

PRIVACY POLICY

Last Updated: June 24, 2026

Novawave is a Digital Asset Service Provider (PSAD) registered with the National Commission of Digital Assets (CNAD) under Registration No. PSAD-0079 (20 April 2026), and a Bitcoin Service Provider (PSB) registered under the Bitcoin Law, Registration Code 6697f7c29c3ab49e3172b9f8 (29 July 2024).

This Privacy Policy describes how Novawave S.A. DE C.V., with NIT: 0623-030624-109-2, located at Calle Cuscatlán, Casa #4312, Colonia Escalón, Distrito de San Salvador, San Salvador Centro, San Salvador, El Salvador ("Monesy," "we," "us," or "our") collects, uses, processes, and protects your personal data when you use our website <https://monesy.io> (the "Platform") and any of our services (the "Services").

This Privacy Policy is issued in compliance with El Salvador's Personal Data Protection Law (Decreto Legislativo No. 144), effective November 23, 2024, and other applicable laws of the Republic of El Salvador, which guarantee the right to honor, personal privacy, and personal image.

All capitalized terms not defined in this Privacy Policy have the meanings outlined in our Terms of Service.

IMPORTANT: Please read this Privacy Policy carefully. By using our Platform or Services, you acknowledge that you have read, understood, and agree to be bound by this Privacy Policy.

1. WHAT DATA WE COLLECT

We collect the following information to provide our cryptocurrency exchange services:

- **Identity Information.** We collect identity data to verify who you are, as required by Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations: Name, date of birth, age, nationality, address, residency, ID documents (passport/DUI), photo, tax ID (NIT), Facial photograph (for biometric verification), and Politically Exposed Person (PEP) status.
- **Financial Information:** Bank account details, payment card information, source of funds, income information, and digital wallet information.

NOTE: We never store your bank card's PIN, CVV, CVV2, CAV2, CVC2, or CID codes. These are processed directly by our payment processors and are not retained

by Monesy.

- **Transaction Data.** We record all transaction information for regulatory compliance, dispute resolution, and service provision: Complete details of all transactions you conduct on the Platform, transaction amounts in both fiat currency and cryptocurrency, timestamps and dates, status and confirmations, recipient and sender information for transfers, purposes and descriptions, payment method used for each transaction, transaction fees, and exchange rates applied.
- **Cryptocurrency-Specific Data.** Due to the nature of blockchain technology, we collect and process cryptocurrency-related information: Digital wallet addresses (public keys) associated with your account, Blockchain network addresses for different cryptocurrencies, Transaction hashes (unique identifiers for blockchain transactions), Information about your cryptocurrency holdings, Blockchain transaction confirmations, Gas fees, and network transaction costs.
- **Technical and Usage Data.** We automatically collect technical information when you use our Platform: IP address and geographical location data, Device information (type, model, operating system, unique device identifiers), Browser type, version, and language settings, Time zone settings and access times, Platform usage patterns and navigation paths, Pages visited, features used, and time spent on the Platform, Referring website or application, Data received through cookies, web beacons, and similar technologies, Login history and authentication logs, Error reports and diagnostic data
- **Communications.** We collect information from your communications with us: Email address and phone number, Content of messages you send to our customer support, your requests, complaints, and inquiries, Records of phone calls with customer service (with your consent), Chat transcripts and support ticket information, your feedback, reviews, and survey responses, and correspondence and interaction history with Monesy.

Sensitive Personal Data

Under El Salvador's data protection law, certain categories of personal data are classified as "Sensitive Personal Data" because their improper use could lead to discrimination or seriously affect your rights. We collect the following sensitive data only when strictly necessary and with your express written consent:

- **Biometric Data.** We collect facial biometric data through facial recognition technology for identity verification purposes. This is required to comply with KYC regulations and prevent identity fraud. The biometric data includes facial geometry measurements derived from your photograph.

- **Financial Situation Data.** We collect detailed information about your financial situation, including source of funds, income levels, credit history, and financial capacity. This is required under AML/CFT regulations to assess transaction risk and detect potential money laundering or terrorist financing activities.

Your Rights Regarding Sensitive Data:

You have the RIGHT NOT to provide Sensitive Personal Data. However, refusing to provide this information may prevent us from offering you our Services, as we are legally obligated to collect it for regulatory compliance. Before collecting Sensitive Personal Data, we will:

- Explicitly inform you that the data is classified as sensitive
- Explain why we need this specific data
- Obtain your separate, express written consent
- Inform you of the consequences of not providing the data
- Implement enhanced security measures to protect this data

IMPORTANT: BLOCKCHAIN TRANSACTIONS ARE PUBLIC

Cryptocurrency transactions are permanently recorded on public blockchains. Anyone can see wallet addresses, amounts, and timestamps. While we don't publicly link your identity to your wallet, others may be able to do so through blockchain analysis. We do not control blockchain networks.

