bank, insurer, broker or other entity regulated by RBI, SEBI, IRDAI or similar bodies, and uses our Services in its regulated activities.	The regulated entity remains responsible to its regulator. We support it under the outsourcing agreement (Section 15).

We are a software and technology company. Unless and until we hold the relevant licence, we do not accept deposits, lend, operate a payment system, sell insurance or provide investment advice through the Services. Where our group later does so through a separately licensed entity, that entity will publish its own notice, and we will not share your data with it without your separate, specific consent.

1.2 Legal framework and timing

The Digital Personal Data Protection Act, 2023 ("**DPDP Act**") and the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") were notified in stages. The Data Protection Board of India was established from 13 November 2025. The provisions on Consent Managers apply from 13 November 2026. The remaining provisions, including notice, consent, security safeguards, breach intimation and Data Principal rights, apply from **13 May 2027**.

Until 13 May 2027 the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**SPDI**")

Rules") continue to apply. We have chosen to meet the DPDP standard now, and we also meet the SPDI Rules for as long as they remain in force. Where this Policy refers to a right or duty that begins on 13 May 2027, we apply it as good practice before that date.

2. Key Terms

Term	Meaning in this Policy
Personal data	Any data about an individual who is identifiable by or in relation to that data.
Data Principal	The individual to whom personal data relates. For a child, this includes the parent or lawful guardian.
Data Fiduciary	The person who alone or together with others decides the purpose and means of processing personal data.
Data Processor	A person who processes personal data on behalf of a Data Fiduciary.
Customer	A business or organisation that subscribes to the Services.
Customer Data	All data, including personal data, that a Customer or its users enter into or generate through the Services.
Regulated Entity	A Customer that is regulated by the Reserve Bank of India or another financial-sector regulator.
Board	The Data Protection Board of India.
ISMS	Information Security Management System, as described in ISO/IEC 27001:2022.

3. Who We Are and How to Reach Us

Field	Detail
Company name	John Thomas Fintech Private Limited
CIN	U62099KL2026PTC106017
Registered office	69/1854 A, A1, A2, SRM Rd, Ernakulam North, Ernakulam, Kerala – 682018, India
Data protection contact (queries about this Policy and your rights)	[John Thomas], [CEO & MD]
Grievance Officer	[John Thomas], [CEO & MD]
Information Security Officer	[John Thomas], [CEO & MD]
Email	johnthomas@johnthomasfintech.com
Phone	+91 8210700278

The DPDP Act requires us to publish the business contact details of a person who can answer your questions about the processing of your personal data. The details above serve that purpose. If we are ever notified as a Significant Data Fiduciary, we will also appoint a Data Protection Officer based in India (Section 20).

4. Personal Data We Collect

4.1 Data you give us

- **Account and contact data:** name, email address, phone number, company name, designation, billing address.
- **Business identity data:** PAN, GSTIN, CIN, TAN and similar details needed to set up your account, issue invoices and meet our legal duties.
- **Payment data:** subscription billing details. Card and bank details are handled by our payment processor and are not stored on our systems in full.
- **Communications:** support tickets, emails, chat messages, call recordings (where we tell you in advance) and feedback.
- **Recruitment data:** if you apply for a job with us, your CV, contact details, education and work history.

4.2 Data collected automatically

- **Usage and audit data:** pages visited, features used, timestamps, and in-app activity logs.
- **Device and technical data:** IP address, browser type, device identifiers, operating system, language setting.
- **Security logs:** authentication events, access to records, administrative actions and system events, kept as described in Section 10.
- **Cookies and similar technologies:** as described in Section 17.

4.3 Customer Data we process for our Customers

When you use the Services, you may enter personal data about other people. Examples are accounting and tax records, GST and TDS data, invoices, customer and vendor details, employee records (names, PAN, bank account, salary, attendance, provident-fund and insurance details), and, for Regulated Entities, borrower and client records. We process this data as a Data Processor (Section 14).

4.4 Data we do not seek

- We do not intentionally collect biometric data, health data, caste, religion or political opinions. Please do not upload them unless your use case needs them and you have a lawful basis.
- **Aadhaar numbers:** the Aadhaar Act, 2016 restricts who may collect and store Aadhaar numbers. We do not require Aadhaar to use the Services. If a Customer's lawful workflow involves Aadhaar, the Customer is responsible for that lawful basis, and we will support masking and restricted storage.
- We do not buy personal data from data brokers.

