

ÂTRIUM PLATFORM PRIVACY POLICY

Last Updated: 30.05.2025

1. INTRODUCTION

- 1.1. This Privacy Policy (the "**Policy**") explains how Âtrium Lab (the "**Platform Operator**," "we," "our," or "us") collects, uses, shares, stores, and protects personal data of individuals ("you," "your," or "**Users**") who interact with the **Âtma Token** (the "**Token**") and the atrium.io platform (the "**Platform**").
- 1.2. This **Policy** is issued in accordance with applicable data protection and privacy regulations, including the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and is designed to promote transparency regarding how your data is handled when engaging with our smart contracts, governance systems, and web interfaces.
- 1.3. By accessing the **Platform**, you acknowledge that you have read and understood this Privacy **Policy** and consent to our practices as described herein. This **Policy** applies to all interactions with the **Platform**, including but not limited to web-based services, mobile applications, and associated communication channels.
- 1.4. The **Platform Operator** processes personal data of **Users** solely where necessary for the provision of services, and only with the **User's** valid consent, in accordance with applicable data protection laws.
- 1.5. This **Policy** should be read in conjunction with our Terms and Conditions, which further outline the legal framework for your use of the **Platform**. If you do not agree to this **Policy**, please refrain from using the **Platform**.

2. DATA CONTROLLER:

The **Platform Operator** acts as the data controller under this **Policy**:

Atrium Lab Inc.
807 Ave Ponce de Leon
PMB [#0113]
San Juan, Puerto Rico 00907
Contact email address: contact@atriumlab.io

As a data controller, we determine the purposes and means of processing personal data in relation to your interaction with the **Token** and **Platform**. If we use third-party data processors to handle

data on our behalf, we ensure they are contractually bound to comply with strict data protection obligations.

3. SCOPE OF APPLICATION:

This **Policy** applies to personal data collected through:

- 3.1. The **Platform's** user interface and any affiliated subsites;
- 3.2. Smart contracts associated with the **Âtma Token** and related Web3 features;
- 3.3. **Token** issuance, governance, staking, transfer, and burn mechanisms;
- 3.4. Communications between **Users** and the **Platform Operator**, including support requests and feedback;
- 3.5. Public forums, social media pages, or community tools hosted or moderated by the **Platform Operator**;
- 3.6. Any off-chain services or events linked to the **Platform** (e.g., workshops, educational webinars, or hackathons).

This **Policy** does not apply to third-party platforms, DApps, or blockchain explorers that may be accessible via links on our **Platform**. We are not responsible for the privacy practices of those external services.

4. INFORMATION WE COLLECT

4.1. Information You Provide to Us

We collect the following types of information that you voluntarily provide when you interact with the **Platform**:

- 4.1.1.1. Account Information: This includes blockchain wallet addresses and interactions with **Smart Contracts**, usernames, passwords (where applicable), and profile-related details such as preferences and account settings. These identifiers are pseudonymous but may become identifiable if linked with other data.
- 4.1.1.2. Communications Data: Information shared through customer support inquiries, emails, and social media interactions.
- 4.1.1.3. User-Generated Content: Any content you upload, submit, or share on the **Platform**, including, messages, comments, and feedback.
- 4.1.1.4. Payment Information: When applicable, **Users** may provide financial details related to transactions carried out on the

Platform, subject to applicable laws.

4.2. Information Collected Automatically

4.2.1. We may collect certain data automatically when you access the **Platform**, including:

- 4.2.1.1. Device Information: Technical details about your device, such as device type, operating system, browser type, wallet address, IP address, and unique device identifiers.
- 4.2.1.2. Usage Data: Information related to how you interact with the **Platform**, including page visits, features used, referral sources, and navigation paths.
- 4.2.1.3. Transaction Data: Details about blockchain transactions conducted on the **Platform**, including timestamps, **Token** amounts, and smart contract interactions.
- 4.2.1.4. Staking and Governance Data: Public votes, staking records, proposal creation, and participation logs, all linked to wallet addresses.
- 4.2.1.5. Cookies and Tracking Technologies: We do **not** use cookies, pixel tags, or other tracking mechanisms to collect data and improve user experience.

4.3. Information from Third-Party Sources

4.3.1. We may obtain information about you from third parties (**Third-Party-Sub-Processor**) including:

- 4.3.1.1. Blockchain Networks: Publicly available data related to blockchain interactions.
- 4.3.1.2. Analytics Providers: Aggregated data insights regarding **Platform** usage trends and performance.
- 4.3.1.3. Customer Due diligence, KYC/AML: Data Collected: Privately obtained personal information of the **Token Holder**.
 - 4.3.1.3.1. **Purpose of Processing**: To conduct initial due diligence on prospective customers to ensure compliance with the **Token's** risk appetite and regulatory requirements.
- 4.3.1.4. Marketing Partners: Information provided through promotional campaigns or referral programs.

