PRIVACY POLICY

Pinicode, powered by Pinitech LTD.
Effective Date: October 7, 2025
Last Updated: October 7, 2025
Version: 1.0

This Privacy Policy explains how **Pinicode** ("**Company**," "**we**," "**our**," or "**us**") collects, uses, stores, shares, and protects personal data in connection with our digital voucher services. Pinicode is committed to maintaining the highest standards of privacy, security, and compliance with applicable data protection laws and other international frameworks.

By using our platform, websites, APIs, or services (collectively, the "Services"), you consent to the practices described in this Privacy Policy.

1. SCOPE AND APPLICABILITY

This Privacy Policy applies to:

- Businesses and corporate clients using Pinicode for voucher management and distribution.
- Resellers and distributors authorized by Pinicode to promote, sell, and distribute vouchers and related services on behalf of the Company.
- End-users purchasing, receiving, or redeeming vouchers through the Pinicode platform.
- Visitors to our websites, apps, or API integrations.

2. INFORMATION WE COLLECT

We collect the following categories of personal and business data:

a. Identification & Verification Data (KYC/AML)

We may request and process identification information to verify your identity, comply with legal and regulatory requirements, and protect against fraud or unauthorized use of our Services. This may include:

- Full name, nationality, and date of birth.
- Government-issued identification documents (such as passport, Emirates ID, or driver's license).

- Proof of residential or business address (utility bills, tenancy agreements, or bank statements).
- Business registration documents and company details for corporate users.

b. Account & Transaction Data

To enable the creation and operation of user accounts, process transactions, and manage voucher-related activities, we collect:

- Contact details, including email address, phone number, and physical or billing address.
- Wallet details, linked payment methods, and account credentials.
- Records of all transactions, including voucher issuance, purchase, and redemption.
- Multi-currency and cross-border payment information where applicable.

c. Technical & Usage Data

When you interact with our platform, websites, or APIs, we automatically collect certain technical and behavioral data to maintain platform security, monitor performance, and improve user experience. This includes:

- Internet Protocol (IP) address, browser type, and device identifiers.
- Geolocation data where permitted.
- Log files, cookies, and analytics information regarding your interactions with our Services.
- API call logs and usage statistics for integrated business accounts.

d. Optional & Voluntary Data

We may also collect additional data that you choose to provide voluntarily. Such data is not mandatory for service delivery but helps us improve customer experience and communication. Examples include:

- Customer support inquiries, service requests, or correspondence.
- Feedback provided through surveys, forms, or communications.
- Marketing preferences and subscription details (e.g., opting in or out of promotional messages).

3. HOW WE USE YOUR DATA

We collect and process personal and business data strictly for legitimate purposes connected to the operation of our Services. The primary ways in which your data is used include:

a. **Service Delivery**
   - To enable the creation, distribution, redemption, and management of digital vouchers and gift cards.
   - To provide secure access to user accounts and ensure the proper functioning of all features.

b. **Compliance and Risk Management**
   - To conduct identity verification and due diligence procedures where necessary.
   - To monitor, detect, and prevent fraud, misuse, or other unauthorized activities.
   - To comply with applicable legal, regulatory, and record-keeping requirements, including anti-money laundering (AML) and counter-terrorist financing (CFT) obligations.

c. **Payment Processing**
   - To process payments and settlements securely, whether through traditional methods (such as bank transfers or card payments) or digital assets (such as cryptocurrency wallets).
   - To support multi-currency and cross-border transactions for global users.

d. **Platform Improvement**
   - To analyze platform usage, monitor system performance, and maintain service reliability.
   - To enhance user experience by developing new features, improving navigation, and optimizing integrations.

e. **Customer Support**
   - To provide responsive assistance through support channels.
   - To troubleshoot technical issues and resolve account or transaction-related concerns.

f. **Marketing and Communication**
   - To share important service updates, security notices, or administrative information.
   - To provide promotional content, product announcements, or offers where you have not opted out.
   - To personalize communication based on your preferences and service usage.

4. LEGAL BASIS FOR PROCESSING

We only process personal and business data where there is a clear and legitimate reason to do so. Depending on the circumstances, processing may take place on one or more of the following grounds:

a. **Contractual Necessity**
   - To establish and maintain your account with Pinicode.
   - To provide the Services you have requested, including the creation, management, and redemption of digital vouchers.
   - To ensure the proper execution of transactions and related activities.

b. **Legal Obligations**
   - To comply with applicable laws and regulations relating to anti-money laundering (AML), counter-terrorist financing (CFT), identity verification (KYC), taxation, accounting, and record-keeping.
   - To respond to lawful requests from government authorities, regulators, or enforcement agencies.

c. **Legitimate Interests**
   - To operate, secure, and improve our Services.
   - To prevent fraud, misuse, or unauthorized access.
   - To develop new features and maintain a reliable platform that benefits both businesses and end-users.

d. **Consent**
   - For marketing communications, promotional offers, or newsletters that you voluntarily opt in to receive.
   - For optional features, surveys, or feedback programs where participation is at your discretion.
   - You have the right to withdraw your consent at any time in relation to activities based solely on consent.

