PRIVACY POLICY

ASSETARA LIMITED

Effective Date: 20 October 2026

1. INTRODUCTION

This Privacy Policy ("Policy") describes how ASSETARA LIMITED, a private company limited by shares incorporated in England and Wales, United Kingdom, under the Companies Act 2006, company number 17530240, with its registered office at 152 Hawthorn Road, Ashington, United Kingdom, NE63 9BG ("Company", "we", "us", or "our"), collects, uses, processes, stores, and discloses personal data of individuals who access and use the Assetara platform and services.

The Assetara platform ("Platform") is accessible through the website assetara.ai, associated mobile applications, and smart contracts deployed on the BNB Chain blockchain.

This Policy applies to:

- **Visitors:** individuals who browse the Platform without registering
- **Users:** individuals who register an account and use the Services

This Policy should be read in conjunction with our Terms of Use available at https://assetara.ai/terms.

This Policy is a transparency notice, not a request for blanket consent. We rely on the lawful bases described below. Where consent is required, we request it separately. Publication of this Policy does not itself transfer personal data or controller responsibilities from any other legal entity.

2. DATA CONTROLLER

ASSETARA LIMITED, company number 17530240, registered in England and Wales, United Kingdom, is the controller for the processing described in this Policy. Registered office: 152 Hawthorn Road, Ashington, United Kingdom, NE63 9BG. Privacy contact: legal@assetara.ai.

The applicable UK framework includes the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended, including by the Data (Use and Access) Act 2025. The EU GDPR and other local laws also apply where their territorial requirements are met.

We apply data protection by design and by default. This notice does not state that a statutory Data Protection Officer has been appointed; requests should be addressed to the privacy contact above.

3. LEGAL BASIS FOR PROCESSING

We process your personal data based on the following legal grounds:

3.1 Contractual Necessity

Processing is necessary for the performance of the Terms of Use to which you are a party, including:

- Account creation and management
- Transaction processing
- Service delivery

3.2 Legal Obligation

Where a specific legal obligation applies to the Company, we process the data necessary to meet it, including applicable anti-money laundering, counter-terrorist financing, sanctions, tax reporting, court order and regulatory reporting requirements. Legal obligations are not assumed solely because the Company is incorporated in the UK.

Where KYC or fraud-prevention checks are not legally required, we assess whether they are necessary for our legitimate interests, subject to the balancing assessment described in section 3.3. Special-category or criminal-offence information requires additional legal conditions; a general legitimate interest is not sufficient on its own.

3.3 Legitimate Interests

Where necessary and proportionate, and after balancing our interests against your rights and freedoms, we rely on legitimate interests for the following purposes:

- Platform security and fraud prevention
- Service improvement and analytics
- Network and information security
- Internal business administration

3.4 Consent

Where required, we obtain freely given, specific, informed and unambiguous consent, and explicit consent where the law requires it, for:

- Marketing communications
- Optional features requiring additional data processing
- Cookies and tracking technologies

You may withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

4. DATA WE COLLECT

Depending on the Services you use and what is necessary, we collect the following categories of personal data:

4.1 Account and Identity Data

- Full name
- Email address
- Password (stored using a one-way hash; never intentionally stored in plain text)
- Date of birth

- Country of residence
- Cryptocurrency wallet address(es)
- Username or display name
- Account registration timestamp

4.2 KYC and AML Verification Data (when required)

- Government-issued identification documents (passport, national ID, driver's license)
- Proof of address documents (utility bills, bank statements)
- Selfie photographs for identity verification
- Source of funds information
- Beneficial ownership information (for corporate accounts)
- Politically Exposed Person (PEP) status
- Sanctions screening results

4.3 Financial and Transaction Data

- Deposit and withdrawal transaction history
- Trading activity and order history
- Investment plan participation and balances
- Staking pool participation and rewards
- Token purchase history (ASRA ICO participation)
- Wallet balances and asset holdings
- Transaction amounts, timestamps, and blockchain addresses
- Gas fees and transaction costs

4.4 Technical and Usage Data

- IP address and geolocation data
- Device type, model, and operating system
- Browser type and version
- Mobile device identifiers (IDFA, Android ID)
- Session duration and activity timestamps
- Pages viewed and features accessed
- Click-stream data and navigation patterns
- API request logs
- Error logs and crash reports

4.5 Referral and Rewards Program Data

- Referral codes and links generated
- Referrer and referee relationships
- Commission earnings and bonuses
- Referral network structure
- Reward claim history

4.6 Communication and Support Data

- Email correspondence
- Support ticket messages
- Live chat transcripts
- Communication preferences

- Newsletter subscription status
- Feedback and survey responses

4.7 Blockchain Data

As a non-custodial platform, certain data is recorded immutably on public blockchains:

- Transaction hashes
- Smart contract interactions
- Wallet addresses
- Token transfers and balances
- *Important:* Blockchain data is permanent, public, and cannot be deleted or modified by Assetara.