We do not knowingly collect or process any special categories of data, such as information regarding your racial or ethnic origin, political opinions, religious beliefs, health, or biometric identifiers.

5. LEGAL BASIS FOR PROCESSING

We rely on the following legal grounds under data protection law to process your data:

- 5.1. Performance of a Contract: Data processing necessary to facilitate your use of the **Platform** and interact with Token functionalities.
- 5.2. Legitimate Interests: Including fraud prevention, **Platform** maintenance, and ensuring an optimal user experience. We ensure that our interests are balanced against your rights.
- 5.3. Compliance with Legal Obligations: We may be legally required to collect, retain, or share certain data under AML, CTF, tax, or securities regulations.
- 5.4. Consent: For optional services such as email updates, newsletters. You may withdraw your consent at any time through available interfaces or by contacting us directly.

6. HOW WE USE YOUR INFORMATION

- 6.1. We process collected information for the following purposes:
 - 6.1.1. To Provide and Maintain the Platform: Ensure seamless operation, access to services, and personalised functionality, including the monitoring of system performance, detecting technical issues, and improving operational efficiency.
 - 6.1.2. Account Management: Facilitating the registration process, wallet ownership and authenticating staking or governance participation, verifying your identity, managing user preferences, and providing administrative notifications.
 - 6.1.3. Transaction Facilitation: Processing on-chain transactions and staking activities, ensuring transparency and compliance with blockchain protocols.
 - 6.1.4. Security and Fraud Prevention: Implementing risk monitoring to prevent unauthorised access, fraudulent activities, and potential cybersecurity threats. This includes monitoring for unusual activity and securing digital

assets.

- 6.1.5. Compliance with Legal Obligations: Meeting regulatory and legal requirements, including financial, tax, and anti-money laundering obligations in accordance with applicable laws.
 - 6.1.6. Marketing and Communication: To respond to support inquiries or complaints submitted via contact forms or email, sending promotional materials, service updates, surveys, and notifications related to **Platform** features, improvements, and relevant offerings.
 - 6.1.7. Analytics and Performance Monitoring: Collecting data to understand usage trends, user engagement, and functionality preferences to enhance **Platform** services and ensure scalability.
 - 6.1.8. User Support: Responding to inquiries, resolving technical issues, and improving customer experience by providing accurate and efficient assistance.
 - 6.1.9. Customisation: Tailoring user experiences based on preferences and behavioural data to offer a personalised interface and suggested content.
- 6.2. **Users** can manage their communication preferences and opt out of certain communications by adjusting their settings within the **Platform**.

We will not use your personal data to create profiles of users, conduct predictive behavior analysis, or engage in automated decision-making that has legal effects.

7. SHARING OF INFORMATION

- 7.1. Public Ledger: All on-chain transactions, including voting and staking, are permanently and publicly visible on the blockchain. This is an inherent feature of blockchain technology.
- 7.2. With Service Providers
- 7.3. We may share personal information with trusted third-party service providers that assist us in operating, maintaining, and improving the **Platform**. This may include hosting services, analytics tools, cloud computing providers, and email service platforms. These providers are required to process data in accordance with applicable data protection standards, including:

Service	Purpose	Data Processed	Cookies/ Tracking	Hosting / Location	Compliance Notes
Vercel	Hosts the frontend application and provides built-in analytics	IP addresses, request headers, user-agent, page views, performance metrics	Cookie-less analytics by default	Global edge network (AWS/GCP-backed)	GDPR-compliant, DPA available (https://vercel.com/legal/dpa)
AWS EC2	Hosts backend API, processes requests from frontend	IPs, request headers, wallet addresses, user data, logs	No cookies; session/token via headers	AWS Region (e.g., US-East-2)	AWS handles infra compliance, app logic is customer responsibility
OVHcloud	Hosts Cardano node for blockchain interactions	Public blockchain data (wallets, txns), server logs, ledger files	None	VPS hosted in selected OVHcloud region (Canada – East)	GDPR-compliant, public pseudonymous data only, customer-controlled configuration
Local Context Provider (in-browser)	Maintains real-time application state for user sessions, syncing with backend and blockchain data	Non-sensitive user session data from blockchain such as wallet address, NFT hash as well as data in our backendlike selected profile, and optionally linked Discord/Twitter IDs	No cookies; data is stored in-memory or browser session	User's local browser	Session state is initialized using backend and blockchain data. If a user links Discord or Twitter/X to their NFT profile, their platform user ID will be stored in the local session for app functionality. All linking is opt-in and user-initiated.

