FINZY

PRIVACY POLICY

Personal Data Processing Policy

Finzy Sociedad de Responsabilidad Limitada

Legal entity No. 3-102-921514, registered in the National Registry of the Republic of Costa Rica on 19 December 2024, legalisation number 4062001335301

Registered office: San José, Montes de Oca, San Pedro, Los Yoses, Avenidas 8 y 10, Calle 39, LY Center, Costa Rica

Service: the Finzy platform (custodial crypto wallet, partner storefront, crypto-to-crypto exchange) — web (desktop/mobile), Telegram Mini App

Version 2.0 | Effective date: 30 March 2026

---

1. General Provisions

1.1. This Personal Data Processing Policy (the "Policy") governs the collection, storage, use, transfer, and protection of personal data of users (the "User", "you") of the Finzy service (the "Service", "Finzy", "we"), operated by Finzy Sociedad de Responsabilidad Limitada (the "Company").

1.2. This Policy has been prepared in accordance with Law No. 8968 of the Republic of Costa Rica "On the Protection of Individuals with Regard to the Processing of Their Personal Data" (Ley N.° 8968) and its implementing Regulation (Decreto Ejecutivo N.° 37554-JP), and, to the extent not inconsistent with the law of Costa Rica as the principal applicable law, having regard to the requirements of the legislation of the CIS countries from which Users of the Service predominantly originate (Federal Law of the Russian Federation No. 152-FZ, Law of the Republic of Belarus No. 99-Z, and similar acts of other CIS countries).

1.3. The Service is not intended for citizens and residents of the United States, the European Union, the European Economic Area, the United Kingdom, or jurisdictions included in the sanctions and "black" lists of the FATF, OFAC, HM Treasury, the EU, and other similar bodies. The Company does not provide services to such categories of persons and does not adapt this Policy to their legislation (GDPR, CCPA, etc.), except where certain principles of such regimes have been voluntarily incorporated as best practice.

1.4. Use of the Service constitutes the User's unconditional agreement to the terms of this Policy. If the User does not agree with any term, they must discontinue use of the Service.

1.5. This Policy is an integral part of the Finzy Terms of Service ("ToS") and applies together with it, as well as with the separate Cookie Policy, which is published as a stand-alone document.

1.6. In the event of a conflict between this Policy and the ToS: on matters relating to the collection, processing, storage, transfer, and protection of personal data, and to the exercise of data subjects' rights, the provisions of this Policy shall prevail; on matters of the parties' liability, limitation of liability, dispute resolution procedure, and the law applicable to the contractual relationship as a whole, the provisions of the ToS shall prevail, except as expressly provided in Section 14 of this Policy.

2. Terms and Definitions

Personal Data — any information relating to an identified or identifiable natural person (a User or other data subject).

Controller (Responsable del Tratamiento) — Finzy S.R.L., which determines the purposes and means of processing personal data.

Processor (Encargado del Tratamiento) — a third party that processes data on behalf of and in the interests of the Company (verification and transaction monitoring providers, hosting providers, payment and communication services, etc.).

Data Subject (Titular) — a natural person whose personal data is processed, including a User, as well as third parties whose data is processed in connection with a User's use of the Service (in particular, address book contacts and transfer recipients not registered with the Service).

Data Processing — any action or set of actions performed with personal data: collection, recording, storage, modification, use, transfer, blocking, deletion.

KYC (Know Your Customer) — the procedure for identifying and verifying a User's identity.

KYT (Know Your Transaction) — the procedure for monitoring and analysing transactions for indicators of money laundering, terrorist financing, and other unlawful activity.

AML/CFT — anti-money laundering and countering the financing of terrorism.

Verification and Monitoring Service Provider — any third party engaged by the Company on a permanent or temporary basis for KYC and/or KYT purposes, the composition and list of which may change in the manner provided for in clause 5.3 of this Policy.

