Privacy Policy

> **Effective Date**: *[05 March, 2025]*

Welcome to VTI3.net ("**the Platform**," "**we**," "**us**," "**our**," or "**the Company**"), along with our subsidiaries and branches. We are committed to respecting and safeguarding your personal data and privacy. This Privacy Policy is a legally binding agreement between you ("**you**" or "**user**") and VTI3.net. Please read it carefully.

By using or registering on the Platform, you acknowledge that you have read, understood, and agreed to this Privacy Policy. If you do not agree with any part of this Privacy Policy, or if you are under the age of 16, please do not provide us with any personal data or use our services. In such cases, you may be unable to access certain features of the Platform.

---

1. Applicability of This Privacy Policy

This Privacy Policy applies to all services and products provided by VTI3.net, its subsidiaries, and branches through the Platform, websites, applications (apps), or other interfaces under our control. This includes (but is not limited to) blockchain technology services, data products, identity verification services, over-the-counter (OTC) trading aggregation platforms, and cryptocurrency- or fiat-related activities offered by us.

---

2. Prohibition of Minors Under Age 16

Our products and services are **not** intended for children under the age of 16. If you are under 16 years old, **please do not use or register** on the Platform or provide any personal data to us. Should we become aware that a user under the age of 16 has provided personal data through the Platform, we will take reasonable steps to verify and delete such information.

We encourage parents or legal guardians to supervise their children's use of the internet. If you are aware that a child under 16 has provided us with personal data, please contact us promptly at info@VTI3.net.

---

3. Data Controllers and Data Processors

Depending on the specific circumstances in which your personal data is handled, VTI3.net may act as either a **Data Controller** or a **Data Processor**:

1. **Data Controller**:
    - For digital signature, identity/registration verification, encryption/authentication, and other core processing activities **we initiate**, we typically determine the purposes and means of processing. Therefore, we act as a Data Controller, as defined by the General Data Protection Regulation ("**GDPR**").
2. **Data Processor**:
    - After your personal information is authenticated by a third party, we encrypt the data you provide and generate a personal data document stored locally on your own device. In such scenarios, **you** (the user) may be considered the Data Controller of any subsequent use or sharing of the locally stored data, and VTI3.net acts merely as the Data Processor, processing data strictly according to your instructions or the technical functionalities you initiate.

If you have questions about the roles we perform (Controller or Processor) for specific data processing activities, please contact us at info@VTI3.net.

---

4. Personal Data Collected by the Platform

4.1 Personal Data You Provide

Type	Specific Description
Personal Data	When you register or connect your Personal account to our website/App, we may collect your personal address (e.g., email), transaction data, sender's/recipient's name, amount, currency preference, payment method, etc.
Public Data	We may analyze public data (e.g., published offer, transaction IDs, digital signatures, social media account, email addresses) which may include personal data if it can identify or link back to you.

4.2 Automatically Collected or Generated Data

Type	Specific Description
App, Browser, and Device Data	Data about the device, operating system, and browser you use, including IP addresses, plugin details, and network connections.
Signatures, Public Key, Private Key	- **Digital Signature**: Generated when you use your private key to encrypt data; can be verified by a corresponding public key. - **Public Key**: A digital string used in asymmetric encryption algorithms for encryption/verification. - **Private Key**: A confidential string known only to you.
Product Usage Data	- **Activity Data**: Content you view or click and how you use our services. - **Diagnostic Data**: Performance logs (e.g., timestamps, crash data, error reports) to help us troubleshoot and improve services.
Data From Cookies & Similar	We use cookies or similar technologies to enhance user experience, perform analytics, etc. For more details, please see our Cookie Policy.

