Privacy Policy

Last Updated: March 20, 2025

At Basal Pay, we are committed to safeguarding your privacy while delivering innovative payment solutions for international travelers in Viet Nam through QR code transactions. This Privacy Policy outlines how we collect, use, disclose, and protect your personal information when you engage with our services, including our mobile application and related platforms (collectively, "Services"). By using our Services, you consent to the practices described herein. This policy complies with applicable laws, including the General Data Protection Regulation (GDPR), Gramm-Leach-Bliley Act (GLBA), Personal Data (Privacy) Ordinance (PDPO), and local regulations in Viet Nam, with a strong emphasis on Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance.

---

1. Information We Collect

We collect various categories of information to deliver our Services and meet legal obligations:

- **Personal Identification Information**: Full name, email address, phone number, date of birth, nationality, and identity verification documents (e.g., passport, driver's license, or government-issued ID). These are collected during account registration to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, ensuring we verify your identity and prevent illicit activities.
- **Financial Information**: Transaction histories (including timestamps, amounts, and recipient details), and payment metadata required to process QR code payments and monitor blockchain activity for AML/CFT purposes.
- **Technical Data**: IP addresses, browser type, operating system details, and application usage logs. These help us secure your account, detect suspicious activity, and optimize performance.
- **Usage Data**: Details of your interactions with our Services, such as transaction frequency, merchant locations, and app navigation patterns, used to enhance user experience and identify potential risks.

- **Aggregate or Anonymized Data**: Non-identifiable data derived from your usage, such as statistical trends, for analytics and service improvements.

We collect this information when you register an account, initiate transactions, contact support, respond to KYC requests, or interact with our website or app.

---

2. How We Use Your Information

We process your information for the following purposes:

- **Service Delivery**: To facilitate payments via QR codes, verify transactions, and ensure interoperability with merchant systems across Viet Nam. This includes real-time processing and confirmation of payments.
- **Legal Compliance, Including KYC/AML/CFT**:
    - **Know Your Customer (KYC)**: We use your personal identification information to verify your identity during onboarding and periodically thereafter, as required by financial regulations in Viet Nam, the EU, and the U.S. This helps us prevent identity theft and unauthorized account use.
    - **Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)**: We analyze financial and technical data (e.g., wallet addresses, transaction patterns) to detect and prevent money laundering, terrorist financing, or other illegal activities. This includes monitoring for unusual transaction volumes, high-risk jurisdictions, or connections to sanctioned entities, in line with guidelines from the Financial Action Task Force (FATF) and local regulators like the Monetary Authority of Singapore (MAS).
    - We may flag, freeze, or report transactions to authorities if suspicious activity is detected, as mandated by law.
- **Security**: To protect your account and our platform from fraud, cyberattacks, or unauthorized access, leveraging technical data and real-time monitoring tools.
- **Improvement**: To analyze usage patterns, troubleshoot issues, and enhance our app's functionality, user interface, and customer support processes.

- **Communication**: To send transactional notifications (e.g., payment confirmations), service updates, and, with your explicit consent, promotional materials about new features, merchants, or stablecoin options.

We may use anonymized data for statistical analysis, research, or to develop new features without identifying you personally.

---

3. Disclosure of Your Information

We may share your information with the following entities under strict conditions to operate our Services effectively:

- **Affiliated Companies**: Subsidiaries or partners within Basal Pay to ensure consistent service delivery across our network.
- **Third-Party Service Providers**: We collaborate with trusted third parties to support our QR code payment platform, with a focus on KYC/AML/CFT compliance and operational efficiency:
    - **Analytics and KYC Providers**: To perform identity verification (KYC) and analyze transactions for AML/CFT compliance. These providers receive personal identification information (e.g., name, ID documents) and financial data (e.g., wallet addresses, transaction histories) to screen against sanctions lists, monitor for suspicious patterns, and ensure regulatory adherence.
    - **Payment Processors**: To process transactions and enable QR code payments at Viet Nam merchants. They receive transaction details (e.g., amount, addresses) to facilitate payments and settlements.
    - **Merchants**: Viet Nam merchants receive minimal data (e.g., transaction amount, unique transaction ID) to confirm payment completion via QR codes.
    - **Cloud Hosting and IT Services**: To securely store and process your data, potentially accessing technical data (e.g., IP addresses, device IDs) to maintain our infrastructure and support AML/CFT monitoring systems.