2. WHY WE USE YOUR DATA

Under El Salvador's data protection law, we must have a valid legal basis for processing your personal data. We only process your data when we have at least one of the following legal grounds:

2.1 Legal Obligation

We process certain data because we are legally required to do so by El Salvador law and international regulations:

- **Identity Verification and KYC Compliance:**

Legal Requirement: Special Law Against Asset Laundering (Legislative Decree No. 426/2025), National Digital Assets Commission (CNAD) regulations

Data Processed: Identity data, biometric data (facial recognition), government ID documents

Purpose: Verify customer identity, prevent identity fraud, comply with CNAD licensing requirements

Retention: 10 years after account closure (as mandated by law)

- **AML/CFT Monitoring and Reporting:**

Legal Requirement: Special Law Against Asset Laundering (Legislative Decree No. 426/2025), UN Security Council resolutions on terrorist financing, FATF (Financial Action Task Force) recommendations

Data Processed: Financial data, transaction data, source of funds, cryptocurrency transaction records

Purpose: Monitor suspicious transactions, file Suspicious Activity Reports (SARs) with authorities, and prevent money laundering and terrorist financing

Retention: 10 years after transaction (as mandated by law)

- **Regulatory Cooperation:**

Legal Requirement: Obligations to cooperate with law enforcement, judicial orders, and administrative investigations

Data Processed: Any personal data relevant to the investigation or legal proceeding

Purpose: Comply with court orders, respond to lawful government requests, and assist in criminal investigations

2.2 Contract Performance

We process data that is necessary to provide you with the Services you requested and to fulfill our contractual obligations:

- **Service Provision:**

We need your identity data, wallet addresses, and transaction information to execute cryptocurrency buy, sell, and exchange orders you place on the Platform. Without this data, we cannot perform the contract (providing cryptocurrency exchange services).

- **Account Management:**

We process your identity data, contact information, and login credentials to create and maintain your account, provide customer support, and enable you to access your transaction history and account settings.

- **Payment Processing:**

We process your financial data and payment information to accept payments for cryptocurrency purchases and transfer funds for cryptocurrency sales. This includes working with payment processors and financial institutions on your behalf.

2.3 Your Consent

For certain processing activities, we rely on your explicit consent. Your consent must be freely given, specific, informed, express, and individualized:

- **Marketing Communications:**

With your consent, we send you promotional emails, product updates, special offers, and newsletters. You can withdraw this consent at any time by clicking "unsubscribe" in our emails or contacting sp@monesy.io.

- **Optional Features:**

Certain platform features (such as saving payment methods for faster checkout or enabling advanced trading features) require your consent as they involve additional data processing beyond what's strictly necessary for basic service provision.

- **Sensitive Personal Data:**

We obtain your separate written consent before processing Sensitive Personal Data (biometric information, detailed financial situation). This consent is separate from your general agreement to this Privacy Policy.

2.4 Legitimate Interests

We process certain data based on our legitimate business interests, provided these interests do not override your fundamental rights and freedoms:

- **Fraud Prevention and Platform Security:**

We have a legitimate interest in protecting our Platform, users, and business from fraud, unauthorized access, and cyberattacks. This includes processing technical data, IP addresses, device information, and transaction patterns to detect suspicious activity.

- **Service Improvement and Analytics:**

We analyze how users interact with the Platform to improve user experience, fix bugs, develop new features, and optimize performance. This involves processing usage data, technical data, and anonymized transaction patterns.

- **Business Operations:**

We process data necessary for internal business operations, including accounting, auditing, business planning, and managing legal claims or disputes.

- **When We Rely on Legitimate Interests:**

We carefully balance our legitimate interests against your rights. You have the right to object to processing based on legitimate interests. If you object, we will stop processing unless we can demonstrate compelling legitimate grounds that override your interests, or the processing is necessary for legal claims.

