

LEGATIO

A Platform of Trayambic LLP • LLPIN: ACW-5820

PRIVACY POLICY

Version 1.1 • Effective Date: 15 July 2026 *Draft. Sign. Secure.* • From Intent to Ironclad.

Preamble

At Legatio, the protection of your personal information is foundational to the trust that underpins our document infrastructure. This Privacy Policy (“Policy” or “Notice”) describes how Trayambic LLP, a Limited Liability Partnership incorporated under the Limited Liability Partnership Act, 2008, bearing LLPIN ACW-5820, with its registered office at Unit 162, J2 Shramaseva Co-Op Society, Wadala Truck Terminal Road, Wadala RTO, Wadala, Mumbai – 400037, Maharashtra, India, doing business under the trade name “Legatio” (collectively “Legatio,” “Trayambic,” “we,” “us,” or “our”), collects, uses, stores, discloses, retains, transfers, and otherwise processes the Personal Data of natural persons and authorised representatives of juridical entities (“you,” “your,” or “User”) who access, browse, register on, or use the Legatio platform available at www.legatio.co and all associated sub-domains, mobile applications, application programming interfaces, and any related services (collectively, the “Platform” or the “Services”).

This Notice is published in accordance with the following legislation and regulatory directions in force in the Republic of India:

- The Digital Personal Data Protection Act, 2023 (“DPDP Act”) and the rules issued thereunder, including those provisions brought into force by way of notification as of the effective date of this Policy;
- The Information Technology Act, 2000 (“IT Act”), and in particular Sections 43A and 79 thereof;
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“SPDI Rules”);
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“IT Intermediary Rules”);
- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (“Aadhaar Act”) and regulations issued by the Unique Identification Authority of India (“UIDAI”); and

- The CERT-In Directions dated 28 April 2022 on mandatory cyber-incident reporting.

This Policy forms an integral and binding part of the Legatio Terms and Conditions v3.0 (“Terms”). Capitalised terms used but not defined herein shall have the meanings ascribed to them in the Terms. By accessing or using the Platform, you confirm that you have read, understood, and agreed to this Policy in its entirety.

Clause 1 — Scope and Applicability

1.1 To Whom This Notice Applies

This Policy applies to all Users of the Platform, including:

- Part A Users / Clients — business owners, document originators, employers, or issuing parties;
- Part B Users / Counterparties — signatories, employees, vendors, or receiving parties who are invited to execute a Document dispatched by a Client;
- Authorised Signatories acting on behalf of a Client or Part A User; and
- Visitors to the informational website at legatio.co who do not create an Account.

1.2 What This Notice Does Not Cover

This Policy does not apply to:

- Third-party websites, applications, or services linked from the Platform, including those operated by Digio, Amazon Web Services, Jio TrueConnect, payment gateway operators, or any other Vendor;
- The internal processing activities of Clients in their capacity as independent Data Fiduciaries with respect to their own Counterparties — Clients are solely responsible for issuing their own privacy notices to their data principals; or
- Information you share publicly on external forums, social media, or other channels not operated by Legatio. You are strongly advised to review the privacy policies of any third-party services before interacting with them.

1.3 Dual Roles Under the DPDP Act

Trayambic operates under a dual-role architecture that determines how we interact with Personal Data:

- **Data Fiduciary:** For Personal Data we collect directly in connection with your Account, billing, authentication, and Platform usage, Trayambic acts as a Data Fiduciary and determines the purpose and means of processing.
 - **Data Processor:** For Personal Data contained within Documents uploaded, drafted, executed, or stored by a Part A User on the Platform — including Personal Data of Counterparties, employees, customers, or other third parties — Trayambic acts as a Data Processor, processing such data solely on the documented instructions of the Part A User, who is the Data Fiduciary in respect of such data.
 - **Sub-Processors:** Digio, AWS (Mumbai region), Jio TrueConnect, AWS Simple Email Service, and PCI-DSS compliant payment gateway operators operate as Data Processors or sub-processors under this framework, engaged by Trayambic to provide specific infrastructure or verification functions.
-

Clause 2 — Categories of Personal Data We Collect

We collect only such Personal Data as is strictly necessary to provide the Services, comply with Applicable Law, and operate the Platform securely.

2.1 Registration and Identity Data

Full name, registered Indian mobile number, email address, business name, GSTIN (where you register as a juridical entity), designation, and Authorised Signatory details provided during Account creation or onboarding.

2.2 Government-Issued Identification

Aadhaar number, PAN, and/or Driving Licence, submitted solely for identity verification and eKYC. These documents are transmitted directly to Digio's verification API and are not stored in raw form on Legatio's systems. Legatio retains only resulting verification metadata — confirmation status flags, transaction reference numbers, and cryptographic hashes — within the secure Audit Trail.