    - **Analytics Providers**: To analyze usage patterns and improve our Services, typically using anonymized or aggregated data unless required for security or compliance purposes.
    - **Marketing and Advertising Partners**: With your explicit consent, limited data (e.g., email address) may be shared to deliver personalized promotions via regional or global platforms.
      All third-party providers are carefully vetted, bound by confidentiality agreements, and required to comply with applicable data protection laws. We conduct regular audits to ensure their adherence to these standards. For an updated list of current third-party service providers, contact [support@basalpay.com].
- **Regulatory Authorities**: We share data when required by law, court orders, or to cooperate with fraud prevention agencies in jurisdictions like Singapore, Thailand, Vietnam, ASEAN, the EU, or the U.S. For AML/CFT purposes, this may include submitting Suspicious Activity Reports (SARs) to regulators, disclosing personal and financial information (e.g., ID details, transaction records) to meet tax, AML, or sanctions obligations.
- **Consent-Based Sharing**: With your explicit permission, we may share data with additional third parties, such as loyalty program partners or other authorized service providers.

International Transfers: Data may be transferred internationally (e.g., to the United States, EU, or Hong Kong) for processing by these third parties. We ensure compliance with GDPR through Standard Contractual Clauses (SCCs), encryption, and other safeguards for cross-border transfers.

Non-Affiliated Third Parties: We do not share your account numbers, wallet addresses, or personal data with non-affiliated third parties for marketing purposes without your explicit consent. You may opt out of non-essential data sharing at any time by contacting [support@basalpay.com].

---

4. Security Measures

We implement robust security practices to protect your data, critical for KYC/AML/CFT compliance:

- **Encryption**: All stored data is encrypted using Chacha20 Poly1305, and data in transit uses Transport Layer Security (TLS) protocols to prevent interception.
- **Authentication**: Two-factor authentication (2FA) is mandatory for account access and high-value transactions, reducing the risk of unauthorized use.
- **Monitoring**: Real-time transaction monitoring systems analyze patterns to detect suspicious activities related to AML/CFT, supported by quarterly security audits conducted by independent experts.
- **Physical Security**: Our servers and backups are housed in secure facilities with restricted access to prevent physical breaches.

Despite these measures, no system is entirely immune to breaches. In case of a significant data incident impacting AML/CFT data, we will notify you and relevant authorities promptly, as required by law.

---

5. How We Deal With Suspicious Funds

At Basal Pay, we prioritize the security and integrity of our platform by proactively identifying and managing suspicious funds to protect our users and comply with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) regulations. We leverage advanced technology from Cube3.AI, a leading real-time fraud detection platform, to assess the risk of cryptocurrency transactions and wallets involved in our QR code payment system. Below is our approach to handling funds that may pose a risk:

