Ciforus Privacy Policy

Privacy-first data handling, transparency, and encryption boundary policy

Brand	Ciforus
Series	Legal and trust documentation
Prepared	April 2026
Status	Launch-ready draft

This document reflects the current Ciforus product, token, privacy, and launch narrative and should be reviewed before user interaction.

Effective Date: April 4, 2026

Document Status: Policy for launch preparation and legal authorities

Applies To: ciforus.com, related launch pages, wait-list forms, future app services, and token-related onboarding flows operated under the Ciforus brand

Important Notice

This Privacy Policy explains how Ciforus handles personal information and service data in connection with the Ciforus website, launch materials, wait-list features, future application services, and token-related onboarding flows.

Ciforus is built around a privacy-first product philosophy. That means data minimization, strong encryption, reduced unnecessary exposure, and deliberate limits on provider-side readability are part of the service design. This document is written to reflect that product direction clearly while staying realistic about the information Ciforus does collect, store, and process.

1. Who We Are

For this policy, **Ciforus**, **we**, **us**, and **our** mean the entity or entities operating the Ciforus website, application services, launch communications, and related compliance or support processes under the Ciforus brand.

Ciforus is a privacy-first digital platform designed for secure communication, encrypted storage, wallet-aware identity, account protection, crypto-native billing, and the CIFORUS token ecosystem.

2. Scope of This Policy

This Privacy Policy applies to:

- visitors to the Ciforus website and token pages
- users who submit a wait-list or launch form
- people who contact Ciforus for support, legal, business, or partnership matters
- future users of Ciforus application services when those services become available
- users who participate in token onboarding, compliance, or related payment-review processes

This policy does not automatically apply to third-party services, wallets, exchanges, block explorers, payment infrastructure providers, or websites that are not operated by Ciforus, even if they are linked from the Ciforus site.

3. Information We May Collect

3.1 Information You Give Us Directly

Depending on how you interact with Ciforus, we may collect:

- name or display name
- email address
- wait-list submission details
- optional presale interest information, including a rough indicated USD amount if you choose to provide one
- support, legal, partnership, or business communications
- account registration information for future app services
- wallet addresses or wallet-verification information where relevant to the service
- compliance or due-diligence information if token participation or higher-risk financial activity requires it

3.2 Information Collected Automatically

When you use the website or future app services, we may automatically receive or generate:

- IP address
- browser type and device information
- approximate location derived from network information
- page requests, referral paths, timestamps, and server logs
- security and abuse-prevention logs
- session-level technical diagnostics

Ciforus aims to keep this category limited to what is reasonably necessary for delivery, stability, and security.

3.3 Application and Platform Data

If you later use Ciforus application services, we may process data related to:

- account creation and authentication
- service entitlements, plan status, and wallet-verification status
- payment status and transaction references
- recovery and security settings
- storage, messaging, note, and communication events needed to operate the service
- encrypted service content and protected metadata, depending on the module used

4. How We Use Information

Ciforus may use information for the following purposes:

- providing, operating, securing, and improving the website and future services
- responding to support, legal, business, and compliance requests
- managing the wait-list and launch communications
- sending launch notices, policy updates, and service-related messages
- performing fraud prevention, abuse prevention, and security monitoring
- conducting wallet review, onboarding checks, or compliance screening where needed
- meeting accounting, tax, legal, or regulatory obligations
- protecting the rights, safety, and integrity of Ciforus, its users, and its infrastructure

Ciforus does not position itself as an advertising data business and does not sell personal information.

5. Legal Bases and Processing Principles

Where data-protection laws require a lawful basis, Ciforus may process personal data on one or more of the following grounds:

- performance of a contract or steps requested before entering a contract
- legitimate interests in operating, securing, and improving the service
- legal or regulatory compliance obligations
- consent, where consent is the appropriate basis

Ciforus follows privacy principles centered on:

- transparency
- purpose limitation
- data minimization
- storage limitation
- integrity and confidentiality
- practical respect for user control

6. Privacy-First Architecture and Encryption Boundaries

Ciforus is designed around stronger privacy boundaries than conventional convenience-first platforms. The product narrative and technical direction emphasize:

- layered encryption architecture

- user-scoped keys
- reduced broad server-side readability
- limits on unnecessary indexing of private content
- minimized exposure of sensitive content and metadata where technically feasible

6.1 What This Means in Practice

Ciforus does not sell personal information. For content that is encrypted with user-bound or user-scoped cryptographic controls and not available to Ciforus in plaintext, Ciforus is not technically able to decrypt and disclose the plaintext content it does not possess.