4.3 Personal Data Obtained from Third Parties

1. **KYC / AML Data from Third-Party Providers**:
    - **Customer Basic Data**: First/last name, ID number, date of birth, address, nationality, email, etc.
    - **Electronic Identification (EIDV)**: Biometric data based on the photos/videos you provide for identity verification.
    - **Certificate Data**: Passport or ID number, certificate type, issuer, issue/expiration date, etc.
2. **Feedback on Registration Compliance**:

- Certain third-party service providers analyze user data for regulatory compliance. They inform us whether a user meets the Platform's requirements (e.g., KYC checks) and may transmit encrypted results back to us.

> **Note**: Unless legally required, we do **not** request special categories of personal data (e.g., health records, racial/ethnic origin, religious beliefs). If you voluntarily provide such data, you explicitly consent to its processing in accordance with this Privacy Policy.

---

5. Purposes of Collecting and Using Personal Data

We process your personal data under lawful bases provided in the GDPR (e.g., Articles 6 and 7) for the following purposes:

1. **Providing Core Services**:
   - Encryption and authentication services, creating/maintaining your digital signatures, public keys, private keys.
   - Verifying if you meet registration requirements (KYC/AML checks).
   - Hosting/maintaining your digital wallets (fiat and/or cryptocurrency).
2. **Platform Operations**:
   - Providing investment, payment, asset listing, and account management.
   - Processing data as a Data Processor based on your instructions (e.g., storing your encrypted personal data document on your device).
   - Sending service-related notifications, security updates, transaction records.
3. **Security and Compliance**:
   - Investigating suspicious activity or illegal behavior.
   - Preventing, detecting, and fighting fraudulent or unauthorized actions.
   - Complying with legal obligations (e.g., anti-money laundering, tax, or regulatory requirements).

---

6. Storage and Retention of Personal Data

1. **Cloud Storage**:
   - We may store certain encrypted digital signatures and compliance feedback on cloud services (e.g., AWS in France). These data elements are retained only as long as needed to fulfill the purposes described in this Privacy Policy or to meet legal/regulatory requirements.
2. **Locally Stored Data**:
   - After verifying and encrypting your personal data, the Platform generates a personal data document on **your local device** (e.g., through blockchain or other distributed storage). We do **not** store such personal data ourselves.
3. **Retention Periods**:
   - Generally, we delete or anonymize personal data once it is no longer necessary for our legitimate business purposes or to comply with law.

- KYC/AML data or related records may be retained **for at least five (5) years** after an account is closed or as required by local regulations.
- If you wish to delete locally stored data, you may revoke or clear the relevant data via the Platform's interface (e.g., **MY SOURCE.ID**).

4. **Deletion Upon Request**:
   - If no legal obligations or technical constraints prevent us from doing so, we will delete or anonymize personal data upon your valid request.
   - In some cases, we may not be able to delete data if it is required to fulfill legal obligations or investigate fraudulent activities, but we will notify you when that is the case.

---

7. Legal Basis for Processing

Our data processing activities comply with applicable data protection laws. The main legal grounds include:

- **Consent**: Where you have expressly given us permission (e.g., optional marketing, certain cookies).
- **Contract**: Where processing is necessary to provide the services you request or to fulfill our contract with you.
- **Legal Obligation**: Where processing is required by applicable laws or regulations (e.g., AML, tax).
- **Legitimate Interests**: Where processing is necessary to pursue our legitimate interests (e.g., preventing fraud, enhancing security), provided such interests do not override your fundamental rights and freedoms.

You have the right to **withdraw consent** at any time without affecting the lawfulness of processing based on consent prior to withdrawal.

---

8. Third-Party Processing of Personal Data

1. **Third-Party KYC Service Provider**
   - When you first register, you may provide personal data directly to an external KYC/AML service provider (e.g., **TOGGLE LIMITED**). Their privacy policy governs the collection methods and contact details.
2. **Encrypted Feedback**
   - After analyzing your data, the KYC provider gives us a compliance result (e.g., pass/fail) and may transmit encrypted data to confirm your status.
3. **Optional Sharing with Third Parties**
   - Once you receive your authenticated personal data from the Platform, you can choose to share or authorize others to access your data for your own purposes (e.g., identity verification or data product transactions).
   - We will obtain your consent if we intend to share your data for any **new** purposes beyond what is described in this Policy. You may always refuse.