3. WHO WE SHARE DATA WITH

We may share your information with:

- **Government authorities:**

- National Digital Assets Commission (CNAD). We report to CNAD regarding our operations, customer due diligence, and transaction monitoring. Data shared includes identity verification records, transaction volumes, and compliance reports.
- State Cybersecurity Agency (ACE). ACE is the supervisory authority for data protection in El Salvador. We cooperate with ACE investigations, provide requested information about our data processing practices, and notify ACE of data breaches within 72 hours.
- Attorney General's Office (Fiscalía General de la República). We respond to lawful requests from the Attorney General's Office in criminal investigations.

This may include providing account information, transaction records, and identity data relevant to investigations of money laundering, fraud, or other criminal activities.

- Law Enforcement Agencies. We comply with valid court orders, search warrants, and subpoenas from law enforcement. Before disclosing data, we verify the legal validity of the request and limit disclosure to what is legally required.
- Other Authorities. We may share information with another authorities as required under applicable laws, including information necessary for tax compliance verification and reporting.
- **Service providers:** Identity verification service, payment processors, cloud storage, cybersecurity services, customer support services, Analytics and Business Intelligence services, and IT support.
- **Financial institutions:** Banks, payment processors, cryptocurrency exchanges, and wallet providers.
- **Business partners:** Companies helping us provide services (all bound by data protection agreements), including professional advisors (lawyers, accountants, auditors) who assist with legal, financial, or regulatory matters, and business associates involved in providing specific features or services on the Platform.
- **Blockchain Networks (Special Case):** When you transact in cryptocurrency, certain information is automatically published to public blockchain networks. This is not a traditional "data sharing" but an inherent feature of blockchain technology. Transaction data is replicated across all nodes and permanently recorded. Anyone can view all transaction data; Monesys has no control over blockchain networks. Blockchain data cannot be edited, deleted, or restricted.
- **Corporate Transactions.** If Monesys is involved in a merger, acquisition, asset sale, or bankruptcy proceeding, your personal data may be transferred to the acquiring entity. The successor entity will be bound by this Privacy Policy unless you consent to a different policy.

This is outside the scope of El Salvador's data protection law because blockchain networks are not "data controllers" under the law. By using cryptocurrency services, you accept that transaction data will be permanently public on blockchain networks.

4. INTERNATIONAL DATA TRANSFERS

Some of our service providers are located outside El Salvador, which means your personal data may be transferred to and processed in other countries. We ensure these transfers comply with El Salvador's data protection law.

4.1 Countries We Transfer Data To

We currently transfer personal data to the following jurisdictions:

United States: Cloud storage providers (Amazon Web Services, Google Cloud), payment processors, identity verification services, cybersecurity tools.

European Union: Cybersecurity service providers, analytics tools, customer support platforms.

Other Locations: Service providers may use data centers in various countries for backup, redundancy, and disaster recovery purposes.

4.2 Legal Safeguards for International Transfers

Under Article 35 of El Salvador's Personal Data Protection Law, international transfers are permitted only when the receiving country offers at minimum the same level of data protection as El Salvador, or when we implement appropriate safeguards:

Standard Contractual Clauses: We use internationally recognized standard contractual clauses (based on EU Standard Contractual Clauses adapted for El Salvador law) with all international service providers. These contracts legally bind recipients to protect your data according to El Salvador's standards.

Adequacy Assessment: We conduct assessments to verify that recipient countries have adequate data protection laws or that our contractual safeguards provide equivalent protection.

Technical and Organizational Measures. International transfers include enhanced security measures:

- End-to-end encryption for data in transit
- Strong encryption for data at rest in foreign data centers
- Pseudonymization where possible
- Access controls limiting who can view transferred data
- Regular audits of international processors

4.3 Central American Economic Integration Exception

Under Article 36 of the law, data transfers within Central American Economic Integration treaties are permitted due to regional integration frameworks. This means transfers to other Central American Integration System (SICA) member countries (Guatemala, Honduras, Nicaragua, Costa Rica, Panama, Belize, Dominican Republic) benefit from simplified procedures, as these countries have adopted reciprocal data protection standards.

4.4 Your Rights Regarding International Transfers

You have the right to:

- Know which specific countries your data is transferred to
- Receive information about safeguards implemented for international transfers
- Object to transfers to specific countries (subject to contractual obligations)
- Request copies of data processing agreements and standard contractual clauses
- Withdraw consent for transfers based on consent (this may limit service availability)

To exercise these rights or request information about international transfers, contact our Data Protection Officer at sp@monesy.io with the subject line "International Data Transfers Inquiry."

4.5 Notification to ACE

We inform the State Cybersecurity Agency (ACE) of our cross-border data flows, including details about recipient countries, data categories transferred, purposes of transfer, and

safeguards implemented. This allows ACE to monitor compliance and intervene if necessary to protect data subjects' rights.