3. Categories of Personal Data Collected

The Company collects and processes the following categories of data, limited to what is minimally necessary for the purposes set out in Section 4:

3.1. Identification and Verification Data (KYC)

Surname, first name, patronymic (including those obtained automatically through OAuth authorisation methods — Telegram ID, VK ID, Apple ID, Google, Yandex ID, MAX); date and place of birth; citizenship; identity document data (type, series, number, date of issue, issuing authority, validity period, scanned copies/photographs of the document); a photograph of the face (selfie) for identity verification and comparison with the document; registered/actual residential address; taxpayer identification number or equivalent (where applicable); information on PEP (politically exposed person) status and beneficial ownership (for corporate clients, where applicable).

3.2. Contact Data

Mobile phone number; email address; messenger identifiers (Telegram username/ID and others obtained upon authorisation).

3.3. Account and Authorisation Data

A unique user identifier in the Finzy system; identifiers received from OAuth authorisation providers (Telegram ID, VK ID, Apple ID, Google ID, Yandex ID, MAX ID); hashed passwords (for email/phone authorisation); hashed session JWT tokens; one-time confirmation codes sent to the User's email address and phone number through communication and mailing service providers engaged by the Company (see Section 6); login and authorisation attempt history.

3.4. Financial and Transaction Data

History of the User's operations within the Service (deposits, withdrawals, crypto-to-crypto exchange, interaction with storefront partner services); blockchain wallet addresses from which funds were received and to which they were withdrawn; transaction hashes; amounts, currencies, and timing of operations; scoring request data, including addresses, transaction hashes, and amounts sent to transaction monitoring (KYT) service providers for the purposes set out in Section 4; data received from storefront partners when transactions are carried out through them.

3.5. Technical Data

IP address; unique device fingerprint; User-Agent, browser type and version, operating system, platform; session data; approximate geolocation via GeoIP (country, city — without precise coordinates unless the User has separately and knowingly provided precise geolocation); device identifiers (for mobile applications and the Telegram Mini App); API key usage logs and system action audit logs; client application version data.

3.6. Data Provided Subject to Separate User Consent

Device address book — phone numbers and email addresses from the User's imported address book, including contacts of persons not registered with Finzy — collected only where the User expressly grants access to contacts for the "transfer to contacts" feature; the phone number or messenger identifier of a P2P transfer recipient specified by the sending User before the recipient registers with the Service.

3.7. Data Received from Third Parties

Verification status and risk-scoring result data received from verification and transaction monitoring service providers; sanctions, PEP, and AML screening data obtained from public and commercial databases (OFAC, HM Treasury, EU sanctions lists, FATF); data transferred by storefront partners in connection with the use of their products through Finzy.

4. Purposes of Personal Data Processing

The specific purposes for which personal data is processed, the corresponding categories of data, and the legal basis for each purpose are set out in the table in Appendix No. 1 to this Policy.

The Company does not process personal data for purposes other than those set out above without obtaining the User's additional consent, except in cases expressly provided for by law. Each processing purpose is applied only to the minimum volume of data necessary to achieve it.

5. Automated Processing and Profiling

5.1. In order to prevent fraud, money laundering, and terrorist financing, the Company applies automated scoring and transaction monitoring systems, which may temporarily suspend operations, request additional verification, or restrict account functionality pending completion of a check.

5.2. Decisions made in an automated manner that entail legally significant consequences for the User (in particular, freezing of funds, refusal to carry out an operation, or restriction of access to the account) are subject to the right to human review at the User's request, submitted in the manner provided for in Section 13. The Company considers such a request on a priority basis and within the period established by clause 9.2.

5.3. The Company may independently determine, engage, replace, and terminate cooperation with one or more identity verification (KYC) and transaction monitoring (KYT) service providers without the need to amend the main text of this Policy. The current list of such providers, the jurisdiction of their activity, and the categories of data transferred to them are published in Appendix No. 1 to this Policy and/or in the corresponding section of the Service interface and are kept up to date. Engaging, replacing, or terminating cooperation with a provider is not considered an amendment to the Policy requiring separate notification of Users under Section 12, provided that the categories of data and the purposes of their processing remain within the scope described in Sections 3 and 4.

