

Pay2Crypto Privacy Policy

Effective Date: July 29, 2026

1. Introduction

Pay2Crypto ("Pay2Crypto," "we," "our," or "us") is committed to protecting your privacy and handling personal information responsibly.

This Privacy Policy explains how we collect, use, disclose, store, and protect information when you access or use the Pay2Crypto website, merchant dashboard, APIs, sandbox environment, white-label services, plugins, integrations, documentation, and related services (collectively, the "Services").

Pay2Crypto is a **non-custodial cryptocurrency payment gateway and SaaS payment detection platform**. We enable businesses and developers to detect blockchain payments made directly to wallet addresses that they own and control.

We do not hold, receive, or control cryptocurrency funds.

We never request, collect, access, or store wallet private keys or recovery phrases.

By using our Services, you acknowledge that you have read and understood this Privacy Policy.

2. Scope of this Policy

This Privacy Policy applies to:

- Visitors to our website.
- Merchant account holders.
- Developers using our APIs.
- Users of our sandbox environment.
- Users of our plugins and integrations.
- Individuals who communicate with us for support or business purposes.

This Privacy Policy does not apply to third-party websites, wallets, exchanges, payment providers, blockchain explorers, or other services that are not operated by Pay2Crypto.

3. Information We Collect

We collect only the information reasonably necessary to provide, secure, maintain, and improve our Services.

3.1 Account Information

When you create an account, we may collect:

- Name
- Business name
- Email address
- Password (stored in encrypted or hashed form)
- Country or region
- Account preferences
- Subscription information

We do **not** require identity verification (KYC) to create a standard merchant account unless required by applicable law or for specific enterprise services.

3.2 Wallet Information

To provide payment detection services, we collect:

- Public cryptocurrency wallet addresses
- Wallet labels or nicknames
- Blockchain network selection
- Wallet configuration settings

Public wallet addresses are not private keys and cannot be used to access cryptocurrency.

We never request or store:

- Private keys
 - Seed phrases
 - Recovery phrases
 - Wallet passwords
 - Hardware wallet credentials
-

3.3 Payment Information

When payment requests are created, we may process information including:

- Payment identifiers
- Invoice numbers
- Merchant reference numbers
- Payment amount
- Supported cryptocurrency or token
- Blockchain network

- Assigned wallet address
- Payment status
- Blockchain transaction hash
- Block confirmation information
- Timestamp information
- Payment expiration information

Because blockchain networks are public, some transaction information may already be publicly available on the relevant blockchain.

3.4 API Information

When you use our APIs, we may collect:

- API key identifiers
- API usage statistics
- Request timestamps
- Response status codes
- Rate limit information
- Technical diagnostics
- Error logs

We do not intentionally collect the content of your applications beyond what is necessary to process API requests.

3.5 Technical Information

When you use the Services, we may automatically collect technical information such as:

- IP address
- Browser type
- Device information
- Operating system
- Language settings
- Time zone
- Referring URLs
- Session identifiers
- Usage statistics
- Error reports
- Security logs

This information helps us secure and improve the Services.

3.6 Support Communications

If you contact us, we may collect:

- Your name
 - Email address
 - Company information
 - Support requests
 - Attachments you voluntarily provide
 - Correspondence history
-

4. Information We Do Not Collect

Pay2Crypto intentionally does **not** collect or store:

- Cryptocurrency private keys
- Recovery phrases
- Seed phrases
- Wallet passwords
- Access to your wallets
- Cryptocurrency custody information
- Biometric information
- Government-issued identification for standard merchant registration
- Cryptocurrency controlled by your wallet

Because we never have access to your private keys, we cannot access, transfer, freeze, recover, or manage your cryptocurrency.

5. How We Use Information

We use information to:

- Provide the Services.
- Detect blockchain payments.
- Generate invoices.
- Operate the merchant dashboard.
- Deliver payment notifications.
- Authenticate users.
- Secure user accounts.
- Prevent fraud and abuse.
- Monitor system performance.
- Improve our Services.
- Respond to support requests.

- Communicate product updates.
- Comply with legal obligations.
- Enforce our Terms and policies.

We do not use personal information to make automated decisions that produce legal or similarly significant effects without appropriate safeguards where required by law.

6. Legal Bases for Processing

Where applicable under relevant privacy laws, we process information based on one or more of the following lawful grounds:

- Performance of a contract.
 - Compliance with legal obligations.
 - Legitimate business interests.
 - Your consent, where required.
 - Protection of our legal rights.
-

7. Blockchain Data

Blockchain networks are public by design.

Transactions recorded on supported blockchain networks may include publicly visible information such as:

- Wallet addresses
- Transaction hashes
- Token amounts
- Confirmation data
- Block numbers
- Transaction timestamps

Pay2Crypto cannot remove, modify, or erase information recorded on a blockchain.