5. DATA SHARING & DISCLOSURE

We respect your privacy and do not sell, rent, or trade personal data to third parties. However, in order to operate effectively and deliver our Services, we may share information with carefully selected third parties under strict confidentiality and data protection obligations. These include:

a. **Regulators and Authorities**
   - To meet legal, regulatory, and supervisory requirements, including anti-money laundering (AML), know-your-customer (KYC), counter-terrorist financing (CFT), and other compliance obligations.
   - To respond to lawful requests, investigations, or enforcement actions by government or regulatory bodies.

b. **Financial and Payment Providers**
   - To enable secure processing, settlement, and reconciliation of transactions.
   - To support both traditional payment methods (e.g., banks, card networks) and digital asset services (e.g., wallet providers).

c. **Business Partners**
   - To facilitate voucher issuance, distribution, and redemption across participating platforms.
   - To integrate partner services that enhance the functionality of the Pinicode platform.

d. **Technology and Cloud Providers**
   - For secure hosting, infrastructure, storage, analytics, and technical support.
   - For integration of APIs and third-party applications that improve performance and scalability.

e. **Professional Advisors**
   - For audits, compliance assessments, and risk management reviews.
   - For legal, financial, or dispute resolution purposes.

6. INTERNATIONAL DATA TRANSFERS

As Pinicode operates on a global scale, your information may be transferred to and processed in jurisdictions outside of your country of residence. These transfers are necessary to ensure the delivery of our Services, particularly where our servers, cloud providers, or business partners are located internationally.

- When transferring data across borders, we take appropriate measures to safeguard your information, including:
- Ensuring that third-party service providers maintain robust confidentiality and security standards.
- Entering into written agreements with partners and vendors that require them to protect data in line with industry best practices.
- Limiting access to authorized personnel with a legitimate business need.

- By using our Services, you acknowledge that your data may be transferred, stored, and processed in countries where data protection standards may differ from those in your home jurisdiction. However, we will always take steps to ensure your information is handled responsibly and securely.

7. DATA RETENTION

We retain personal and business data only for as long as it is reasonably necessary to fulfill the purposes for which it was collected. The retention period will vary depending on the nature of the data and the requirements of applicable laws or business practices. Specifically, data may be retained for the following purposes:

a. **Service Delivery and Account Management**
   - To maintain active user accounts and ensure the continued provision of our Services.
   - To provide historical transaction records and account activity for customer reference.

b. **Legal and Regulatory Compliance**
   - To satisfy statutory obligations, such as anti-money laundering (AML), counter-terrorist financing (CFT), taxation, and accounting requirements.
   - Certain records may be retained for a period of 5 to 10 years, or longer, where required by local laws.

c. **Dispute Resolution and Enforcement**
   - To resolve disputes, investigate claims, and enforce our agreements or terms of service.
   - To protect our legal rights and respond to regulatory or law enforcement inquiries.

8. DATA SECURITY

At Pinicode, protecting your information is a top priority. We implement industry-standard security measures designed to safeguard personal and business data against loss, misuse, unauthorized access, disclosure, alteration, or destruction. These measures include:

a. **Encryption and Secure Transmission**
   - End-to-end encryption of sensitive data during storage and transmission.
   - Use of secure communication protocols (such as HTTPS/TLS) across all platforms.

b. **Wallet and Payment Security**
   - Deployment of secure wallet infrastructure and payment processing systems.
   - Transaction verification and fraud-prevention mechanisms to reduce risks.

c. **Access Controls and Authentication**
   - Multi-factor authentication for user and administrator accounts.
   - Role-based access restrictions to limit data access to authorized personnel only.

d. **Monitoring and Testing**
   - Continuous system monitoring, activity logging, and incident detection.
   - Regular penetration testing, vulnerability assessments, and security audits.

