

LEGATIO SERVICE CONTINUITY POLICY

How We Keep Legatio Running Reliably for You

Trayambic LLP | LLPIN: ACW-5820

Effective: From Commercial Launch Date

Contact: BUSINESS@LEGATIOINFO.COM

1. Why This Policy Matters

Legatio handles your most important documents—contracts, agreements, and records that shape your business. We take that responsibility seriously. This Service Continuity Policy explains how we keep the platform running reliably, protect your data from loss or breach, and ensure you can always access what you've signed and stored.

2. Data Location & Encryption

All your documents are stored in AWS servers located in the Mumbai region, India. They are encrypted using AES-256 encryption while stored and while being transmitted to you. We use TLS 1.3 (the latest security standard) to protect data in transit. Only you—using your account credentials—can decrypt and view your documents. Legatio employees and infrastructure do not have keys to access your content.

IMPORTANT: Your documents are encrypted. During specific service operations (Aadhaar eSign via Digio, DSC signing via eMudhra, and storage on AWS), third-party service providers may access your documents in encrypted form for their stated purposes only. See Section 13 for details.

3. Backup & Redundancy

Your documents are not stored in a single location. We maintain redundant backup copies on separate, geographically distinct infrastructure within India. If one system fails, your data is automatically accessible from the backup. This redundancy is continuously monitored and tested.

4. The 8-Year Retention Guarantee

Every document you execute on Legatio is automatically kept in the Vault for 8 years from the date you signed it, at no additional charge. You do not need to ask us to keep it—it is automatic. After 8 years, the document is permanently deleted from our systems (unless you request deletion sooner). This retention applies to executed documents, not drafts.

5. Access Control & Document Privacy

Legatio uses encryption such that your document content is not accessible to Legatio employees, administrators, or support staff once stored. Only you, and the parties you have shared documents with, can access them. Even if someone gains unauthorized access to our servers, they would receive encrypted data, not readable documents.

6. Audit Trail & Proof of Signing

Every action on every document is recorded in a cryptographically signed audit trail that cannot be modified after the fact. This includes:

- Who accessed the document and when
- What IP address and device was used
- When OTP codes were sent and verified
- The exact timestamp of signature (with cryptographic proof)

This Audit Trail stays with your document for 8 years and helps prove that it was genuinely signed and has not been tampered with.

IMPORTANT LEGAL DISCLAIMER: Legatio's audit trail meets the technical requirements of Section 65A(B) of the Indian Evidence Act, 2012. However, admissibility in any legal proceeding depends on proper execution by your authorized signatories, proper authentication by the document controller, witness testimony, and judicial discretion. Legatio provides the technical infrastructure; you ensure compliance with evidentiary standards.

7. Aadhaar & eKYC Security

When you or a counterparty sign a document using Aadhaar-based eSignature, Legatio connects to UIDAI's secure servers through a licensed partner (Digio). Legatio does not store your full Aadhaar number—only a masked version and confirmation that eKYC verification succeeded. All Aadhaar data is handled according to the Aadhaar Act, 2016 and UIDAI regulations.

eKYC data and masked Aadhaar are retained only for the duration of the signing process (typically 24-72 hours) and then permanently deleted. Personal data embedded in your documents is retained per the 8-year storage guarantee, then deleted.

8. Security & Compliance Reviews

Legatio operates under the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; CERT-In Directions, 2022; and relevant industry standards. We conduct internal security audits and review encryption standards, backup systems, and access controls regularly to stay current with threats and regulations. Any material changes to our security measures will be communicated to you in advance.

9. Data Deletion (You're in Control)

At any time, you can request deletion of a specific document or your entire account. When you do, we securely and permanently delete the document and associated metadata from our systems and backups within 7 days. This deletion is permanent—we cannot recover the data even if you request recovery later.