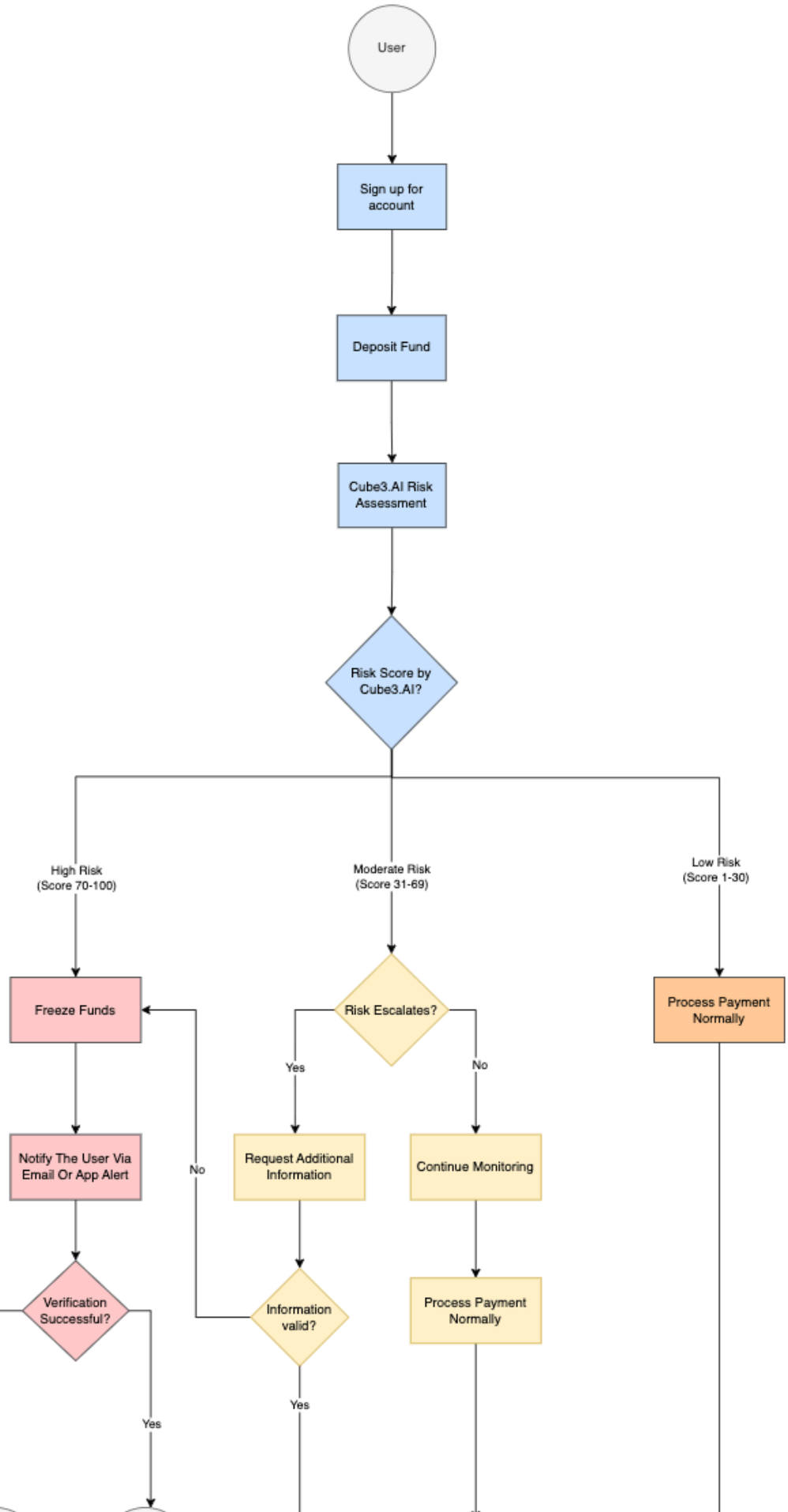
- **Risk Assessment with Cube3.AI**:
    - Cube3.AI provides us with real-time risk scores for every transaction processed through our platform. These scores are generated using proprietary AI models that analyze blockchain data (e.g., transaction history, wallet connections) and Web2 data (e.g., social media chatter, dark web activity) to detect potential fraud, money laundering, or terrorist financing risks.
    - Risk scores range from 1 (low risk) to 100 (high risk), with specific thresholds triggering automated actions to ensure swift response.
- **Action Based on Risk Scores**:

