Privacy Policy

This Privacy Policy (the “Policy”) describes how F-Tech (the “Company”, “we”, “us”, “our”) collects, uses, stores, transfers, and protects the personal data of users of the website https://kashbi.io, the KashBi application, the Telegram bot, Telegram Mini App, web version, API, and other related services of the Company (collectively, the “Platform”).

This Policy applies to users, website visitors, registered account holders, participants in P2P transactions, wallet holders, support applicants, and other persons whose data may be processed when using the Platform.

This Policy forms part of the user terms, Platform rules of use, AML/KYC/CTF policies, and other documents of the Company, where such documents apply. If you do not agree with this Policy, please discontinue using the Platform.

1. Terms and Definitions

1.1. Personal Data means any information relating to an identified or identifiable natural person, whether directly or indirectly.

1.2. Processing of Personal Data means any operation or set of operations performed on personal data, including collection, recording, organization, accumulation, storage, clarification, updating, modification, retrieval, use, transfer, provision of access, anonymization, blocking, deletion, and destruction.

1.3. User means a natural person who visits the website, registers on the Platform, uses a wallet, participates in P2P transactions, contacts support, or otherwise interacts with the Platform.

1.4. Account means a user account on the Platform created through the Telegram Mini App, Telegram bot, web version, mobile application, or any other available method.

1.5. Digital Assets means cryptocurrencies, tokens, stablecoins, and other digital units of account supported by the Platform.

1.6. P2P Transaction means a transaction between users of the Platform, within which users independently agree on the terms of exchange, payment, transfer of digital assets, fiat funds, goods, services, or other valuables, where such functionality is provided by the Platform.

1.7. AML/KYC/CTF means procedures for countering money laundering, terrorist financing, sanctions evasion, fraud, and other prohibited activities, as well as procedures for user identification, verification, and risk assessment.

1.8. Processor means a third party that processes personal data on behalf of the Company, in the interests of the Company, or for the purpose of ensuring the operation of the Platform.

2. About the Company and Contact Details

F-Tech is the controller, operator, or other responsible person in respect of personal data processed in connection with the use of the Platform, unless otherwise follows from applicable law or from a specific service.

Contact details:

- Website: https://kashbi.io

- Application: KashBi

- Support email: legal@kashbi.io

- Telegram support: kashbi_support

- Country of registration: Kazakhstan

- Registered address: 44/1 Al-Farabi Avenue, Apartment 207

3. General Principles of Personal Data Processing

We seek to process personal data lawfully, fairly, and transparently. We are guided by the principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, security, and confidentiality.

We do not seek to collect more data than is necessary for the operation of the Platform, compliance with law, security, fraud prevention, dispute resolution, AML/KYC/CTF procedures, and protection of the rights of the Company and users.

4. Legal Bases for Processing

Depending on the specific purpose and applicable law, we may process personal data on the following legal bases:

- the user's consent;

- performance of a contract or taking steps prior to entering into a contract;

- compliance with legal obligations;

- the Company's legitimate interest;

- protection of the vital interests of the user or other persons, where applicable.

Where processing is carried out on the basis of consent, the user has the right to withdraw consent. Withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal and does not prevent the processing of data on other lawful bases.

5. Data We May Process

5.1. Account and registration data:

- Telegram ID;

- Telegram username;

- first name, last name, or display name from Telegram, if transmitted by Telegram;

- avatar or profile image, if available through Telegram or uploaded by the user;

- Telegram WebApp initData required for authorization and verification of login authenticity;

- information on linking a Telegram account to an account created in the web version;

- email address;

- phone number;

- login;

- password in the form of a cryptographic hash for the web version;

- PIN code in the form of a cryptographic hash or other protected technical value for the Telegram Mini App;

- information on enabling and using 2FA for the web version;

- biometric settings only in the form of a technical indication that the feature is enabled, without receiving or storing biometric templates;

- other security factors in the form of technical identifiers, hashes, or indications that a feature is enabled;

- registration date, account status, interface language, notification settings;

- referral code, ID of the inviting user, or information on an affiliate program, where applicable.