2.3 Authentication Data

OTP issuance, delivery, and verification logs; eSignature authentication events; biometric authentication factors used by Digio for Aadhaar-based eSign (processed by UIDAI and Digio, never accessible to Legatio); DSC-related metadata; and device authentication timestamps.

2.4 Technical and Device Data

IP address, device fingerprint, browser type and version, operating system, approximate geo-location metadata (IP-derived), session identifiers, referral URLs, and timestamps, captured as part of the immutable Audit Trail maintained on each Document.

2.5 Document Content

The content of Documents drafted, uploaded, executed, or stored by Part A Users on the Platform. Such Documents may contain Personal Data of Counterparties, employees, customers, or other third parties. Legatio operates a zero-knowledge architecture in respect of Document content stored within the Encrypted Vault — no employee or human operator of Legatio can view, open, or read the text of any Document stored therein.

2.6 Payment Metadata

Transaction reference numbers, payment gateway confirmation codes, invoice records, GST details, and refund records. Full payment card data is not stored on Legatio's servers; all card data is processed exclusively by PCI-DSS compliant payment gateway operators.

2.7 Communication Preferences and Consent Records

WhatsApp opt-in or opt-out status, email communication preferences, marketing consent records, timestamps of consent or withdrawal, and grievance correspondence.

2.8 Usage and Session Logs

Platform interaction logs, feature usage data, click-stream events on authenticated dashboard sessions, and session duration records — used solely for security, fraud prevention, service improvement, and statutory audit compliance purposes.

2.9 Cookies

2.9.1 Categories of Cookies

The Platform uses two categories of cookies:

- **(a) Strictly Necessary Cookies** — Session cookies that maintain secure login states and dashboard preferences across authenticated sessions. These are essential to the operation of the Platform and cannot be disabled. They do not track you across third-party websites and are deleted automatically when your browser session ends.
- **(b) Analytics Cookies (optional — requires your consent)** — Performance and analytics cookies that help us understand how authenticated Users interact with dashboard features.

This data is used solely to improve the Platform and is not linked to your identity or shared externally. These cookies are activated only upon your express consent.

2.9.2 Cookie Consent

When you first visit the informational website at legatio.co, a cookie preference banner is displayed. You may choose to: (i) accept all cookies and tracking tools; (ii) permit only strictly necessary session cookies; or (iii) individually enable or disable analytics and marketing cookies. Your preference is stored locally on your device. You may withdraw or update your consent at any time via the preference link in the website footer or by clearing local storage for legatio.co.

2.9.3 No Tracking Inside the Platform

No cookies, pixels, or tracking scripts are active within the authenticated Encrypted Vault environment or within any Document execution session. Tracking tools described in this Clause 2.9 and Clause 2.10 operate exclusively on the publicly accessible informational website (legatio.co).

2.10 Meta Pixel and Marketing Tracking

What Is the Meta Pixel? The Meta Pixel (also known as the Facebook Pixel) is a JavaScript-based analytics tool operated by Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland (“Meta”). It is deployed on the informational website at legatio.co only — never within the authenticated Platform environment.

2.10.1 What the Pixel Does

When enabled, the Meta Pixel sends anonymised behavioural signals — including page views, button click events, and time-on-page data — from your browser to Meta’s servers. Meta uses these signals to: (i) measure the reach and effectiveness of Legatio’s advertisements displayed on Facebook and Instagram; and (ii) enable Meta to show Legatio advertisements to users who have previously visited the website (retargeting).

2.10.2 What We Do Not Share via the Pixel

The Meta Pixel is configured in standard mode. We do not transmit to Meta any of the following:

- Aadhaar numbers, PAN, or any government-issued identification;
- Document content or metadata;
- Account login credentials, OTPs, or authentication data;

- Payment card data or transaction reference numbers; or
- Any data collected inside the authenticated Platform environment.

2.10.3 Data Transmitted to Meta

Data Point	Purpose
Browser IP address (hashed)	Geographic reach measurement
Browser user-agent string	Device and platform analytics
Page URL visited	Event mapping
Pixel event type (e.g. PageView)	Conversion measurement
Facebook Click ID (fbclid), if present	Ad attribution
Facebook Browser ID (fbid) cookie	Session deduplication

2.10.4 Legal Basis

We rely on your consent as the lawful basis for activating the Meta Pixel, pursuant to the DPDP Act and applicable guidance. The Pixel is not loaded until you have expressly accepted marketing cookies via the cookie preference banner described in Clause 2.9.2.