5. Why We Process Personal Data and On What Basis

The DPDP Act allows processing on the basis of your consent or for certain "legitimate uses". We use the grounds below. Where we process as a Data Processor, the Customer determines the ground.

Purpose	Examples	Basis
Provide and operate the Services	Creating accounts, recording transactions, generating invoices and reports, running AI features you ask for	Consent; and legitimate use where you voluntarily give data for a stated purpose
Billing and account administration	Invoices, payment confirmation, plan changes	Consent; legal obligation (tax and accounting law)
Communicate with you	Service notices, security alerts, support replies	Legitimate use (response to your request); consent
Security, fraud prevention and abuse detection	Monitoring logins, blocking suspicious activity, investigating incidents	Legitimate use (legal obligation and security safeguards); consent
Meet legal and regulatory duties	Tax records, statutory filings, CERT-In reporting, responding to lawful orders	Legitimate use (compliance with law and orders)
Improve the Services	Fixing bugs, measuring performance, planning features, using de-identified usage statistics	Consent; de-identified data where possible
Marketing	Product updates, offers, newsletters	Consent only. You can opt out at any time
Recruitment	Assessing job applications	Consent

We use personal data only for the purposes for which we gave notice. If we want to use it for a new purpose, we will ask again.

6. Notice, Consent and Consent Managers

- **Itemised notice.** Before we ask for consent, we tell you in clear, plain language what data we want, why, how to withdraw consent, how to complain to us and to the Board, and how to exercise your rights.
- **Free, specific and unbundled.** Consent for one purpose is not tied to another. We do not use pre-ticked boxes or interface designs that push you toward consent (dark patterns).
- **Language.** Notices are available in English and, as we expand, in other languages listed in the Eighth Schedule to the Constitution [Hindi].
- **Withdrawal.** You can withdraw consent as easily as you gave it, through account settings or by writing to us. Withdrawal does not affect processing done before it. If the data is needed to provide a feature, that feature may stop working.

- **Consent Managers.** From 13 November 2026, you may manage consent through a Consent Manager registered with the Board. We will honour requests that arrive through a registered Consent Manager
- **Records.** We keep records of notices given and consents received so that we can demonstrate compliance.

7. Artificial Intelligence Features

Some of our Services use machine-learning or generative AI to help with tasks such as classifying transactions, reading invoices, drafting entries and answering questions about your books. We handle AI features as follows :

- **No training on Customer Data without your permission.** We do not use Customer Data to train or fine-tune models that serve other customers unless you opt in in writing.
- **Provider terms.** If we send content to a third-party AI model provider, that provider is a sub-processor listed in Annex A, is bound by confidentiality and security terms, and is not permitted to use the content to train its own models.
- **Human oversight.** AI output is a suggestion. Accounting entries, tax computations and filings should be reviewed by a qualified person before use. AI output can be wrong.
- **No solely automated decisions about individuals.** We do not use AI to make decisions that produce legal or similarly significant effects on an individual without human review.
- **Minimisation.** We send only the data needed for the task and mask identifiers where practical.

8. Sharing and Disclosure

We do not sell personal data. We share it only as follows:

- **Service providers and sub-processors** that host, secure, support or deliver the Services, such as cloud hosting, payment processing, email and messaging delivery, customer support tools, analytics and AI providers. Each is bound by a written contract that requires confidentiality, appropriate security, use only on our instructions, and deletion or return of data at the end of the engagement. The current list is in Annex A.
- **Within our group,** only to the extent needed for a service you requested, and never for a regulated group entity's own purposes without your separate, specific consent.
- **Regulators, courts and authorities,** where required by law, court order or a lawful request. For Regulated Entities, this includes supporting inspection and audit by their regulators.
- **Business transfers.** In a merger, acquisition or asset sale, the buyer must be bound by materially equivalent protections, and we will tell you.
- **Professional advisers,** such as auditors and lawyers, under confidentiality duties.
- **With your consent,** for any other purpose we disclose when we ask.

9. Data Location and Cross-Border Transfers

- **Primary storage in India.** Production data is stored in data centres located in India AWS India Mumbai location.