6. Disclosure of Data to Third Parties

6.1. The Company discloses personal data to the following categories of third parties, strictly to the extent necessary for them to perform their functions:

- Third-party authorisation service providers (in particular, Telegram, VK, Apple, Google, Yandex, and other similar services) — to the extent necessary for User authentication; processing of data by such providers is governed by their own privacy policies, which the User is advised to review separately.
- Communication and mailing service providers — organisations that deliver one-time confirmation codes and service notifications by email and SMS/messengers; the current list of such providers and their jurisdiction is published in Appendix No. 1 to this Policy.
- Identity verification (KYC) and transaction monitoring (KYT) service providers — organisations engaged by the Company for the purposes set out in items 2 and 3 of Section 4; the current list of such providers, the jurisdiction of their activity, and the scope of data transferred are published in Appendix No. 1 to this Policy in the manner provided for in clause 5.3.
- Finzy storefront partners — third-party services whose products are available through the Service; data is disclosed to such partners only to the extent and for the purposes necessary to carry out an operation initiated by the User, and is accompanied by notice to the User of such partner in the Service interface prior to the operation.

- Government authorities and regulators — upon a lawful request of a competent authority of the Republic of Costa Rica or another applicable jurisdiction, in connection with compliance with AML/CFT legislation, tax legislation, or a court decision or other authorised body's ruling.
- Infrastructure providers — hosting, cloud services, security analytics and monitoring tools, acting as processors on behalf of the Company under agreements providing for data protection obligations no lower than those established by this Policy.

6.2. The Company does not sell Users' personal data and does not provide it to third parties for their own marketing purposes without the User's separate explicit consent.

6.3. Before engaging any new processor, including verification and transaction monitoring service providers, the Company carries out a reliability review and enters into an agreement containing confidentiality and data protection obligations no lower than those established by this Policy, including obligations relating to secure processing, restricting the use of data strictly to the stated purposes, and notifying the Company of security incidents.

7. Cross-Border Data Transfer

7.1. Because the Company is registered in the Republic of Costa Rica while Users are predominantly located in CIS countries, the processing of personal data necessarily involves cross-border data transfer, including to communication, mailing, verification, transaction monitoring, and cloud infrastructure service providers, regardless of their jurisdiction of registration.

7.2. The Company takes measures to ensure an adequate level of data protection in connection with cross-border transfer, including: entering into contractual confidentiality and data protection terms with data recipients; limiting the volume of data transferred to the minimum necessary for the specific purpose; using encryption during data transfer (TLS/SSL and similar protocols); and vetting data recipients for compliance with security requirements before transfer begins.

7.3. By consenting to use the Service, the User provides informed consent to the cross-border transfer of their personal data in the manner described in this Section, as provided for by Law No. 8968 of the Republic of Costa Rica in respect of cases where such transfer is necessary for performance of the contract with the data subject or for compliance with the Company's legal obligations.

8. Data Retention Periods

8.1. Personal data is retained no longer than necessary for the purposes of its processing, subject to the following periods:

- Account and profile data — throughout the term of the User's account and for the applicable limitation period after its closure.
- KYC verification data and transaction history — not less than five (5) years from termination of the business relationship with the User or the last operation, in accordance with international AML/CFT standards (FATF recommendations).
- Technical logs, session data, audit logs — up to thirty-six (36) months, except where longer retention is required for investigating security incidents or at the request of a competent authority.

- Address book data imported with the User's consent — retained until consent is withdrawn or the account is deleted, after which it is deleted within no more than thirty (30) calendar days.
- Data of unregistered P2P transfer recipients — retained until the recipient registers with the Service or until expiry of the period established by the Service for the transfer/invitation, after which it is deleted or anonymised if the recipient does not register.

8.2. Upon expiry of the established periods, personal data is subject to secure deletion or anonymisation, except where its further retention is expressly required by applicable law.