2.10.5 Data Localisation Note

Meta Pixel data is transmitted to and processed on Meta's servers, which are located outside India. By consenting to marketing cookies, you acknowledge that this specific data transfer occurs and is governed by Meta's terms and applicable cross-border data transfer mechanisms. No other Personal Data processed by Trayambic is transferred outside India (see Clause 5.4).

2.10.6 How to Opt Out

You may withdraw consent for the Meta Pixel at any time by:

- Updating your cookie preferences via the preference centre on legatio.co;
- Using Meta's Ad Preferences tool at www.facebook.com/adpreferences;
- Enabling "Limit Ad Tracking" or equivalent settings on your device; or
- Installing a browser-based ad blocker or script blocker.

Withdrawing consent will stop all future Pixel signals from your browser. It will not affect data already transmitted to Meta prior to withdrawal.

Clause 3 — Purposes and Legal Bases for Processing

Purpose	Categories of Data	Legal Basis
Account creation and authentication	Registration, Identity, Authentication	Contract performance; Legal obligation
eKYC and identity verification	Government IDs (routed to Digio)	Legal obligation (Aadhaar Act, IT Act); Contract performance
Document drafting, execution, and storage	Document Content, Audit Trail	Contract performance; Legal obligation
Payment processing and invoicing	Payment Metadata	Contract performance; Legal obligation (GST)
Security, fraud prevention, and audit	Technical, Authentication, Usage Logs	Legal obligation; Legitimate interest
Service improvement	Usage and Session Logs (anonymised)	Legitimate interest
Marketing communications	Contact details (opted-in Users)	Consent
Meta Pixel (website analytics)	Browser signals (anonymised)	Consent
Compliance with legal obligations	All categories as required	Legal obligation
Grievance redressal	Identity, Communications	Legal obligation (IT Intermediary Rules)

Clause 4 — How We Use Your Personal Data

4.1 Platform Operation

We use your Personal Data to create and manage your Account; authenticate your identity; facilitate the drafting, execution, and storage of Documents; generate and maintain the immutable Audit Trail; and deliver OTP codes, execution links, and system notifications.

4.2 Legal and Regulatory Compliance

We process Personal Data to comply with applicable statutory obligations, including eKYC requirements under the Aadhaar Act, CERT-In cybersecurity reporting obligations, DPDP Act compliance, GST invoicing requirements, and any order of a competent court or regulatory authority.

4.3 Security and Fraud Prevention

Technical and device data, session logs, and authentication records are used to detect, investigate, and prevent unauthorised access, fraudulent activity, platform abuse, and security incidents.

4.4 Service Improvement

Anonymised usage data and session logs are used to understand how the Platform is used, identify friction points, and improve the quality and reliability of our Services. This data is not linked to any individual User.

4.5 Communications

We use your registered contact details to send you: (i) transactional notifications (OTPs, execution alerts, document copies, invoices); (ii) system notices (policy updates, scheduled maintenance); and (iii) marketing communications, solely where you have provided explicit opt-in consent. You may opt out of marketing communications at any time via the unsubscribe mechanism in any such communication or by contacting the Grievance Officer.

4.6 What We Do Not Do With Your Data

Trayambic shall not:

- Use Document content, User Content, or Personal Data for the training, fine-tuning, or benchmarking of any artificial intelligence, machine learning, or large language model;
- Sell, rent, or commercially transfer your Personal Data to any third party;

- Use your Personal Data for any purpose unrelated to the provision of the Services without your express prior written consent; or
 - Disclose your Personal Data to any government authority except as required by Applicable Law or by order of a competent court.
-

Clause 5 — Disclosure and Third-Party Sharing

5.1 Authorised Sub-Processors

Trayambic shares Personal Data with the following authorised sub-processors solely to the extent necessary to deliver the Services:

Sub-Processor	Function	Data Shared	Location
Digio	Aadhaar eSign, eKYC, DSC-based eSign	Government IDs (image, not stored by Legatio); authentication metadata	India
Amazon Web Services (AWS) — Mumbai Region	Platform infrastructure and Encrypted Vault hosting	All Platform data (encrypted at rest)	India (Mumbai)
Jio TrueConnect	SMS and OTP gateway	Mobile number; OTP content	India
AWS Simple Email Service	Transactional email delivery	Email address; notification content	India
PCI-DSS Payment Gateway Operators	Payment processing	Payment transaction data (no card data stored by Legatio)	India

All sub-processors are contractually bound to process Personal Data only on Trayambic’s documented instructions and in accordance with security standards equivalent to or exceeding those in this Policy.