5. YOUR PRIVACY RIGHTS (ARCO-POL)

You have seven rights to control your personal data under El Salvador's Personal Data Protection Law:

RIGHT	WHAT YOU CAN DO	HOW TO USE IT
ACCESS	Get a copy of your data and info about how we use it	Request format: PDF, Excel, JSON. FREE. 20 days.
RECTIFICATION	Correct inaccurate or outdated information	Submit corrections with proof. We block data during review. FREE. 20 days.
CANCELLATION	Delete data when no longer needed	Request deletion. We keep data required by law (10-yr AML). Blockchain data permanent. FREE. 20 days.
OPPOSITION	Stop marketing or object to processing	Marketing stops immediately. Other opposition will be reviewed in 20 days. FREE.
PORTABILITY	Get data in a transferable format	Receive CSV/JSON/XML. We can transfer directly to another provider. FREE. 20 days.
OBLIVION	Remove data from online/search results	We remove from our sites and request search engine de-indexing. FREE. 20 days.
LIMITATION	Restrict processing temporarily	Data stored but not used during accuracy/lawfulness verification. FREE. Immediate.

HOW TO EXERCISE YOUR RIGHTS

Email: sp@monesy.io | **Subject:** "ARCO-POL Request - [Right Name]"

Include: (1) Full name, (2) Contact email/address, (3) Copy of government ID (both sides), (4) Which right you're exercising, (5) Specific data affected (if applicable), (6) Your signature or typed name, (7) Supporting documents (if needed, e.g., updated ID for rectification, power of attorney for representatives, death certificate + heir proof for deceased persons).

Process: We confirm receipt in 5 days → Review in 20 days (up to 40 if complex) → Send decision with reasoning. If denied, we explain why and inform you of complaint rights.

Cost: FREE (except physical shipping/reproduction costs, which you'll be informed of first).

WHEN WE MAY DENY YOUR REQUEST

We can only deny if:

- You can't prove identity

- Data not in our systems
- Would harm third-party rights
- Legal obligation requires retention (10-yr AML)
- Court order restricts access
- Request already fulfilled
- Data anonymized
- Essential for legal claims.

If denied, you can:

- Request clarification
- File a complaint with the State Cybersecurity Agency (ACE): <https://ace.gob.sv>, (503) 7530-6114, contacto@ace.gob.sv
- Pursue legal action.

IMPORTANT: Blockchain transactions are permanent and public. Even if we delete your data, blockchain records cannot be removed.

Deceased Persons: Heirs can exercise rights by providing a death certificate, proof of heir status, and the heir's ID. Same procedures and timelines apply.

QUICK REFERENCE

Contact	sp@monesy.io
Response Time	20 business days (40 if complex)
Cost	FREE (electronic delivery always free)
Marketing Opt-Out	Immediate (click unsubscribe or email us)
Complaint Authority	ACE: https://ace.gob.sv • (503) 7530-6114
Blockchain Data	Cannot be deleted (permanent public record)

6. HOW LONG WE KEEP YOUR DATA

We retain data only as long as necessary:

- **KYC/Identity data:** 10 years after account closure (AML law requirement)
- **Transaction records:** 10 years (regulatory requirement)
- **Financial records:** 10 years (tax and AML law)
- **Customer support:** 5 years
- **Marketing consent:** Until withdrawn or 3 years of inactivity
- **Technical logs:** 2 years
- **Blockchain data:** Permanent (cannot be deleted from public blockchains)

After retention periods expire, we securely delete or anonymize your data unless legally required to keep it longer.

7. HOW WE PROTECT YOUR DATA

We implement strong security measures:

- **Encryption:** AES-256 for stored data, TLS 1.3 for data in transit

- **Access controls:** Multi-factor authentication, role-based access
- **Technical protection:** Firewalls, intrusion detection, regular security updates
- **Physical security:** Restricted facility access, secure document storage
- **Personnel:** Confidentiality agreements, regular security training
- **Audits:** Regular internal and external security audits

Data Breach Notification:

If a security breach occurs, we will notify you, ACE, and the Attorney General within 72 hours, including breach details and steps to protect yourself.

7. CONSENT AND SENSITIVE DATA

Your consent is required for processing personal data. Consent must be FREE (voluntary, no coercion), SPECIFIC (for defined purposes), INFORMED (you know what will happen), EXPRESS (affirmative action required), and INDIVIDUALIZED (each person consents separately).