- **Books of account.** Backups of electronic books of account and related records are kept on servers physically located in India, as the Companies (Accounts) Rules, 2014 require for our Customers.
- **Regulated-sector data.** For Regulated Entities, we follow their instructions on data location, including RBI requirements on storage of payment system data and digital-lending data in India, where those apply to them.
- **Security logs** are retained within Indian jurisdiction, as the CERT-In Directions of 28 April 2022 require.
- **Transfers outside India.** If personal data is processed outside India (for example, by a support tool or AI provider), we do so only to countries not restricted by the Central Government under Section 16 of the DPDP Act, under contract, and never in a way that breaches a sectoral rule or a Customer instruction. As of the date of this Policy, no restricted-country list has been notified.

10. Data Retention and Deletion

We keep personal data only as long as needed for the purpose it was collected for, or as the law requires. Statutory retention for accounting records can be longer than the time you might want data erased. In that case the law prevails and we will tell you what we are keeping and why.

Data	Retention	Reason
Accounting records, books of account and audit trail (edit log)	At least 8 years from the end of the financial year to which they relate, or longer if the Customer instructs or the law requires	Companies Act, 2013 (Section 128); Companies (Accounts) Rules, 2014; tax and GST law
Know-your-customer and anti-money-laundering records held for a Regulated Entity	As the Regulated Entity instructs, and not less than the period its law requires	Prevention of Money-Laundering Act, 2002 and RBI KYC requirements (the Regulated Entity's duty)
Payroll and employee records processed for a Customer	As the Customer instructs, subject to labour and tax law	Customer's statutory duties
Account and billing data (our own)	Duration of the subscription plus [1 month], then up to the longer of that period and any legal requirement	Contract administration; tax law
Security, access and system logs	At least one year (and never less than 180 days, kept in India)	DPDP Rules security safeguards; CERT-In Directions
Consent and notice records	[7 years]	To demonstrate compliance
Support tickets and communications	[3 years]	Service quality and dispute handling
Marketing contacts	Until you withdraw consent	Consent

Data	Retention	Reason
Job applications	[12 months] unless you ask us to delete earlier	Recruitment
Backups	Rolling [35 days]; backups age out on schedule	Resilience

10.1 End of contract

When a subscription ends, the Customer can export its data for [30] days. After that we delete or irreversibly anonymise Customer Data within [90] days, except what the law requires us to keep, and on request we confirm deletion in writing. For Regulated Entities we follow the exit and data-return terms in the outsourcing agreement.

11. Information Security (ISO/IEC 27001:2022)

11.1 Our approach

We run our security programme as an Information Security Management System aligned with **ISO/IEC 27001:2022**. The ISMS follows the standard's management clauses: understanding our context and interested parties (including regulators and Customers); leadership commitment and a board-approved security policy; risk assessment and risk treatment, recorded in a Statement of Applicability; competence, awareness and documented information; operational controls; monitoring, internal audit and management review; and corrective action and continual improvement.

Certification status

[We operate an ISMS designed to meet ISO/IEC 27001:2022 and are preparing for independent certification. We do not currently hold an ISO/IEC 27001 certificate.]

11.2 Controls, by the four themes of Annex A

ISO/IEC 27001:2022 Annex A has 93 controls in four themes, including 11 new controls. We apply the controls our risk assessment shows are relevant. These are the main ones, with the new 2022 controls marked (new).

Theme	What we do
Organisational controls	Information security policies, defined roles and segregation of duties; an owner for every system and data set; classification and handling of information. Threat intelligence (new) from CERT-In advisories and vendor bulletins. Supplier due diligence, security terms in contracts and monitoring of sub-processors. Security of cloud services (new): documented rules for selecting, using and exiting cloud services; shared-responsibility mapping. Incident management with defined roles; ICT readiness for business continuity (new): disaster-recovery plans with set recovery-time and recovery-point target one day, tested annually A register of legal, regulatory and contractual requirements (Section 16), and independent review of the ISMS.
People controls	Background verification for staff with access to Customer Data, where the law allows. Confidentiality undertakings, security duties in employment terms, a disciplinary process. Security and privacy awareness training on joining and at least [annually]; phishing exercises. Rules for remote work; a simple way to report security events.
Physical controls	Production systems run in third-party data centres that hold their own independent security certifications [confirm]. Secured offices, visitor control, clear-desk and clear-screen rules, managed disposal of devices and media. Physical security monitoring (new) at our premises.