5. HOW WE COLLECT DATA

- **Direct Collection:** Data you provide directly when creating an account, completing KYC verification, making deposits/withdrawals, or contacting customer support.
- **Automatic Collection:** Technical data through cookies, usage analytics, log files, and blockchain transaction monitoring.
- **Third-Party Sources:** Data received from KYC/AML verification providers, blockchain explorers, security services, and payment processors.

6. PURPOSES OF DATA PROCESSING

We use your personal data for Service Provision, Regulatory Compliance (KYC/AML), Platform Security, Customer Support, Analytics & Improvement, Marketing (with consent), and Business Operations.

7. DATA SHARING AND DISCLOSURE

7.1 No Sale of Data

We do not sell, rent, or trade your personal data to third parties for marketing or commercial purposes.

7.2 Service Providers and Data Processors

We may share your data with trusted third-party service providers who process data on our behalf and under our strict instructions, including:

- Identity verification and KYC/AML service providers
- Cloud hosting and infrastructure providers
- Payment gateways and fiat-to-crypto processors
- Analytics, monitoring, and security service providers
- Customer support and communication platform tools

7.3 Legal and Regulatory Disclosures

We may disclose your personal data if required to do so by law, court order, subpoena, or valid regulatory request, or when we reasonably believe in good faith that disclosure is necessary to:

- Comply with legal obligations or statutory mandates
- Protect against legal liability or defend legal claims
- Investigate, prevent, or act regarding illegal activities, fraud, or security threats
- Protect the safety and rights of Assetara, our Users, or the public

7.4 Corporate Reorganization

In the event of a merger, acquisition, corporate restructuring, asset sale, or joint venture involving ASSETARA LIMITED, user personal data may be transferred to the acquiring or surviving legal entity subject to the commitments in this Privacy Policy.

8. INTERNATIONAL DATA TRANSFERS

8.1 Cross-Border Transfers

Personal data collected by Assetara may be stored, processed, or transferred outside the United Kingdom to countries where our third-party infrastructure or service providers operate.

8.2 Safeguards for Restricted Transfers

When transferring personal data internationally outside the UK under the UK GDPR, we ensure that appropriate safeguards are implemented to protect your data, including:

- **Adequacy Decisions:** Transfers to countries recognized by the UK Secretary of State as providing an adequate level of data protection.
- **Standard Contractual Mechanisms:** Use of the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses (SCCs).
- **Derogations:** Transfer based on explicit consent or performance of a contract in limited circumstances.

9. DATA RETENTION

9.1 Account and Service Data

We retain personal data for as long as your Assetara Account remains active or as needed to provide you with access to the Platform Offerings.

9.2 Statutory AML Retention Period

Under the UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, personal data collected for KYC and AML identity verification is retained for a mandatory period of **five (5) years** following the termination of the business relationship or the completion of a transaction.

9.3 Blockchain Data Notice

Due to the technical architecture of public blockchains (including BNB Chain), transaction data, wallet addresses, and smart contract execution records posted to the blockchain are immutable and cannot be deleted or altered by Assetara.

10. DATA SECURITY

10.1 Security Measures

ASSETARA LIMITED implements robust technical and organizational security measures to protect personal data against unauthorized access, destruction, loss, alteration, or disclosure, including:

- End-to-end encryption for data in transit (TLS 1.3) and data at rest (AES-256)
- Password hashing using salt and bcrypt algorithms
- Multi-factor authentication (2FA) support
- Regular penetration testing and vulnerability assessments
- Strict role-based access control (RBAC) for internal staff

10.2 Non-Custodial Security Notice

As a Non-Custodial SaaS platform, Assetara does not store, hold, or have access to your private cryptographic keys. You remain solely responsible for the security of your non-custodial wallet and private credentials.

11. YOUR RIGHTS

11.1 Rights Under UK GDPR

Subject to statutory conditions and exceptions, you have the following data protection rights:

- **Right of Access:** Request a copy of the personal data we hold about you.
- **Right to Rectification:** Request correction of inaccurate or incomplete personal data.
- **Right to Erasure ("Right to be Forgotten"):** Request deletion of your personal data, except where retention is required by legal obligations (e.g., 5-year AML retention) or public blockchain immutability.
- **Right to Restriction of Processing:** Request temporary restriction of your data processing under certain circumstances.
- **Right to Data Portability:** Request transfer of your data to another controller in a structured, commonly used machine-readable format.
- **Right to Object:** Object to processing based on legitimate interests or for direct marketing purposes.

11.2 Exercising Your Rights

To exercise any of these rights, submit a written request to our Privacy Contact at `legal@assetara.ai`.