10. Aadhaar Act Compliance & Data Minimization

We only store Aadhaar-linked data (eKYC records, masked Aadhaar) for as long as it is needed to prove you signed a document. Once the signature is complete, eKYC data is not retained longer than required by law. Personal data in your documents is stored only for the purpose of providing the Service, and will be deleted when you delete your account or your documents, or 8 years after execution, whichever is earlier.

11. System Uptime & Availability

Legatio is built on AWS infrastructure with multiple layers of redundancy. We aim to keep the platform available and operational, but do not provide a specific uptime service-level agreement (SLA) at this time. Planned maintenance will be communicated at least 7 days in advance and typically takes less than 1 hour.

During system downtime or outages, you can still view and download your signed documents (they are encrypted and backed up independently). However, you may not be able to execute new transactions, send new documents, or add counterparties until service is restored.

12. What Happens If There's a Data Breach

If we detect a confirmed security breach affecting your data, we will:

- Investigate immediately and contain the breach
- Notify you within 72 hours (as required by the DPDP Act, 2023)
- Tell you exactly what data was affected and what we are doing about it
- Provide contact information for questions

Because your documents are encrypted, a breach of our servers does not automatically expose your actual document content. However, we treat any breach with the utmost seriousness. A detailed root-cause analysis will be shared within 30 days, and findings will be available to relevant regulators.

13. Third-Party Service Providers

Legatio uses trusted partners to deliver parts of the Service:

- AWS (storage, infrastructure, backup)
- Digio (Aadhaar eSign, eKYC verification, DSC signing support)
- eMudhra (DSC certificate verification, UIDAI licensing)

- AWS SES or equivalent (transactional email and SMS)

All service providers are bound by Data Processing Agreements compliant with the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and CERT-In requirements. We do not share your documents with any other third party except as required by law or with your explicit consent.

You may request a copy of any data processing agreement by contacting BUSINESS@LEGATIOINFO.COM.

14. Changes to This Policy

We may update this policy to reflect changes in technology, law, or our security practices. If we make changes that reduce your protections, we will provide 30 days' notice before they take effect. Material changes will be communicated via email and the Legatio dashboard.

15. What This Policy Does NOT Promise

This policy is about how we keep your data safe and accessible. It does not:

- Promise that the platform will never have any downtime or technical issues
- Obligate us to provide legal advice or legal compliance guidance
- Replace your own backup and business continuity planning

16. CERT-In and Regulatory Compliance

Legatio complies with CERT-In Incident Response Directions, 2022. Incidents involving unauthorized access, data loss, or system compromise are reported to CERT-In within the timeframes specified by CERT-In, and to customers per DPDP Act timelines. All incidents are investigated and documented. You may request incident reports relevant to your account by contacting BUSINESS@LEGATIOINFO.COM.

17. Data Localization

Legatio certifies that all customer data is processed, stored, and backed up within India, in compliance with the Digital Personal Data Protection Act, 2023, and any applicable RBI or sectoral data localization requirements. Cross-border transfers of your data are not permitted without your explicit written consent.

18. Questions or Concerns

If you have questions about how we protect your data, or concerns about a security issue, contact us at BUSINESS@LEGATIOINFO.COM or use the Grievance Officer contact published on the Platform. We will respond within 48 business hours. Any disputes will be resolved through binding arbitration in Mumbai under the Arbitration and Conciliation Act, 1996, and the laws of India.

POLICY SUMMARY: KEY TIMELINES & COMMITMENTS

Event / Requirement	Timeline
Shutdown Notice to Customers	120 calendar days (minimum)
Download Window for Export Package	Full 120-day notice period
Data Deletion by Legatio (post-download)	Within 30 days
User-Requested Document Deletion	Within 7 days
Data Breach Notification to Affected Users	Within 72 hours (DPDP Act requirement)
Breach Root-Cause Analysis	Within 30 days
Regular Document Retention (automatic)	8 years from execution date
Support Response Time	Within 48 business hours