5.2 Legal Disclosures

We may disclose Personal Data where required by: (i) an order of a competent court, tribunal, or regulatory authority; (ii) the CERT-In Directions (cyber-incident reporting); (iii) a request from a

law enforcement authority with lawful authority to compel disclosure; or (iv) any other Applicable Law. We will, where legally permissible, notify you of such a disclosure.

5.3 Business Transfers

In the event of a merger, acquisition, restructuring, or sale of assets involving Trayambic, Personal Data may be transferred to the successor entity, provided that the successor entity is bound by data protection obligations at least as protective as those in this Policy. Trayambic shall provide Users with prior notice of any such transfer.

5.4 Data Localisation — Cross-Border Transfer Exception

All Personal Data processed by Trayambic is stored exclusively on AWS Mumbai region servers within India. The sole exception is Meta Pixel data, which is transmitted to Meta's servers outside India upon your consent for marketing cookies (see Clause 2.10). No other Personal Data is transferred, processed, or stored outside the territorial borders of the Republic of India.

Clause 6 — Data Retention

6.1 Retention Periods

Data Category	Retention Period	Basis
Executed Documents and Audit Trails	8 years from date of execution, then permanent purge	T&C Clause 4.6.1; statutory record-keeping norms
Account and registration data	Duration of active Account + 90 days post-termination	Contract performance
Authentication and OTP logs	8 years (as part of Audit Trail)	Legal obligation; fraud prevention
Government ID verification metadata	8 years (as part of Audit Trail); raw IDs not stored	Legal obligation (UIDAI norms)
Payment metadata and invoices	8 years from transaction date	GST Act; Income Tax Act record-keeping
Usage and session logs	2 years	Security; service improvement
Marketing consent records	Until consent withdrawn + 3 years	DPDP Act compliance; evidence of consent
Grievance correspondence	3 years from resolution	IT Intermediary Rules

6.2 Post-Termination

Upon termination of your Account, Trayambic shall deliver a final copy of all your Executed Documents to each signatory party on record. Following delivery, all such Documents shall be permanently deleted from active storage within seven (7) days. The 8-year retention obligation applies to Documents executed prior to termination and retained in accordance with Clause 6.1.

6.3 Deletion on Purge

At the expiry of the applicable retention period, all Document files, metadata records, authentication logs, and transaction data shall be permanently deleted from active storage

arrays and secure backup mirrors. There is no commercial option to extend storage beyond the 8-year limit for Executed Documents.

Clause 7 — Data Principal Rights

Every verified Data Principal on the Platform retains the following rights under the DPDP Act, 2023, exercisable by a written request to the Data Protection Officer at the contact details set out in Clause 10:

Right	What It Means	Limitations
Right to Summary	Receive a plain-language summary of what Personal Data we hold about you and how it is being processed.	None — available to all verified Data Principals.
Right to Correction	Correct, complete, or update inaccurate or outdated Personal Data.	Identity verification required before changes are made.
Right to Erasure	Request deletion of your Personal Data.	Cannot apply to data subject to the 8-year retention obligation (Executed Documents and Audit Trails), data required for active legal proceedings, or data required by Applicable Law.
Right to Grievance Redressal	Register a formal complaint regarding any perceived data handling issue with the Grievance Officer.	Response within 48 hours of acknowledgment; resolution within 30 days.
Right to Withdraw Consent	Withdraw consent for marketing communications or Meta Pixel tracking at any time.	Withdrawal applies prospectively; does not affect prior processing.
Right of Nomination	Nominate an individual to exercise your rights in the event of your death or incapacity (as and when operative under the DPDP Act).	Operative upon relevant DPDP Act provisions being notified.

To exercise any of the above rights, please submit a written request to the Data Protection Officer at the contact details in Clause 10. We will acknowledge your request within 48 hours and endeavour to resolve it within thirty (30) days.

Clause 8 — Information Security

8.1 Security Framework

Trayambic maintains a comprehensive information security framework encompassing the following controls:

Control	Details
Encryption at Rest	AES-256 encryption applied to all Documents and metadata stored in the Encrypted Vault.
Encryption in Transit	TLS 1.3 or higher across all network layers and API communications.
Zero-Knowledge Architecture	No Legatio employee, engineer, or human operator can view or access the contents of Documents stored in the Encrypted Vault.
Immutable Audit Logging	Write-once-read-many (WORM) audit logs capture timestamps, IP addresses, user sessions, and cryptographic events.
Aadhaar Data Handling	Raw Aadhaar numbers, PAN digits, and Driving Licence images are routed directly to Digio's API. No raw identification data is stored on Legatio's systems. Only verification metadata (flags, reference numbers, hashes) is retained.
Vulnerability Management	Regular automated vulnerability assessments and penetration testing to identify and remediate weaknesses.
Network Isolation	Fine-grained access controls and network segmentation separating application layers from active data processing environments.
Access Control	Role-based access controls limiting internal access to Personal Data on a strict need-to-know basis.