11.3 Supervisory Authority Complaint

You have the right to lodge a complaint with the UK Information Commissioner's Office (ICO), the UK data protection supervisory authority:

- **Website:** https://ico.org.uk
- **Address:** Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

12. COOKIES AND TRACKING TECHNOLOGIES

12.1 Cookie Types

We use cookies and similar tracking technologies on assetara.ai for:

- **Essential Cookies:** Necessary for basic platform functionality and security.
- **Functional Cookies:** Remember user preferences and custom configurations.
- **Analytics Cookies:** Track aggregated platform performance and user engagement metrics.

12.2 Managing Preferences

Non-essential cookies are set only with your prior consent. You can manage or withdraw your cookie choices at any time via the cookie settings banner on assetara.ai or through your internet browser settings.

13. CHILDREN'S PRIVACY

The Platform is not intended for individuals under 18 years of age. We do not knowingly collect or solicit personal data from minors. If we become aware that we have inadvertently collected personal data from a minor without verified parental consent, we will take immediate steps to delete such information from our servers and systems.

14. AUTOMATED DECISION-MAKING

We may use automated algorithms and processing systems for the following purposes:

- **Fraud Detection & Security:** Automated monitoring of transaction patterns to detect suspicious account activities.
- **KYC/AML Screening:** Automated cross-referencing of identity details against international sanctions lists and PEP databases.
- **AI Trading Engine:** Automated processing of algorithmic strategies and market data execution.

Where an automated decision produces legal effects or similarly significant effects concerning you, you have the right to request human intervention, express your point of view, and contest the decision by contacting `legal@assetara.ai`.

15. DATA BREACH NOTIFICATION

In the event of a personal data breach affecting your information, ASSETARA LIMITED will assess the risk to your rights and freedoms. If required under the UK GDPR, we will notify the UK Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after becoming aware of it. Where the breach is likely to result in a high risk to your rights and freedoms, we will also communicate the breach to affected users without undue delay.

16. CHANGES TO THIS POLICY

We reserve the right to update or modify this Privacy Policy at any time to reflect changes in our legal obligations, platform features, or operational practices. We will notify users of any material changes by:

- Posting the updated Privacy Policy on assetara.ai with a revised "Effective Date"
- Sending an email notification to registered account holders, where appropriate
- Displaying a prominent notice on the Platform interface

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your personal data.

17. CONTACT INFORMATION

If you have any questions, concerns, or requests regarding this Privacy Policy or our data protection practices, please contact our team using the following details:

- **Data Controller:** ASSETARA LIMITED
- **Companies House Registration No.:** 17530240
- **Country of Registration:** United Kingdom (England and Wales)
- **Registered Office Address:** 152 Hawthorn Road, Ashington, United Kingdom, NE63 9BG
- **Privacy & Legal Contact:** legal@assetara.ai
- **Support Contact:** support@assetara.ai
- **Official Website:** https://assetara.ai

18. JURISDICTION-SPECIFIC PROVISIONS

18.1 European Economic Area (EEA) Users

If you are located in the European Economic Area (EEA), you benefit from additional rights and protections under the EU General Data Protection Regulation (EU GDPR), including:

- Enhanced transparency requirements regarding data processing activities.
- Strengthened and explicit consent provisions where consent is used as a lawful basis.
- The right to data portability in a structured, commonly used, and machine-readable format.
- The absolute right to lodge complaints directly with your national data protection supervisory authority within your country of residence or work.

Where an EU representative is legally required under Article 27 of the EU GDPR, we provide its identity and direct contact details before the relevant processing begins. You may contact `legal@assetara.ai` to inquire about representation relevant to your specific location.

18.2 California Residents (CCPA)

Where the California Consumer Privacy Act (CCPA), as amended, applies to the Company and its processing activities, California residents have specific applicable statutory rights, including:

- The right to know what categories of personal information are collected, used, disclosed, or sold.
- The right to request the deletion of personal information collected, subject to statutory exceptions (such as legal obligations and immutable blockchain records).
- The right to opt-out of the "sale" or "sharing" of personal information.
- The right to non-discrimination for exercising your privacy rights under the CCPA.

Important Notice: **ASSETARA LIMITED does not sell personal information** as defined by the CCPA.

To exercise your California privacy rights, you may submit a request by emailing `legal@assetara.ai` with the subject line "California Privacy Rights".

18.3 Other Jurisdictions

Users residing in jurisdictions outside the United Kingdom, EEA, and California may possess additional local statutory rights under their respective data protection laws. We invite users in other regions to contact us at `legal@assetara.ai` to inquire about specific rights applicable to their geographic location.

THIS POLICY EXPLAINS OUR PERSONAL DATA PRACTICES AND YOUR RIGHTS. IT DOES NOT WAIVE YOUR STATUTORY RIGHTS OR REPLACE ANY SEPARATE CONSENT REQUIRED BY LAW.

ASSETARA LIMITED. Your Capital. Optimized by AI. Protected by Blockchain.

Last updated: 10 November 2026 | Version: 2.1 | England and Wales

Companies House Registry Link:
https://find-and-update.company-information.service.gov.uk/company/17530240