9. Rights of Data Subjects

9.1. In accordance with Law No. 8968 of the Republic of Costa Rica and its implementing Regulation, and having regard to best practices applied under CIS legislation, a data subject has the right to:

- Access (Acceso) — obtain confirmation of whether their data is being processed and obtain access to it;
- Rectification (Rectificación) — request correction of inaccurate, incomplete, or outdated data;
- Erasure/Cancellation (Cancelación/Supresión) — request deletion of data where there is no lawful basis for its further retention;
- Objection (Oposición) — object to the processing of data for specific purposes, in particular direct marketing;
- Withdrawal of consent — withdraw previously given consent to data processing at any time via account settings in the Service or by submitting a written request in the manner provided for in Section 13; withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal;
- Data portability — obtain a copy of their data in a structured, machine-readable format (PDF/CSV);
- Complaint — lodge a complaint with the Costa Rican Data Protection Agency (PRODHAB), as well as with the competent data protection authority of the country of the data subject's citizenship or residence, where provided for by local law.

9.2. To exercise the above rights, a data subject shall submit a request using the contact details set out in Section 13. The Company reviews the request and provides a response within thirty (30) calendar days of receipt, with the possibility of extending this period for a similar duration in the case of a complex request, and with mandatory notification to the applicant of the reasons for such extension before expiry of the initial period.

9.3. The Company may refuse to delete data where its retention is necessary to comply with legal obligations (in particular, AML/CFT requirements), to protect the Company's legitimate interests in connection with possible judicial or administrative proceedings, or where deletion would undermine the integrity of records required to be maintained by law. In the event of refusal, the Company shall provide the applicant with a reasoned explanation and inform them of their right to apply to PRODHAB.

9.4. The rights set out in this Section are exercised free of charge, except in the case of manifestly unfounded or excessive repetitive requests, in respect of which the Company may charge a reasonable administrative fee covering administrative costs, or refuse to consider the request, stating the reasons for such refusal.

9.5. A person whose contact details were disclosed to the Company by a User under clause 3.6 of this Policy (including through address book import or specifying a P2P transfer recipient) and who is not a registered User of the Service, is entitled to request deletion of the relevant data by submitting a request using the contact details set out in Section 13, without the need to create an account with the Service. The Company reviews such a request in the manner and within the periods provided for in clause 9.2.

10. Security Measures

10.1. The Company applies technical and organisational measures to protect personal data, commensurate with the level of risk, including: encryption of data in transit (TLS/SSL) and, where applicable, at rest; hashing of passwords and session tokens; role-based access control for employees and contractors; logging and audit of access to systems processing personal data and transaction data; regular vulnerability analysis and monitoring of suspicious activity; and storage of biometric verification data (selfies) in encrypted form with restricted access for authorised personnel.

10.2. The Company takes reasonable security measures consistent with industry standards; however, it cannot guarantee absolute protection against all types of security threats and recommends that Users observe basic digital hygiene practices (using unique passwords, securing devices, exercising caution when following links, and promptly reporting suspicious activity).

10.3. In the event of a security incident likely to result in a high risk to the rights and freedoms of data subjects, the Company notifies the affected persons and, where applicable, the competent authority without undue delay, within a reasonably practicable period not exceeding seventy-two (72) hours from the time the Company became aware of the incident, unless applicable law establishes a different period.

11. Processing of Minors' Data

11.1. The Finzy Service is not intended for persons under 18 (eighteen) years of age, or such other, higher age of digital capacity established by the law applicable to the data subject. The Company does not knowingly collect personal data of persons below such age. Upon discovering that such a person has registered, the Company promptly blocks the relevant account and deletes the data collected, except where its retention is required to comply with the Company's legal obligations.

12. Changes to This Policy

12.1. The Company may amend this Policy in connection with changes in legislation, the engagement or replacement of service providers, the development of the Service's functionality, or other reasonable grounds.