Theme	What we do
Technological controls	Strong authentication, multi-factor authentication for administrators and available to all users; role-based access and least privilege; privileged-access reviews. Encryption in transit (TLS 1.2 or higher) and at rest (AES-256 or equivalent), with managed keys and rotation. Cryptography is documented in our key-management standard. Logical separation of each Customer's data (tenant isolation). Configuration management (new), vulnerability management and timely patching; anti-malware and endpoint protection. Data masking (new) in non-production systems and support tools; data-leakage prevention (new) on email and endpoints; web filtering (new). Information deletion (new) on schedule and on request, as in Section 10. Monitoring activities (new) with central logging, alerting and review; clocks synchronised to the National Informatics Centre or National Physical Laboratory time sources, as CERT-In requires. Secure development lifecycle and secure coding (new): code review, dependency scanning, separation of development, test and production, and test data protection. Daily backups with restore tests; redundancy for critical services. Immutable audit trail on accounting records that cannot be switched off (Section 16).

11.3 Independent assurance

We commission vulnerability assessment and penetration testing by an independent, preferably CERT-In-empowered, auditor at least **annually** and after major releases, fix findings by risk, and run internal ISMS audits and management reviews. For Regulated Entities, we share relevant summaries under confidentiality. We use ISO/IEC 27017 (cloud security), ISO/IEC 27018 (protecting personal data in public cloud) and ISO/IEC 27701 (privacy information management) as reference guidance for our controls.

No system is completely secure. If you suspect a security issue, write to us at the contact in Section 3.

12. Personal Data Breach and Incident Response

We maintain a written incident-response plan with defined roles, severity levels, evidence handling and post-incident review. In an incident:

- **CERT-In.** We report cybersecurity incidents within 6 hours of noticing them or being told of them, as the CERT-In Directions require (incident@cert-in.org.in).
- **Customers.** We tell affected Customers without undue delay and give them the facts they need to meet their own duties **target: within 24 hours of confirmation**. For Regulated Entities, we notify fast enough for them to meet RBI reporting timelines, as agreed in the contract.
- **The Data Protection Board and affected individuals.** Where we are the Data Fiduciary, we inform the Board and each affected Data Principal without delay after becoming aware of a

personal data breach. The notice to individuals is in plain language and says what happened, the likely harm, what we have done, what you can do, and who to contact. We give the Board fuller details within 72 hours, or any longer period it allows.

- **Learning.** We record the cause, the response and the fixes, and keep evidence.

13. Your Rights as a Data Principal

Under the DPDP Act you have the right to:

- **Access** a summary of the personal data we process about you, the processing activities, and the identities of the other Data Fiduciaries and Data Processors we have shared it with, with a description of that data.
- **Correction, completion and updating** of inaccurate, incomplete or out-of-date data.
- **Erasure** of data that is no longer needed for the purpose, or where you withdraw consent, unless the law requires us to keep it (Section 10).
- **Withdraw consent** at any time (Section 6).
- **Grievance redressal.** To have your complaint heard by us first (Section 22).
- **Nominate** another person to exercise your rights if you die or become incapable.

To exercise a right, write to the data protection contact in Section 3 and tell us who you are, so we can verify the request. We aim to reply within **[30]** days and in any case within the period set by the DPDP Rules. If your data is in a Customer's account, we will pass your request to that Customer, because it is the Data Fiduciary for that data (Section 14).

The DPDP Act also places duties on Data Principals: to comply with the law, not to impersonate anyone, not to hide material information, not to file false or frivolous complaints, and to give only verifiably authentic information when asking for correction or erasure. Breach of these duties can attract a penalty under the Act.