For an updated list or categories of third-party partners (e.g., payment processors, cloud service providers), please refer to any additional documentation on our website or contact info@VTI3.net.

---

9. Cross-Border Data Transfers

- We primarily process personal data within the **European Union (EU)** and the **European Economic Area (EEA)**. However, we may also process data in or transfer data to other jurisdictions to the extent necessary.
- Where personal data is transferred outside the EU/EEA, we use **appropriate safeguards**—such as Standard Contractual Clauses (SCCs)—to ensure compliance with GDPR.
- Once you have access to your authenticated personal data, you (as Data Controller) may authorize third parties outside the EU/EEA to process your personal data. In such situations, **you** are responsible for ensuring an appropriate legal basis and mechanism (e.g., SCCs, user consent) for any cross-border transfers you initiate.

---

10. Data Subject Rights

Depending on your location and specific usage scenarios, you may have the following rights regarding your personal data:

1. **Right of Access**:
    - You may request confirmation of whether we process your personal data and obtain a copy, provided we have access to and are processing it.
2. **Right to Rectification**:
    - You may request correction or completion of inaccurate/incomplete data, where technically feasible and we have access to it.
3. **Right to Erasure**:
    - You may request deletion of your personal data, subject to exceptions (e.g., legal obligations). We will delete the data unless technical or legal constraints prevent us from doing so.
4. **Right to Restrict Processing**:
    - You may request restricted processing if (a) you contest data accuracy, (b) processing is unlawful but you oppose erasure, or (c) we no longer need data, but you need it for legal claims.
5. **Right to Data Portability**:
    - You may request to receive personal data you provided in a structured, commonly used, machine-readable format, and to have it transmitted to another Data Controller where feasible.
6. **Right to Object**:
    - You may object to processing based on our legitimate interests if you have reasons related to your specific situation. We may continue processing if we demonstrate overriding legitimate grounds or need the data to exercise or defend legal claims.
7. **Right to Withdraw Consent**:
    - You may withdraw previously granted consent at any time. Withdrawal does not affect the lawfulness of processing prior to withdrawal.
8. **Right to Lodge a Complaint**:

- If you believe our data handling violates the GDPR or other data protection laws, you have the right to lodge a complaint with a **supervisory authority** in your habitual residence or place of alleged infringement.

> To exercise any of these rights, please contact us via info@VTI3.net. We may require additional information to verify your identity. If we cannot verify your identity or confirm your authority, we cannot fulfill your request.

Important: After you receive Platform-authenticated data (which we do not store), you act as the Data Controller for subsequent data activities. Certain actions (e.g., erasing local data) may require you to adjust your device settings or uninstall browser plugins. We will do our best to guide you through these processes if needed.

---

11. Protection Measures for Personal Data

We take data security seriously and implement comprehensive measures to protect your personal data from accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, or access. These measures include, but are not limited to:

- SSL encryption for data transmission.
- Pseudonymization/anonymization where appropriate.
- Ensuring confidentiality, integrity, availability, and resilience of our systems.
- Regular reviews and assessments of our security measures.
- Internal IT security training and incident response management.

In the event of a data breach that poses a high risk to you, we will notify you and the relevant supervisory authority, as required by law.

---

12. Updates to This Privacy Policy

We regularly review this Privacy Policy to reflect changes in our data processing practices and to ensure transparency. If we make **material changes**, we will provide notice (e.g., prompt you to review an updated version upon login) and allow you an opportunity to review the updated policy before continuing to use the Platform.

---

13. Contact Us

If you have any questions about this Privacy Policy, wish to exercise your data subject rights, or have complaints or suggestions, please contact us:

- **Email**: info@VTI3.net

You also have the right to lodge a complaint with a supervisory authority (such as an EU/EEA Data Protection Authority) if you believe your personal data protection rights have been infringed.