5.2. Technical data:

- IP address;

- approximate location determined by IP address;

- device, browser, operating system, application version, and language data;

- session identifiers;

- account login information;

- security logs;

- data on errors, failures, application events, and diagnostics;

- date, time, and duration of Platform use;

- information on user actions in the interface necessary for security, analytics, and service improvement.

5.3. Wallet and digital asset transaction data:

- internal wallet and balance identifiers;

- public blockchain addresses;

- memo, tag, comment, or other payment identifiers;

- txid, transaction hash, block number, number of confirmations, network, asset, amount, fee;

- sender and recipient addresses on the blockchain;

- history of deposits, withdrawals, transfers, internal transfers, holds, blocks, reservations, freezes, refunds, fees, and adjustments;

- transaction status information;

- data on the source of incoming digital assets, where necessary for AML analysis or verification of the origin of funds;

- results of automated or manual risk checks of blockchain transactions, where such checks are applied.

Public blockchain data may be available in the relevant blockchain networks independently of the Company. The Company does not control public blockchain ledgers and cannot delete or modify data that has already been recorded in a public blockchain network.

5.4. P2P transaction data:

- ID of an advertisement, offer, or transaction;

- user’s role in the transaction;

- transaction type;

- selected digital asset, network, and settlement currency;

- amount, price, rate, margin, limits, fees;

- transaction status;

- date and time of creation, acceptance, payment, confirmation, completion, cancellation, or opening of a dispute;

- transaction terms, comments, and instructions;

- payment method;

- payment details provided by the user for the performance of the transaction;

- payment confirmations, receipts, screenshots, checks, messages, attachments, and other evidence;

- correspondence between transaction participants, where such functionality is provided;

- actions of moderators or arbitrators in a dispute;

- outcome of the dispute and grounds for the decision taken.

The user must not transmit through chat, transaction descriptions, attachments, or other fields any excessive personal data, data of third parties, secret codes, passwords, seed phrases, private keys, or other confidential information that is not required for the performance of the transaction.

5.5. Fiat payment data

Within P2P transactions, fiat payments are made directly between users, unless otherwise expressly provided by a separate service of the Platform. The Company is not a bank, payment institution, or party to a fiat transfer between users; however, for the purposes of supporting P2P transactions, resolving disputes, preventing fraud, and complying with applicable requirements, we may process:

- the selected payment method;

- the name of the holder of the account or payment instrument, if provided by the user;

- masked card or account details;

- bank, payment system, or provider;

- country of the payment instrument;

- amount, currency, date, and payment status;

- payment identifier assigned by the provider, if such identifier is provided by the user;

- information on a refund, cancellation, chargeback, dispute, or suspicious transaction.

We must not request or store full bank card details, CVV/CVC codes, passwords for banking applications, payment confirmation codes, or other secret payment data.

5.6. AML/KYC/CTF and risk assessment data

We apply a risk-based approach to AML/KYC/CTF. Identification, verification, additional checks, or requests for documents may not be applied to all users by default, but may be applied where necessary in light of applicable law, internal risk management rules, limits, the type of transaction, indicators of suspicious activity, partner requirements, a dispute, a support request, or other risk factors.

Where AML/KYC/CTF procedures are applied to a user, we may process:

- first name, last name, patronymic or other full name;

- date of birth;

- citizenship;

- country of residence;

- residential address;

- phone number;

- email;

- identity document;

- photograph, selfie, video verification, or liveness check;

- information on the beneficial owner, source of funds, source of wealth, occupation, or purpose of transactions, where applicable;

- sanctions, PEP, adverse media, and other screening results;

- results of AML checks of blockchain addresses and transactions;

- internal user risk profile;

- documents and explanations provided by the user at the Company’s request;

- information on suspicious, unusual, prohibited, or high-risk activity.

The mere fact of registration on the Platform does not mean that the user is required in all cases to undergo full KYC verification, unless otherwise provided by the interface, the terms of a specific service, or applicable requirements.