14. Our Role as Data Processor for Customers

For Customer Data, the Customer is the Data Fiduciary. Under the DPDP Act a Data Fiduciary may use a Data Processor only under a valid contract. Our customer agreement, with its data processing terms, provides that we will:

- process Customer Data only on the Customer's documented instructions and for the purposes of providing the Services, and never for our own marketing or to build profiles;
- keep Customer Data confidential and limit access to staff who need it;
- maintain the security safeguards in Section 11, and tell the Customer of a breach without undue delay (Section 12);
- engage sub-processors only with equivalent obligations, and keep the list in Annex A current and give notice of changes **[24 hours]**;
- help the Customer respond to rights requests and grievances from its employees, clients and other individuals, and pass requests we receive to the Customer;
- help the Customer with audits, regulator requests and impact assessments;
- return or delete Customer Data at the end of the contract (Section 10.1).

Customer duties. Customers are responsible for having a lawful basis, giving notices and obtaining any needed consents from their own employees, clients and others, for the accuracy of the data, and for answering rights requests. A Customer using the HRM module should make sure its own employee privacy notice explains that a processor is used.

15. Our Role as a Technology Provider to NBFCs, Banks and Financial Institutions

A Regulated Entity that uses our Services stays fully responsible to its regulator for the outsourced activity. RBI's directions on managing risks in outsourcing, including outsourcing of IT services and use of cloud services, set out what a regulated entity must require from its service provider. Whatever the entity's type or layer, we are ready to agree contract terms that support these, and we commit to the following:

- **Written outsourcing agreement** that defines scope, service levels, security and confidentiality duties, sub-contracting, data ownership, liability and exit.
- **Audit and inspection access** for the Regulated Entity, its auditors and its regulator, including to our relevant records, logs and facilities, and to those of material sub-contractors.
- **Data segregation and confidentiality.** Each Regulated Entity's data is logically separated from other customers' data, and we do not use it for any purpose other than providing the Services.
- **Data location.** Storage in India, and originals of records kept in India, where the Regulated Entity's directions require it.
- **Prompt incident reporting** to the Regulated Entity, in time for it to report to the regulator [6 hours].
- **Business continuity and disaster recovery,** tested and available for review, with agreed recovery targets.
- **Sub-contractor controls:** consent, flow-down of the same obligations and auditability.
- **Exit:** orderly transition, return of data in a usable format, and certified secure deletion afterwards.
- **Customer rights are not diluted.** Complaints from a Regulated Entity's customers about outsourced activities remain the entity's responsibility. We cooperate in resolving them, and we do not contact its customers directly unless instructed.
- **Key control.** Where the Regulated Entity needs it, we support customer-managed encryption keys .

Our Services do not make credit, insurance or investment decisions for a Regulated Entity unless the contract expressly says so, and the Regulated Entity remains accountable for every such decision, for its KYC and anti-money-laundering programme, and for its dealings with credit information companies, Account Aggregators and payment systems.

16. Indian Laws and Regulations We Design For

The table lists the main laws and requirements that shape our Services and how we address them. Some apply to us directly. Others apply to our Customers, and we build the Services to let them comply.

Law or requirement	How we address it
Digital Personal Data Protection Act, 2023 and Rules, 2025	Notice, consent, purpose limitation, minimisation, accuracy, security safeguards, breach intimation, retention limits, Data Principal rights, grievance redressal and processor contracts, as described in this Policy.
Information Technology Act, 2000 , including Sections 43A, 72A and 70B, and the SPDI Rules, 2011 (until superseded)	Reasonable security practices, written privacy policy, consent for sensitive personal data (such as financial information and passwords), grievance officer, and protection against disclosure without consent.
CERT-In Directions of 28 April 2022	Incident reporting within 6 hours; logs kept for at least 180 days within India; clock synchronisation; a designated point of contact.
Companies Act, 2013 (Section 128) and Companies (Accounts) Rules, 2014 (Rule 3)	An audit trail of every change to books of account, recording the date of the change and who made it, that cannot be disabled; retention of the audit trail for at least 8 years; daily backups kept on servers in India; books accessible in India.
Income-tax law (the Income-tax Act, 1961 and the Income-tax Act, 2025, as applicable) and the CGST Act, 2017	Record-keeping features, e-invoicing and e-way-bill integrations, and tax portal connections that run only with the Customer's authorisation and credentials.
RBI directions on managing risks in outsourcing (including IT services and cloud)	Contract terms and operating practice described in Section 15, for Regulated Entities that are our Customers.
RBI directions on IT governance, risk, controls and assurance, and on cyber resilience	Controls in Section 11 aligned so that Regulated Entities can evidence their own compliance when they use our Services.
RBI digital lending directions and storage of payment system data	Data location in India and consent, purpose and data-minimisation features, for Regulated Entities that use our Services in lending or payments.
Prevention of Money-Laundering Act, 2002 and RBI KYC requirements	Retention and confidentiality of KYC records as the Regulated Entity instructs. We do not carry out KYC unless we are contracted and permitted to.
Credit Information Companies (Regulation) Act, 2005	Credit information is accessed only through members authorised under the Act, by Regulated Entities that are permitted to do so, and is not used for any other purpose.
Aadhaar Act, 2016	No Aadhaar collection by us without lawful authority; masking and restricted storage where a Customer's lawful workflow involves Aadhaar.
Account Aggregator framework (RBI)	Where a feature connects through an RBI-licensed Account Aggregator, data flows only under a valid consent artefact and for the stated purpose.