    - **Low Risk (Score 1-30)**: Transactions and wallets with low risk scores proceed normally without interruption, ensuring a seamless payment experience for legitimate users.
    - **Moderate Risk (Score 31-69)**: Transactions or wallets with moderate risk scores are flagged for additional monitoring. We observe patterns and activities over time to assess potential risks without imposing immediate restrictions. No funds are held at this stage; instead, we increase scrutiny and may request voluntary clarification from the user (e.g., additional KYC documents) if patterns escalate. If the provided information is invalid or if the risk escalates further, the transaction or wallet will be reclassified as High Risk (Score 70-100) and subject to the corresponding actions, such as freezing funds and further investigation. This approach ensures minimal disruption for legitimate users while maintaining vigilance against potential threats."
    - **High Risk (Score 70-100)**: Transactions identified as high risk are subject to immediate action, including:
        - **Freezing Funds**: We temporarily freeze the associated funds to prevent potential misuse.
        - **User Notification**: We notify the user via email or app alert, explaining the issue and requesting clarification or additional documentation.
        - **Reporting**: If the risk is confirmed (e.g., linked to sanctioned entities or known fraud), we file Suspicious Activity Reports (SARs) with relevant authorities, such as the Monetary Authority of Singapore (MAS) or Financial Action Task Force (FATF)-aligned bodies, and may permanently lock the user's account & fund, also block the wallet from our platform.
- **Preventive Measures**:
    - Using Cube3.AI's proactive alerts, we block suspicious transactions before they are completed on the blockchain, minimizing the risk of illicit funds entering our ecosystem. For example, if a wallet is flagged for connections to phishing scams or rug pulls, we halt QR code payments involving that wallet instantly.
    - We maintain an internal watchlist of high-risk wallets and entities, updated in real-time by Cube3.AI's data, to prevent future interactions.

- **User Cooperation and Resolution**:
    - If your transaction or wallet is flagged, you will be contacted at [support@basalpay.com] with clear instructions to resolve the issue. Funds are released promptly once compliance is verified, ensuring minimal disruption for legitimate users.
    - In cases where funds are deemed unrecoverable due to legal restrictions, we work with authorities to ensure proper handling while keeping you informed.
- **Continuous Improvement**:
    - We regularly review Cube3.AI's risk scoring methodology and adjust our thresholds in response to emerging fraud patterns, regulatory updates, or technological advancements. This ensures our approach remains robust and adaptive.

This process underscores our commitment to safeguarding your funds and maintaining a trusted payment platform for international travelers in Southeast Asia. For more details, visit [basalpay.com/security].

Cube3.AI-Powered Suspicious Funds Handling Process


User
Sign up for account
Deposit Fund
Cube3.AI Risk Assessment
Risk Score by Cube3.AI?
High Risk (Score 70-100)
Moderate Risk (Score 31-69)
Low Risk (Score 1-30)
Freeze Funds
Risk Escalates?
Process Payment Normally
Yes
No
Notify The User Via Email Or App Alert
Request Additional Information
Continue Monitoring
No
Verification Successful?
Information valid?
Process Payment Normally
Yes
No
Yes

---

5. Retention of Your Information

We retain your personal data only as long as necessary:

- **Active Use**: Data is kept while your account remains active to ensure uninterrupted service and ongoing KYC/AML monitoring.
- **Post-Termination**: After account deactivation, we retain data for up to 5 years to comply with legal obligations (e.g., AML/CFT record-keeping requirements under FATF standards, tax laws) or resolve disputes, unless a longer period is mandated by specific jurisdictions.
- **Deletion**: Post-retention, data is securely deleted or anonymized. You may request earlier deletion where no legal obligation exists, though AML/CFT records may be exempt.