8.2 Data Breach Response

In the event of a personal data breach involving Personal Data for which Trayambic is the Data Fiduciary, Trayambic shall:

- Isolate affected server clusters within two (2) hours of discovery;
- Report the incident to CERT-In within six (6) hours of becoming aware of the incident, in accordance with the CERT-In Directions dated 28 April 2022;

- Notify the Data Protection Board of India and affected Data Principals in the manner and within the timelines prescribed under the DPDP Act, as applicable; and
- Maintain a record of the breach, its impact, and remediation steps taken.

Where a breach involves Personal Data for which the User (as Part A User) is the Data Fiduciary, Trayambic shall notify the User without undue delay, and the User shall be solely responsible for all obligations of notification and remediation in respect of such data.

8.3 Limitations

Despite the security measures described above, no system can guarantee absolute security. Trayambic cannot guarantee that Personal Data will never be subject to a breach. Users are strongly advised to: (i) maintain strong, unique passwords; (ii) never share OTPs with any person; and (iii) notify Trayambic immediately upon becoming aware of any suspected unauthorised access to their Account.

Clause 9 — Children’s Privacy

The Platform is not directed at, and does not knowingly collect Personal Data from, individuals under the age of eighteen (18) years. If you become aware that a minor has provided Personal Data to Legatio without parental consent, please notify the Grievance Officer immediately. Upon verification, Trayambic shall take prompt steps to delete such data.

Clause 10 — Grievance Officer and Data Protection Officer

In accordance with Rule 4 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the DPDP Act, Trayambic has designated the following as its Grievance Officer and Data Protection Officer:

Grievance Officer / Data Protection Officer — Contact Details Name: [To be inserted before go-live] **Designation:** [To be inserted before go-live] **Email Address:** grievance@legatio.co [confirm before go-live] **Response Timeline:** Acknowledgment within 48 hours; resolution within 30 days of receipt.

If you are dissatisfied with the resolution provided by the Grievance Officer, you may escalate the matter to the Data Protection Board of India (for DPDP Act-related complaints) or approach the appropriate judicial forum in Mumbai, Maharashtra.

Clause 11 — Changes to This Policy

Trayambic reserves the right to update or modify this Policy at any time to reflect changes in Applicable Law, regulatory guidance, or our data processing practices. Where any modification is material, we will:

- Publish the revised Policy on the Platform with a revised version number and effective date; and
- Provide not less than fifteen (15) days' prior notice to registered Users by email or WhatsApp notification to the registered contact details on record.

Continued use of the Platform after the effective date of the revised Policy constitutes your acceptance of the modifications. If you do not accept any modification, your sole remedy is to discontinue use of the Platform and request Account termination in accordance with the Terms.

The version history of this Policy is maintained below:

Version	Effective Date	Key Changes
1.0	15 July 2026	Initial publication.
1.1	15 July 2026	Added Clause 2.9.2 (Cookie Consent mechanism); inserted Clause 2.10 (Meta Pixel disclosure); added cross-border transfer exception in Clause 5.4; expanded data principal rights table in Clause 7; updated version history table.

Clause 12 — Governing Law and Dispute Resolution

This Policy shall be governed by and construed in accordance with the laws of India. Any dispute arising out of or in connection with this Policy shall be resolved in accordance with the dispute resolution mechanism set out in the Terms and Conditions v3.0. The courts of Mumbai, Maharashtra shall have exclusive territorial jurisdiction over all matters not subject to arbitration.

Clause 13 — Contact Us

For any questions, concerns, or requests relating to this Privacy Policy or the processing of your Personal Data, please contact:

Contact Legatio Platform: www.legatio.co **Registered Office:** Unit 162, J2 Shramaseva Co-Op Society, Wadala Truck Terminal Road, Wadala RTO, Wadala, Mumbai – 400037, Maharashtra, India **Email:** grievance@legatio.co [confirm before go-live]

Legatio • A Platform of Trayambic LLP • LLPIN: ACW-5820 *Draft. Sign. Secure. • From Intent to Ironclad.*

LEGATIO • A Platform of Trayambic LLP • LLPIN: ACW-5820 *Privacy Policy v1.1 • Effective 15 July 2026 • www.legatio.co*