Law or requirement	How we address it
Sector rules for Customers regulated by SEBI, IRDAI, PFRDA or NPCI	We support their cyber-security and outsourcing requirements under contract, as applicable.
Labour and social-security laws (EPF, ESI, wages and related codes)	Payroll and HRM features process employee data for the Customer's statutory duties.
Consumer Protection Act, 2019 and E-Commerce Rules, 2020; Guidelines on Prevention of Dark Patterns, 2023	Clear pricing and terms, a grievance mechanism, and consent and cookie screens free of dark patterns.

Laws and directions change. We review this register at least **[every six months]** and whenever a significant change is notified, and we update this Policy when needed. We do not claim any licence, registration or empanelment that we do not hold.

17. Cookies and Tracking Technologies

We use cookies and similar technologies on our website and applications. When our cookie banner is live, you will be able to accept or reject each category separately, with the same ease. Strictly necessary cookies do not need consent.

Category	Purpose	Consent needed
Strictly necessary	Sign-in, session security, load balancing, remembering consent choices	No
Functional	Language and display preferences	Yes
Analytics	Understanding how the Services are used [name tools]	Yes
Marketing	Measuring campaigns [none are used]	Yes

You can also control cookies through your browser settings. Blocking some cookies may affect how the Services work.

18. Children's Data

The Services are for business use by adults. Under the DPDP Act, a child is a person under 18. We do not knowingly collect personal data of children for our own purposes. We never track or monitor the behaviour of children or direct advertising at them, and we do not process their data in a way that is likely to harm their well-being. If we learn that we hold a child's data without verifiable consent from a parent or lawful guardian, we will delete it. A Customer that enters records about minors (for example, apprentices or dependants in HR records) is responsible for the lawful basis and parental consent.

19. Your Responsibilities as a Customer or User

- Keep your sign-in credentials secret, use multi-factor authentication, and remove access for people who leave your organisation.
- Enter only data you are entitled to enter, and keep it accurate.
- Give your employees, clients and other individuals the notices the law requires and obtain any needed consent.
- Tell us promptly of any suspected unauthorised access to your account.
- Follow your own regulator's rules if you are a Regulated Entity.

20. Significant Data Fiduciary Obligations

The Central Government may notify a Data Fiduciary as a "Significant Data Fiduciary" based on the volume and sensitivity of data, risk to individuals and other factors. We do not presently expect to be one, but if we are notified we will appoint a Data Protection Officer based in India who reports to our board, appoint an independent data auditor, carry out periodic data protection impact assessments and audits, and observe any further measures the Rules prescribe. We will update this Policy accordingly.

21. Changes to This Policy

We update this Policy when our practices, the Services or the law change, including as the DPDP Act comes fully into force on 13 May 2027. We post the new version with a new effective date and keep earlier versions on request. For material changes we give advance notice by email or in the application, and where the law requires fresh consent we ask for it again.

Version	Date	Summary
1.0	[22 nd October 2026]	Initial draft under the DPDP Act, 2023
2.0	[22 nd October 2026]	Added ISO/IEC 27001:2022 alignment, sector and RBI requirements for NBFC and financial-institution customers, AI, retention schedule, incident handling and sub-processor register

22. Grievance Redressal

If you have a concern about how we handle your personal data, please contact our Grievance Officer first.