---

6. Your Rights

You have extensive rights over your personal data, balanced with our legal obligations:

- **Access**: Request a copy of your data, including KYC/AML records, in a machine-readable format.
- **Rectification**: Correct inaccurate or incomplete information, such as outdated ID details.
- **Erasure**: Request deletion of your data, subject to AML/CFT retention requirements.
- **Portability**: Obtain your data for transfer to another service, excluding certain compliance-related records.
- **Objection**: Oppose automated processing or marketing communications, though AML/CFT monitoring may continue as required by law.
- **Withdrawal of Consent**: Revoke consent at any time, though this may limit service access or trigger account closure if KYC/AML obligations cannot be met.

To exercise these rights, contact our Data Protection Officer (DPO) at [support@basalpay.com]. We will respond within 30 days, per GDPR standards, unless delayed by legal investigations.

---

7. Marketing Communications

We may send you promotional messages about new merchants, or app features if you opt in during registration or later. To unsubscribe, email [support@basalpay.com] or use the “unsubscribe” link in our communications.

---

8. Legal Compliance

We adhere to a robust framework of laws, with a focus on KYC/AML/CFT:

- **GDPR (EU)**: Ensures lawful processing, transparency, and data rights for European users.
- **GLBA (USA)**: Protects nonpublic personal information (NPI) for U.S. customers.
- **PDPO (Hong Kong)**: Aligns with local privacy standards if applicable.
- **Southeast Asia Laws**: Complies with regulations in countries like Singapore (MAS guidelines), Vietnam,... including AML/CFT requirements.
- **FATF Recommendations**: Guides our global AML/CFT practices, ensuring we combat money laundering and terrorist financing effectively.

Our legal basis for processing includes your consent, contractual necessity (e.g., payment processing), and compliance with legal obligations.

---

9. International Data Transfers

As a global service, your data may be transferred to jurisdictions outside your residence (e.g., servers in the U.S. or EU). We use SCCs, encryption, and contractual safeguards to ensure equivalent protection, meeting GDPR and other international standards.

---

10. Cookie Usage

When you access our website or use our Services, we may use cookies and similar technologies to improve your experience and ensure the security of your account.

Cookies are small data files that your browser saves on your device (such as your computer or smartphone) when you visit our site. These cookies help us recognize you as a user, understand how you interact with our Services, and provide a more personalized experience. They also assist us in maintaining the security of your account by detecting irregular or suspicious activities, such as potential fraud, and ensuring compliance with our Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) program.

We use cookies for several purposes, including enabling essential functionalities (like logging in and processing payments), analyzing usage patterns to enhance our platform, and, with your consent, delivering personalized marketing content. Some cookies are temporary and expire when you close your browser, while others may remain on your device for a longer period until they expire or you delete them.

You can choose to disable cookies through your browser settings, but please note that doing so may affect the functionality of our Services or your overall user experience. For example, disabling cookies might prevent you from logging in or completing QR code payments smoothly. Additionally, some browsers offer a "Do Not Track" (DNT) feature to signal that you do not want your online activities tracked. At this time, our Services do not respond to DNT signals, but you can still manage your cookie preferences directly via your browser.

For more information about how we handle your data, please refer to the other sections of this Privacy Policy or contact us at [support@basalpay.com].

---

11. Updates to This Policy

We may revise this policy to reflect legal, operational, or technological changes. Updates will be posted at [basalpay.com/privacy] and, if significant, notified via email or app alerts. Continued use of our Services after updates implies acceptance of the revised terms.

---

12. Contact Us

For questions, concerns, or to exercise your rights, reach out to:

- **General Inquiries**: [support@basalpay.com]
- **Privacy Requests**: [support@basalpay.com]
- **Data Protection Officer**: [DPO Name], [support@basalpay.com]
- **Website**: [basalpay.com]

New customers may limit data sharing with non-affiliated third parties within 30 days of receiving this notice by contacting us.

---

13. Additional Notices

- **Annual Notice**: We provide this policy annually to active customers via email or app, as required by GLBA.
- **Opt-Out**: You may opt out of non-essential data sharing with unaffiliated third parties at any time.
- **Children's Privacy**: Our Services are not intended for individuals under 18. We do not knowingly collect data from minors.