This technical limitation does not change based on the identity of the requesting party. If Ciforus does not hold the usable decryption keys or plaintext, it cannot hand over plaintext content simply because a third party asks for it.

6.2 Important Limitation

This does **not** mean Ciforus never has any information. Ciforus may still hold and may need to disclose, where legally required, data it actually controls or receives in readable form, such as:

- account contact details
- wait-list records
- payment or transaction records
- security and access logs
- support requests
- compliance documents
- corporate records or internal business records

The privacy model is strong, but it is not magical. It depends on what Ciforus actually stores, what is encrypted, and what information is or is not readable by design.

7. Cookies, Similar Technologies, and Site Operations

Ciforus may use strictly necessary technical mechanisms to operate the website and protect sessions or forms. If Ciforus later introduces analytics, marketing cookies, or similar technologies beyond what is strictly necessary, Ciforus will update its notices and controls accordingly.

8. Sharing and Disclosure

Ciforus may share information only where necessary and appropriate with:

- hosting or infrastructure providers

- security, compliance, fraud-prevention, or monitoring vendors
- professional advisers such as legal, audit, and accounting providers
- payment, blockchain, or wallet-related service providers where required to complete or verify a transaction or entitlement
- authorities, courts, regulators, or law-enforcement bodies where disclosure is legally required or reasonably necessary to protect rights and safety
- a buyer, investor, or successor entity in the event of a corporate transaction, subject to appropriate confidentiality and data-handling controls

Ciforus does not sell personal information or user data as a commercial advertising asset.

9. International Transfers

Because online services may involve infrastructure or professional service providers in different jurisdictions, personal data may be processed outside your country of residence. Where required, Ciforus will use appropriate safeguards for such transfers.

10. Data Retention

Ciforus retains information only for as long as reasonably necessary for the purposes described in this policy, including:

- providing and securing the service
- preserving launch or account records
- meeting legal, accounting, tax, or regulatory obligations
- resolving disputes and enforcing agreements

Examples:

- wait-list records may be retained until launch communications are complete, the data is no longer useful, or you request deletion where applicable
- support and security records may be retained for operational and evidentiary reasons
- compliance and financial records may be retained for longer periods where required by law or risk policy

11. Your Rights and Choices

Depending on applicable law, you may have rights to:

- access personal data held about you
- request correction of inaccurate data

- request deletion of certain data
- object to or restrict certain processing
- withdraw consent where consent is relied on
- request portability of certain personal data
- lodge a complaint with a relevant data-protection authority

These rights are not absolute and may be limited where legal obligations, security concerns, fraud prevention, or the rights of others require it.

12. Security Measures

Ciforus uses a mix of administrative, technical, and organizational safeguards designed to protect service integrity, confidentiality, and access control. These measures may include:

- encryption controls
- access restrictions and role separation
- security hardening
- logging and abuse detection
- wallet verification and account protection controls
- recovery and authentication controls such as TOTP or recovery-based workflows where relevant

No system is perfectly secure. Users also remain responsible for safeguarding their own devices, credentials, wallets, recovery materials, and operational security.

13. Children and Age Restrictions

Ciforus is not intended for children. You must be at least the legal age required to use the service in your jurisdiction, and at least the age required for token participation or compliance onboarding where those features apply.

14. Token, Payment, and Compliance-Related Privacy

If Ciforus operates token sales, wallet-linked entitlements, or compliance screening, additional privacy handling may apply. Ciforus may need to collect or verify information connected to:

- wallet ownership
- sanctions or restricted-jurisdiction checks
- source-of-funds review
- anti-money laundering review
- transaction screening and dispute handling

Where these processes apply, Ciforus will aim to collect only what is reasonably necessary for legitimate risk control and legal compliance.

15. Changes to This Policy

Ciforus may update this Privacy Policy from time to time to reflect product development, legal obligations, launch changes, or operational improvements. The updated version will become effective when published unless a later date is stated.

16. Contact

Privacy questions, rights requests, and legal notices related to this policy may be directed through the official Ciforus contact details or legal channels published on the Ciforus website.

17. Reference Principles Used in Drafting

This document was structured using the current Ciforus product narrative and informed by official transparency and privacy-notice guidance, including GDPR transparency principles, ICO guidance on the right to be informed, and related privacy-law best practices.