5.7. Support service data:

- contact details;

- content of the request;

- attachments, screenshots, documents, and messages;

- correspondence history;

- records of requests, if the relevant communication channel provides for recording;

- information on the resolution of the request;

- data necessary to confirm ownership of the account.

5.8. Marketing and communications data:

- consents and opt-outs from mailings;

- email, Telegram username, Telegram ID, or another communication channel;

- notification history;

- preferences regarding language and types of messages;

- delivery and message interaction statistics, where applicable.

We may send service, informational, and marketing messages related to the Platform, security, updates, new features, changes to terms, promotions, or other offers of the Company. We do not seek to send the user excessive, misleading, or intrusive messages. The user may opt out of marketing communications where such opt-out is provided by applicable law or the Platform interface. Service and legally significant notices may be sent regardless of any opt-out from marketing messages.

6. Purposes of Personal Data Processing

We may process personal data for:

- registration and account management;

- authorization, authentication, and access recovery;

- provision of wallets and digital asset transactions;

- processing deposits, withdrawals, internal transfers, balances, fees, and confirmations;

- provision of P2P functions, creation of offers, opening and completion of transactions;

- reservation, holding, or release of digital assets;

- exchange of messages and evidence between transaction participants;

- dispute resolution and arbitration;

- recording payment methods and verifying payment confirmations in P2P disputes;

- AML/KYC/CTF, sanctions screening, and risk management;

- transaction monitoring and verification of blockchain addresses;

- security, prevention of fraud, multi-accounting, spam, phishing, attacks, and other violations;

- user support;

- improvement of the Platform, error correction, feature testing, and analytics;

- legal purposes, settlement of claims, and protection of the Company’s rights.

7. Cookies and Similar Technologies

We may use local storage, session storage, technical session identifiers, server logs, first-party analytics not based on cookies, and other similar technologies for authorization, saving settings, session protection, fraud prevention, analytics, error diagnostics, improvement of Platform operation, and compliance with security requirements.

If in the future the Company begins to use cookies or third-party cookie-based analytics, such processing will be reflected in this Policy, a separate Cookie Policy, or a consent interface, where required by applicable law.

8. Automated Processing and Profiling

We may use automated and semi-automated tools to analyze technical events, transactions, AML risks, suspicious activity, rule violations, multi-accounting, and other security factors.

The Platform is positioned as privacy-first: we seek to minimize the collection of personal data, not to request identification documents without necessity, and to use a risk-based approach to checks. Privacy-first does not mean complete anonymity and does not exclude the processing of data necessary for security, compliance with law, AML/KYC/CTF procedures, dispute resolution, fraud prevention, and protection of the Platform.

Such processing may affect the availability of certain Platform functions, limits, the need for additional verification, suspension of a transaction, or referral of a case for manual review.

9. Transfer of Data to Third Parties

We do not sell users’ personal data and do not transfer it to third parties for the independent marketing purposes of such third parties without the user’s consent.

We may transfer personal data to the following categories of recipients:

1. infrastructure providers;

2. AML/KYC/CTF service providers;

3. banks, payment providers, and processors, only where such persons are involved in a specific service or transaction;

4. analytics and diagnostics providers;

5. communications providers;

6. legal, audit, and compliance advisers;

7. affiliates of the Company;

8. competent authorities;

9. counterparties to a P2P transaction, only to the extent necessary for the performance of the transaction;

10. potential or actual successors in the event of corporate changes.

In an ordinary P2P transaction, the fiat payment is made directly between users, and the Company does not process the fiat payment as a payment intermediary.

10. Cross-Border Data Transfers

The Platform may use infrastructure, partners, contractors, and processors located in different countries. In this regard, personal data may be transferred, stored, and processed outside the user’s country of residence or the Company’s country of registration.

When carrying out cross-border data transfers, we take reasonable measures to ensure an appropriate level of personal data protection, including contractual confidentiality obligations, technical and organizational security measures, vendor due diligence, and other mechanisms provided for by applicable law.

11. Retention of Personal Data

We retain personal data for as long as necessary for the purposes for which it was collected, as well as for compliance with legal obligations, dispute resolution, fraud prevention, and protection of the rights of the Company and users.