7.3.1. Professional Advisors: Legal, tax, or cybersecurity consultants may be given access to data in the course of performing their services.

7.3.2. These service providers are contractually obligated to use the information solely for the purpose of providing services to us and must implement security measures to protect the data.

7.4. Legal and Regulatory Disclosures

7.4.1. We may disclose your information if required by applicable laws, regulations, legal processes, or government requests. Such disclosures

may occur in cases involving:

- 7.4.1.1. Compliance with court orders or subpoenas;
- 7.4.1.2. Enforcement of our legal rights;
- 7.4.1.3. Prevention of fraud or illegal activities;
- 7.4.1.4. Protection of the safety and security of our **Users** and **Platform**.

7.5. Aggregated or Anonymised Data

- 7.5.1. We may share aggregated or anonymised data that cannot reasonably identify you with third parties for purposes such as research, analytics, and business development.

8. **DATA SECURITY**

8.1. Security Measures

- 8.1.1. We take appropriate technical and organisational measures to safeguard your personal information from unauthorised access, disclosure, alteration, and destruction. These measures include:

- 8.1.1.1. Encryption: Encrypting sensitive information during transmission and storage.
- 8.1.1.2. Access Controls: Restricting access to personal data to authorised personnel only.
- 8.1.1.3. Regular Security Audits: Conducting periodic assessments of our security infrastructure.
- 8.1.1.4. Incident Response Plans: Implementing strategies to respond promptly to potential data breaches.

8.2. User Responsibilities

- 8.2.1. While we take reasonable measures to protect your data, **Users** are responsible for maintaining the security of their accounts by:

- 8.2.1.1. Using strong and unique passwords;
- 8.2.1.2. Enabling multi-factor authentication (if available);
- 8.2.1.3. Avoiding sharing sensitive login credentials with others;
- 8.2.1.4. Regularly reviewing account activity.

8.3. Security Breaches

- 8.3.1. In the event of a personal data breach, the **Platform Operator** will take all appropriate technical and organizational measures to mitigate its impact and protect affected **Users**. In compliance with the General Data

Protection Regulation (GDPR), the **Platform Operator** shall notify the relevant National Competent Authority (NCA) without undue delay and, where feasible, no later than **72 hours** after becoming aware of the breach, unless a reasoned justification exists for a delay.

- 8.3.2. Furthermore, where the breach is likely to result in a high risk to the rights and freedoms of affected data subjects, the **Platform Operator** will also notify those individuals without undue delay, in accordance with applicable legal obligations and exemptions.

8.4. No Absolute Security Guarantee

- 8.4.1. Despite our efforts to protect your data, no system can guarantee absolute security. **Users** acknowledge the inherent risks of online interactions and blockchain-based transactions.

9. **COOKIES AND TRACKING TECHNOLOGIES:**

The **Platform** does **not** use cookies or related technologies. To enhance clarity, the **Platform Operator** provides the following information:

Cookies are small text files that are stored on your device (computer, smartphone, or other internet-enabled device) when you visit a website. They are widely used to make websites work more efficiently, as well as to provide information to the site owners. Depending on their purpose, cookies can be categorized as:

- 9.1. Essential Cookies: Enable core site functionality and authentication mechanisms;
- 9.2. Performance Cookies: Collect aggregated statistics about **User** behavior and site performance;
- 9.3. Functional Cookies: Remember **User** preferences and settings for a personalized experience;
- 9.4. Analytics Tools: Such as Google Analytics or open-source equivalents to track session behavior and optimize site functionality.

10. **Data Retention**

10.1. Retention Period

- 10.1.1. We retain your personal data for as long as necessary to fulfill the purposes outlined in this **Policy**, comply with legal and regulatory obligations, resolve disputes, and enforce our agreements.
- 10.1.2. The retention period may vary depending on the type of data and the purposes for which it is processed. The criteria used to determine the

retention period include:

- 10.1.2.1. Regulatory and Legal Requirements: Compliance with applicable laws and industry regulations that require certain records to be maintained for a specific duration (**five years**).
- 10.1.2.2. Business Needs: Fulfilling operational, contractual, and performance obligations (e.g., staking records)- **One year**.
- 10.1.2.3. Security Considerations: Preventing fraud, ensuring data integrity, and addressing security vulnerabilities.

10.2. Data Minimisation and Anonymisation

- 10.2.1. We take measures to ensure that personal data is only retained as long as necessary. Where possible, data is anonymised or pseudonymised to minimise exposure. Anonymised data, which no longer identifies a **User**, may be retained indefinitely for analytical and statistical purposes.