12.2. Users are notified of material changes affecting the scope of data collected, the purposes of its processing, or the rights of data subjects, by publication of a new version of the Policy in the Service and/or by sending a notice to the specified email address or via a push notification, not less than 14 (fourteen) calendar days before the changes take effect, except for changes made to comply with a direct requirement of law, which may take effect immediately with subsequent notification. Updating Appendix No. 1 in the manner provided for in clause 5.3 does not constitute a material amendment to the Policy and does not require separate prior notification.

12.3. Continued use of the Service after the changes take effect constitutes the User's consent to the new version of the Policy. If the User does not agree with the changes, they may discontinue use of the Service and request deletion of their data in the manner provided for in Section 9.

13. Contact Information

For matters relating to the processing of personal data, and to exercise the rights set out in Section 9, any person may contact:

- Company: Finzy Sociedad de Responsabilidad Limitada, legal entity No. 3-102-921514.
- Registered office: San José, Montes de Oca, San Pedro, Los Yoses, Avenidas 8 y 10, Calle 39, LY Center, Costa Rica.
- Contact email address for inquiries, including on personal data processing matters: info@finzypay.io.
- A data subject may also contact the Costa Rican Data Protection Agency (PRODHAB), website: www.prodhab.go.cr, telephone: +506 2528-3315.

14. Governing Law and Dispute Resolution

14.1. The processing of personal data, the exercise of data subjects' rights, and matters of this Policy's compliance with applicable law are governed by the law of the Republic of Costa Rica, including Law No. 8968 and its implementing Regulation, regardless of the data subject's location.

14.2. Nothing in this Policy or in the ToS, including any arbitration clause or choice-of-law agreement contained in the ToS in relation to the parties' contractual relationship, limits or deprives a data subject of the right to: (a) lodge a complaint with PRODHAB or the competent data protection authority of the country of their citizenship or residence; or (b) apply to a court of competent jurisdiction on matters relating to the protection of personal data, where applicable law mandatorily guarantees such right and does not permit it to be limited by agreement of the parties.

14.3. Disputes between the Company and a User arising from the contractual relationship in connection with use of the Service, but not directly relating to the protection of personal data, are resolved in the manner provided for in the ToS.

Appendix No. 1 — Service Providers and Purposes of Processing

The current list of identity verification (KYC), transaction monitoring (KYT), and communication/mailing service providers engaged by the Company under clauses 5.3 and 6.1 of this Policy is published and kept up to date in the Service interface and/or on the Company's web page at https://app.finzypay.io/ and forms an integral part of this Policy.

No.	Processing Purpose	Data Categories	Legal Basis
1	Account registration and creation, authentication	cl. 3.2, 3.3	Performance of contract
2	Identification and identity verification (KYC)	cl. 3.1	Legal obligation (AML/CFT legislation), contract
3	Transaction monitoring, risk scoring, fraud prevention (KYT)	cl. 3.4, 3.5	Legal obligation (AML/CFT legislation)

4	Execution of crypto-to-crypto exchange operations and interaction with the storefront partner	cl. 3.4	Performance of contract
5	Sending confirmation codes and service messages	cl. 3.2, 3.3	Performance of contract, legitimate interest (account security)
6	P2P transfers, including transfers to unregistered recipients	cl. 3.4, 3.6	Performance of contract on the instruction of the sending User
7	"Transfer to contacts" feature	cl. 3.6	Separate explicit User consent
8	Ensuring security, preventing unauthorised access, detecting anomalous behaviour	cl. 3.3, 3.5	Legitimate interest, proportionate to the balance between User rights and the need to protect the Service
9	Compliance with legal requirements (AML/CFT, sanctions compliance, tax reporting where applicable)	cl. 3.1, 3.4, 3.7	Legal obligation
10	Customer support and dispute resolution	all categories	Performance of contract, legitimate interest
11	Service improvement, product usage analytics (in aggregated/anonymised form where possible)	cl. 3.5	Legitimate interest
12	Sending service notifications (push, email)	cl. 3.2	Performance of contract
13	Marketing communications	cl. 3.2	Separate consent (opt-in), withdrawable at any time