HOW WE OBTAIN CONSENT

WHEN	WHAT YOU CONSENT TO	HOW
Account Registration	Basic data processing for service provision	Check box after reviewing Privacy Policy & Terms
Biometric/Financial Data	Sensitive data collection (facial recognition, financial info)	Separate written consent form upon verification
Marketing	Promotional emails and communications	Opt-in checkbox (separate from mandatory consents)
Optional Features	Additional processing for saved payments, advanced features	Consent when activating each feature

WITHDRAWING CONSENT

You can withdraw consent anytime.

Marketing: Click 'unsubscribe' in emails (immediate).

Other consents: Email sp@monesy.io with subject 'Consent Withdrawal' (processed within 5 days). Withdrawal stops future processing but doesn't affect past lawful processing.

If consent was the only legal basis, we must stop processing. Withdrawing KYC consent means we cannot provide services. We may deny withdrawal only if processing is based on legal obligation (not consent) or necessary for contract performance.

SENSITIVE PERSONAL DATA

Sensitive data receives enhanced protection. Under El Salvador law, this includes: religious beliefs, ethnic origin, political affiliation, union membership, sexual orientation, health information, biometric data, genetic data, family situation, personal habits.

What We Collect:

TYPE	PURPOSE	LEGAL BASIS	RETENTION	SECURITY
------	---------	-------------	-----------	----------

Biometric Data (facial recognition)	KYC identity verification	Legal obligation (AML law) + your written consent	10 years after account closure	Encrypted storage, compliance team only, regular audits
Financial Situation	AML/CFT risk assessment, transaction monitoring	Legal obligation (AML law) + your written consent	10 years after account closure	Separate encrypted databases, enhanced encryption, strict access controls

Your Right to Refuse:

You can refuse to provide sensitive data. Consequences: Without biometric data, we cannot verify your identity per KYC regulations—account remains inactive, no cryptocurrency services. Without financial data, we cannot complete required AML/CFT assessment—account severely limited or closed.

Special Consent Process for Sensitive Data:

Before collecting sensitive data, we: (1) Present separate consent form labeled 'sensitive', (2) Explain exactly why necessary, (3) Describe enhanced security measures, (4) Inform of your right to refuse and consequences, (5) Obtain WRITTEN consent with electronic signature and timestamp, (6) Provide copy for your records.

Enhanced Security Measures:

- Separate encrypted databases
- Access logs tracking every viewer
- Senior compliance officers only
- Separate encryption keys
- More frequent audits
- Automatic deletion when retention expires.

WHEN CONSENT IS NOT REQUIRED

We can process data without consent if:

- Data is publicly accessible (NOT sensitive data)
- Medical emergency or vital interests protection
- You're unable to consent
- Emergency situation
- Data is anonymized
- You're reported missing
- Necessary for contractual/professional relationship
- You made data manifestly public
- Historical/scientific/statistical research with pseudonymization.

Even without consent, we comply with all other data protection principles (security, accuracy, purpose limitation).

8. COOKIES AND TRACKING

We use cookies and similar technologies for:

- **Essential functions:** Login, security, fraud prevention (cannot be disabled)
- **Analytics:** Understanding platform usage, improving user experience
- **Marketing:** Personalized content, ad effectiveness (can be disabled)

You can control cookies through your browser settings. Disabling non-essential cookies may affect platform functionality.

9. AGE RESTRICTION

Our services are only for people 18 years and older. We do not knowingly collect data from minors. If we learn we have collected a minor's data, we will delete it immediately.

Contact sp@monesy.io if you believe a minor provided data.

10. COMPLAINTS AND ENFORCEMENT

If you believe your privacy rights were violated:

File a complaint with:

State Cybersecurity Agency (ACE)

- Website: <https://ace.gob.sv/contacto.php>
- Phone: (503) 7530-6114
- Email: contacto@ace.gob.sv

You can also file a lawsuit in the El Salvador courts or a criminal complaint with the Attorney General.

11. POLICY UPDATES

We may update this Privacy Policy to reflect changes in our practices, laws, or services. Material changes will be notified via email and posted on our website 30 days before taking effect. Continued use after changes means you accept the updated policy.

12. CONTACT INFORMATION

Data Protection Officer (Privacy Questions & Rights Requests):

Email: sp@monesy.io

Response time: 20 business days

General Inquiries:

Email: legal@monesy.io

Regulatory Authority:

State Cybersecurity Agency (ACE)

<https://ace.gob.sv>