11. DATA SECURITY

We take your privacy seriously and implement the following protective measures:

- 11.1. Secure HTTPS communication;
- 11.2. Blockchain-level cryptographic protections;
- 11.3. Firewalls, DDoS mitigation, and multi-region redundancy for our infrastructure;
- 11.4. Access controls based on roles and business necessity;
- 11.5. Ongoing monitoring and threat detection systems.

We encourage you to secure your own access credentials, update wallets regularly, and avoid sharing private keys or personal identifiers on-chain.

12. USER RIGHTS AND CHOICES

Considering the inherent characteristics of blockchain technology, particularly its immutability and decentralized nature, access, correction, erasure, and portability of **User** data may not always be technically feasible. However, where such actions can be reasonably implemented, the **Platform** will take all appropriate steps to facilitate the exercise of these rights. In general, the **Platform** processes **User** data in anonymised or pseudonymised form, meaning it cannot directly identify an individual. Nonetheless, in specific cases where the **Platform** collects or processes identifiable personal data (such as for Know-Your-Customer (KYC) or Anti-Money

Laundrying (AML) purposes), **Users** retain the right to exercise the following rights, in accordance with applicable data protection laws:

12.1. Access and Correction

- 12.1.1. **Users** have the right to request access to their personal data and verify its accuracy. You may request corrections to any inaccurate or incomplete personal information that we hold about you.

12.2. Right to Erasure

- 12.2.1. Subject to applicable laws, **Users** have the right to request the deletion of their personal data under the following circumstances:

- 12.2.1.1. When the data is no longer necessary for the purposes for which it was collected;
- 12.2.1.2. When consent is withdrawn (if processing was based on consent);
- 12.2.1.3. When the data was processed unlawfully.

- 12.2.2. We will comply with such requests unless retention is necessary to comply with legal obligations.

12.3. Data Portability

- 12.3.1. **Users** have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another data controller where technically feasible.

12.4. Right to Object

- 12.4.1. **Users** may object to the processing of their data in cases where processing is based on legitimate interests or direct marketing purposes. Upon receiving an objection, we will assess whether compelling legitimate grounds override the **User's** interests and act accordingly.

12.5. Right to Restriction of Processing

- 12.5.1. **Users** have the right to request restrictions on the processing of their personal data if they contest the accuracy of the data, object to its processing, or require data for legal claims while the request is being reviewed.

12.6. Withdrawal of Consent

- 12.6.1. Where processing is based on **User** consent, Users have the right to withdraw their consent at any time. Withdrawal of consent does not affect the lawfulness of processing conducted prior to such withdrawal.

- 12.7. Lodging a Complaint

- 12.7.1. If **Users** believe their rights under applicable data protection laws have been violated, they have the right to lodge a complaint with the data protection authority of the British Virgin Islands, [the Office of the Information Commissioner](#).

The **Platform** will respond to such requests within one month, unless doing so would infringe upon the rights or freedoms of others (e.g., intellectual property rights or confidentiality obligations). In such cases, the **Platform** will provide a justified explanation for any limitations on the request.

13. INTERNATIONAL DATA TRANSFERS

- 13.1. Cross-Border Transfers

- 13.1.1. We may transfer personal data to jurisdictions outside of the **User's** country of residence where data protection laws may differ. When such transfers occur, we implement safeguards to ensure adequate protection, including:

- 13.1.1.1. Standard Contractual Clauses approved by regulatory authorities;
- 13.1.1.2. Privacy Shield frameworks (where applicable);
- 13.1.1.3. Binding corporate rules adopted by affiliated entities.
- 13.1.1.4. Technical safeguards such as encryption;
- 13.1.1.5. Verification of third-party compliance with recognized data protection frameworks.

By using the **Platform**, you agree to the transfer of your data across borders as necessary for the services.

- 13.2. Security Measures for International Transfers

- 13.2.1. In all international transfers, we implement encryption, access controls, and secure communication protocols to ensure personal data remains protected regardless of jurisdiction.

14. CHANGES TO THIS PRIVACY POLICY

- 14.1. We reserve the right to modify this **Policy** at any time to reflect changes in legal requirements, operational needs, or technological advancements. In the event of significant changes, we will notify **Users** through:
 - 14.1.1. Posting updates on the **Platform**;
 - 14.1.2. Sending notifications via email (if applicable);
 - 14.1.3. Providing a summary of key changes.
- 14.2. Continued use of the **Platform** after any updates to this **Policy** signifies acceptance of the changes.