Indicative retention periods:

1. account data — for the duration of the existence of the account and for a reasonable period after its closure;

2. data on transactions, balances, deposits, withdrawals, and P2P transactions — for at

least the period required by applicable law, AML/CTF rules, accounting requirements, or internal risk management rules;

3. AML/KYC/CTF data — for the period established by applicable law;

4. support data — for the period necessary to process the request, resolve a dispute, improve the service, and protect the Company’s rights;

5. technical logs and security data — for the period necessary for security, diagnostics, incident investigation, and prevention of abuse;

6. marketing data — until consent is withdrawn or the user opts out of communications, unless longer retention is required to confirm the fact of consent or opt-out.

Account deletion or withdrawal of consent does not always mean immediate deletion of all data. We may retain data where this is necessary for compliance with law, AML/KYC/CTF, accounting, fraud prevention, dispute resolution, compliance with judicial or regulatory requirements, or protection of the Company’s rights.

12. Public Blockchain Data

The user understands that digital asset transactions may be recorded in public or partially public blockchain networks. The Company is not an operator of such networks, does not control their operation, and cannot delete, hide, modify, or restrict the dissemination of information already published on the blockchain.

13. Account Confidentiality and User Responsibility

The user is responsible for maintaining the confidentiality of account access credentials, including the web version password, Telegram Mini App PIN code, 2FA codes, devices, email, Telegram account, and other authorization means.

The user must not disclose to third parties the password, PIN code, one-time codes, 2FA codes, seed phrase, private keys, backup codes, access to the device or Telegram account, or any other data that enables access to the account or digital assets.

The Company does not request seed phrases, private keys, full bank card details, CVV/CVC codes, or passwords for third-party services.

14. Data of Third Parties

The user must not provide the Company with personal data of third parties without a lawful basis and the consent of such persons, where such consent is required. If the user provides data of third parties within a P2P transaction, support request, dispute, document upload, or other interaction with the Platform, the user confirms that they have the right to provide such data.

15. User Rights

Depending on applicable law, the user may have the right:

- to access personal data;

- to receive a copy of the data;

- to rectify inaccurate, incomplete, or outdated data;

- to delete data;

- to restrict processing;

- to object to processing;

- to data portability;

- to withdraw consent;

- to lodge a complaint with a competent supervisory authority.

We may refuse full or partial deletion of data where retention is necessary for compliance with law, AML/KYC/CTF obligations, accounting, fraud prevention, dispute resolution, performance of contracts, or protection of the Company’s rights.

16. Security of Personal Data

We apply reasonable technical and organizational measures to protect personal data, including encryption of data transmission, access control, segregation of rights, action logging, monitoring of suspicious activity, backup, incident response procedures, and internal information security rules.

Despite the measures taken, no method of data transmission over the Internet and no storage system is absolutely secure. The user must observe security measures on their side.

17. Children and Minors

The Platform is not intended for persons who have not reached the minimum age required to independently use the relevant services in the user’s country of residence.

18. Links to Third-Party Resources

The Platform may contain links to third-party websites, applications, wallets, blockchain explorers, payment services, Telegram resources, or other external services. The Company does not control such third-party resources and is not responsible for their privacy policies, security, content, or data processing.

19. Changes to the Policy

We may amend this Policy from time to time to reflect changes in the Platform, legislation, partner requirements, technologies, risks, or internal processes. The current version of the Policy is published on the website https://kashbi.io or in the Platform interface.

20. Contact Us

For questions regarding this Policy, the processing of personal data, the exercise of user rights, or complaints, the user may contact:

- Company: F-Tech

- Country of registration: Kazakhstan
- Website: https://kashbi.io
- Application: KashBi
- Email: legal@kashbi.io
- Telegram: kashbi_support
- Registered address: 44/1 Al-Farabi Avenue, Apartment 207

21. Language Versions

This document may be published in different languages. If applicable law requires priority to be given to a particular language version, such version shall apply. In all other cases, in the event of discrepancies between language versions, the English-language version shall prevail.