Contact	Detail
Grievance Officer	[John Thomas, Designation: MD & CEO]
Email	johnthomas@johnthomasfintech.com [or customersupport@johnthomasfintech.com]
Phone	+91 8210700278

Contact	Detail
Postal address	69/1854 A, A1, A2, SRM Rd, Ernakulam North, Ernakulam, Kerala – 682018, India
Acknowledgement	Within [48 hours] of receipt
Resolution	Within [30] days, and in any case within the period prescribed by the DPDP Rules

If you are not satisfied with our response, or do not receive one in time, you may complain to the Data Protection Board of India. The Board expects you to have used our grievance process first. If your data sits in a Customer's account, please also contact that Customer, which is the Data Fiduciary for it. If you are a customer of a Regulated Entity, you can also use the grievance channels of that entity and its regulator.

23. Governing Law and Jurisdiction

This Policy is governed by the laws of India. Subject to the DPDP Act and any other law that gives you a right to approach a particular forum, disputes are subject to the exclusive jurisdiction of the courts at Ernakulam, Kerala. For Customer Data, the data processing terms of the customer agreement prevail if they conflict with this Policy. If this Policy is translated, the English version prevails unless the law says otherwise.

24. Contact Us

For questions about this Policy or our data practices, write to johnthomas@johnthomasfintech.com [\[customersupport@johnthomasfintech.com\]](mailto:customersupport@johnthomasfintech.com), call +91 8210700278, or write to John Thomas Fintech Private Limited, 69/1854 A, A1, A2, SRM Rd, Ernakulam North, Ernakulam, Kerala – 682018, India.

Annex A: Sub-processor Register

Complete and keep this list current. Publish it, or make it available to Customers on request.

Sub-processor	Service	Data involved	Location
[AWS]	Application hosting, database, backup	All Customer Data and account data	[India, Mumbai region]
[Cashfree]	Subscription billing	Billing contact and payment data	[India]
[Email -Go Daddy and messaging provider Jio]	Transactional email, SMS	Name, email, phone	[India]
[Goggle Gemini]	AI features	Content you submit to AI features	[Google India]
[John Thomas Fintech Private limited]	Customer support	Contact details, ticket content	[India]
[Analytics tool-John Thomas Fintech Private limited]	Usage analytics	Usage and device data	[India]

Annex B: Pre-publication Checklist (delete before publishing)

#	Action	Why it matters
1	Name a Grievance Officer, a data protection contact and an Information Security Officer, and put their details in Sections 3 and 22.	The IT Rules and DPDP Act expect a named, reachable person.
2	Choose Option A or B in Section 11.1. Do not claim ISO/IEC 27001 certification unless a certificate exists.	Certification needs an audit by an accredited certification body. A false claim is a misrepresentation.
3	Confirm hosting provider and regions, and complete Annex A. Confirm no restricted-country list has been notified.	Sections 9 and 8 make factual claims.
4	Check that each security control in Section 11 is in place: MFA, encryption, logging for one year in India, NTP sync, backups kept in India, PEN test, DR test.	DPDP penalties for failing to keep reasonable security safeguards can reach ₹250 crore; for failing to notify a breach, ₹200 crore.
5	Check that the accounting product has a non-disableable audit trail with 8-year retention.	Companies (Accounts) Rules, 2014, Rule 3.
6	Confirm the AI statements in Section 7 match your architecture and provider contracts.	The statements bind you once published.

#	Action	Why it matters
7	Fill in the bracketed retention periods, response times and incident-notification targets.	They must be periods you can actually meet.
8	Prepare a customer data processing agreement and, for NBFC and bank customers, an outsourcing addendum covering audit access, incident timing, sub-contracting and exit.	RBI-regulated customers must contract for these.
9	Decide the cookie tools and build a banner with separate choices and no dark patterns.	Section 17.
10	Plan for Consent Manager integration by 13 November 2026 and full DPDP compliance by 13 May 2027. Check for any change to these dates.	Section 1.2 states the current dates.
11	If the group will ever hold a payment, lending, insurance or investment licence, the licensed entity needs its own privacy notice and regulatory compliance. This Policy does not cover it.	Your MOA currently scopes the Company to software and technology.
12	Have a lawyer review the whole document, and revisit it every six months and on any change in law.	This draft is not legal advice.