You acknowledge that blockchain transactions may remain publicly accessible indefinitely.

8. Cookies and Similar Technologies

We use cookies and similar technologies to:

- Maintain user sessions.
- Authenticate users.

- Remember preferences.
- Improve website performance.
- Analyze usage.
- Detect security threats.

Additional information regarding cookies is available in our Cookie Policy.

9. Information Sharing

We do not sell personal information.

We may disclose information in limited circumstances including:

9.1 Service Providers

We may share information with trusted service providers who assist with:

- Cloud infrastructure
- Website hosting
- Email delivery
- Customer support
- Security monitoring
- Analytics
- Error reporting
- Payment processing for Pay2Crypto subscription fees

These providers may access information only as necessary to perform services on our behalf and are expected to protect it appropriately.

9.2 Legal Compliance

We may disclose information where required to:

- Comply with applicable law.
 - Respond to lawful governmental requests.
 - Enforce our Terms.
 - Protect our legal rights.
 - Protect users.
 - Prevent fraud.
 - Investigate criminal activity.
 - Cooperate with regulators or law enforcement where legally required.
-

9.3 Corporate Transactions

If Pay2Crypto undergoes a merger, acquisition, restructuring, financing, or sale of assets, information may be transferred as part of that transaction, subject to applicable law.

10. International Data Transfers

Because Pay2Crypto serves users globally, information may be processed in countries other than your country of residence.

We take reasonable steps to ensure that personal information transferred internationally receives an appropriate level of protection consistent with applicable law.

11. Data Retention

We retain information only for as long as reasonably necessary to:

- Provide the Services.
- Maintain account functionality.
- Meet legal obligations.
- Resolve disputes.
- Enforce agreements.
- Protect security.
- Maintain financial and operational records.

Retention periods may vary depending on the type of information and applicable legal requirements.

When information is no longer required, we will securely delete, anonymize, or otherwise dispose of it where reasonably practicable.

12. Security

We implement reasonable administrative, technical, and organizational safeguards designed to protect information against unauthorized access, disclosure, alteration, or destruction.

These measures may include:

- Encryption in transit
- Password hashing
- Access controls

- Authentication mechanisms
- Network security controls
- Monitoring and logging
- Security testing
- Principle of least privilege

No internet-based service or electronic storage system can be guaranteed to be completely secure.

You are responsible for protecting your account credentials and devices.

13. Your Responsibilities

You are responsible for:

- Maintaining accurate account information.
- Protecting your login credentials.
- Protecting your wallet credentials.
- Securing your devices.
- Configuring wallet addresses correctly.
- Complying with applicable privacy laws affecting your own customers.

Where you collect personal information from your own customers, you are solely responsible for complying with all applicable data protection and privacy obligations.

14. Your Privacy Rights

Depending on your jurisdiction, you may have rights including:

- Access to personal information.
- Correction of inaccurate information.
- Deletion of certain information.
- Restriction of processing.
- Objection to processing.
- Data portability.
- Withdrawal of consent where processing is based on consent.
- Lodging a complaint with an appropriate supervisory authority.

Some rights may be limited where exceptions apply under applicable law.

Requests may be submitted through our official support channels.

15. Children's Privacy

The Services are intended for businesses and developers.

They are not directed to children under the age of eighteen (18), and we do not knowingly collect personal information directly from children.

If we become aware that personal information has been collected from a child in violation of applicable law, we will take reasonable steps to delete that information.

16. Marketing Communications

We may send service-related communications that are necessary for the operation of your account, including:

- Security notifications
- Billing notices
- Service announcements
- Platform updates
- API notices
- Maintenance notifications

Where permitted by law, we may also send marketing communications. You may opt out of marketing emails at any time by using the unsubscribe mechanism provided or by contacting us.

Service-related communications may still be sent where necessary to administer your account.

17. Third-Party Services

Our Services may link to or integrate with third-party services, including:

- Cryptocurrency wallets
- Blockchain explorers
- Cloud providers
- E-commerce platforms
- Payment services for subscription billing
- Analytics providers

We are not responsible for the privacy practices or content of third-party services.

Your use of those services is governed by their respective privacy policies and terms.

18. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our Services, technology, legal requirements, or business practices.

Updated versions become effective upon publication unless otherwise stated.

Your continued use of the Services after an updated Privacy Policy becomes effective constitutes acknowledgment of the revised policy.

19. Governing Law

This Privacy Policy shall be governed by and interpreted in accordance with the laws of the **United Arab Emirates**, except where mandatory data protection laws require otherwise.

20. Contact Us

If you have questions about this Privacy Policy or our privacy practices, please contact Pay2Crypto through the official contact methods made available on our website.

We will make reasonable efforts to respond to privacy-related inquiries in accordance with applicable law.