9. YOUR RIGHTS

We respect your rights regarding your personal information. Depending on the laws that apply in your jurisdiction, you may be entitled to exercise one or more of the following rights:

a. **Access and Updates**
   - You may request access to the personal data we hold about you.
   - You may also ask us to correct or update inaccurate or incomplete information.

b. **Deletion and Restriction**
   - You may request the deletion of your personal data where it is no longer required for the purposes for which it was collected.
   - In certain cases, you may also request that we restrict the processing of your information.

c. **Objection to Processing**
   - You have the right to object to the processing of your data for specific purposes, including direct marketing or promotional communications.

d. **Data Portability**
   - Where technically feasible, you may request to receive a copy of your data in a portable format or request that it be transferred to another provider.

e. **Withdrawal of Consent**
   - If processing is based on your consent, you may withdraw that consent at any time without affecting the lawfulness of prior processing.

f. **Complaints**
   - If you believe your rights have been violated, you may have the right to file a complaint with the relevant data protection authority in your jurisdiction.

All requests relating to your rights should be submitted to us at: **[compliance@pinicode.com]**

10. COOKIES AND TRACKING TECHNOLOGIES

Like most digital platforms, Pinicode uses cookies and similar technologies to enhance your experience, improve our Services, and ensure the platform operates effectively. These technologies may collect certain information automatically when you interact with our websites, applications, or APIs.

- **How We Use Cookies**

We use cookies and tracking technologies for the following purposes:

  - **Essential Functionality** – to enable core platform features, such as account login, voucher redemption, and secure session management.
  - **Performance and Analytics** – to monitor traffic, measure usage trends, and improve usability and reliability of our Services.
  - **Personalization and Marketing** – to deliver relevant content, offers, and promotions tailored to your preferences (if you have not opted out).

- **Managing Cookies**

You can manage or disable cookies through your browser or device settings. Please note that some features of the platform may not function properly if cookies are disabled or restricted.

11. ADDITIONAL TERMS FOR RESELLERS AND DISTRIBUTORS

Pinicode works with authorized resellers and distributors who play a role in promoting, selling, and distributing our digital vouchers and related services. To ensure transparency, compliance, and protection of personal data, the following provisions apply specifically to Resellers:

a. **Data Handling Responsibilities**

  - Resellers may collect and process limited personal and business data (such as contact details or transactional information) solely for the purpose of facilitating voucher sales and distribution.
  - Resellers must ensure that any personal data shared with Pinicode is accurate, complete, and collected in compliance with applicable laws, including data protection and consumer protection regulations.
  - Resellers are strictly prohibited from selling, renting, or otherwise disclosing customer data for purposes outside the scope of Pinicode Services.

b. Compliance with Privacy and Security Standards

- Resellers are required to comply with the principles outlined in this Privacy Policy, as well as with all applicable data protection, anti-money laundering (AML), and counter-terrorist financing (CFT) obligations.
- Resellers must implement appropriate technical and organizational measures to protect customer information against unauthorized access, disclosure, or misuse.

c. Role as Independent Data Controllers or Processors

- In most cases, Resellers act as independent data controllers for data they collect directly from their customers. Pinicode acts as the data controller only for data shared with or processed through our platform.
- Where Resellers act as data processors on behalf of Pinicode, they are required to enter into written agreements that ensure compliance with applicable data protection laws, including obligations related to confidentiality, security, and lawful processing.

d. Accountability and Liability

- Resellers are responsible for obtaining all necessary consents from their customers prior to sharing data with Pinicode.
- Any breach of data protection obligations, including unauthorized disclosure or misuse of personal data, will be the sole responsibility of the Reseller, unless directly caused by Pinicode's systems or actions.
- Pinicode reserves the right to suspend or terminate partnerships with Resellers who fail to meet these standards.

12. ELIGIBILITY AND AGE RESTRICTIONS

The Pinicode Services are intended for use only by individuals who are 18 years of age or older. We do not knowingly collect or process personal data from anyone under the age of 18.

If we become aware that we have inadvertently collected personal information from a minor, we will take immediate steps to delete such data from our systems.

13. CHANGES TO THIS POLICY

We may revise or update this Privacy Policy periodically to reflect changes in our business practices, technological developments, or legal and regulatory requirements.

Any updates will be posted on our official website, and the “Last Updated” date at the top of this document will be amended accordingly. Where appropriate, and if the changes are material, we may also notify you directly via email or through in-platform alerts.

We encourage you to review this Privacy Policy regularly to stay informed about how we protect and handle your information.

14. CONTACT US

If you have any questions, concerns, or requests relating to this Privacy Policy or the way we handle your information, please contact us using the details below:

Pinicode – Compliance & Data Protection
Email: compliance@pinicode.com

We will review and respond to all legitimate requests in a timely manner. Depending on the nature of your inquiry, we may ask for additional information to verify your identity before processing your request.