

PRIVACY POLICY

Version dated July 24, 2025

1. General Provisions

This Privacy Policy (hereinafter referred to as the “Policy”) is developed and applied by Bitbanker KG Limited Liability Company (hereinafter referred to as the “Company”) to define the procedures for the collection, storage, processing, use, and protection of User data obtained through the use of the platform <https://bitbanker.kg/ru> (hereinafter referred to as the “Platform”).

The Platform operates in accordance with the Law of the Kyrgyz Republic “On Virtual Assets,” the Law of the Kyrgyz Republic “On Personal Information,” as well as other applicable regulations and international standards in the field of data protection.

By registering on the Platform, including creating an account, completing identification and verification procedures, and using any features and services offered by the Platform (including viewing trading information, conducting transactions with virtual assets, contacting support, and other actions), the User hereby:

- Provides informed, voluntary, and explicit consent to the collection, storage, systematization, updating, use, anonymization, blocking, and deletion of their personal data, as well as to its transfer to third parties in accordance with this Policy and applicable law;
- Acknowledges the legal force of this Policy as an integral part of the User Agreement, having equal binding effect;
- Confirms that, prior to using the Platform, they have read this Policy, fully understand its content, including the consequences of consenting to personal data processing, as well as potential risks associated with breaches of confidentiality beyond the Platform’s control;
- Agrees that the Platform may unilaterally amend this Policy by publishing an updated version on the official website <https://bitbanker.kg/ru>, and that continued use of the Platform after such publication constitutes acceptance of the updated Policy;
- Acknowledges that refusal to provide mandatory personal data required for identification, verification, or service provision may result in the inability to use certain features or the Platform as a whole.

If the User does not agree with the terms of this Policy or does not wish to provide personal data to the extent necessary for proper performance of the User Agreement, the User must refrain from registering and using the Platform.

2. Purposes of Personal Data Processing

The processing of Users' personal data is carried out by the Platform strictly for specific, lawful, and pre-defined purposes aimed at ensuring the legality, transparency, and security of the Platform's operations, namely:

2.1. User Account Registration and Verification

Personal data is used to:

- identify the User when creating an account;
- verify the accuracy of the information provided;
- conduct verification procedures (KYC), including initial verification and periodic data updates;
- screen data against international sanctions lists, PEP (Politically Exposed Persons) lists, and other registries established by the legislation of the Kyrgyz Republic and international standards.

2.2. Performance of the User Agreement

Data is processed for the purpose of concluding, performing, maintaining, and terminating the User Agreement, including:

- providing access to the User account;
- facilitating virtual asset transactions;
- executing transfers, deposits, exchanges, or withdrawals of assets;
- maintaining internal records of transactions and User activities;
- resolving technical and legal disputes.

2.3. Compliance with AML/KYC Requirements

In fulfilling obligations related to anti-money laundering and counter-terrorist financing, the Platform processes personal data for:

- identifying the source of funds;
- monitoring suspicious transactions;
- analyzing User behavior;
- interacting with supervisory and authorized government authorities.

2.4. Provision of Services under the User Agreement

For the full provision of Platform services, including but not limited to:

- trading operations with virtual assets;
- wallet management;
- access to market quotes;
- ensuring technical compatibility with DApps, third-party wallets, protocols, and other services;
- User support and handling of inquiries.

2.5. Compliance with the Laws of the Kyrgyz Republic

The Platform processes personal data in cases explicitly required by law, including:

- maintaining accounting and financial records;
- fulfilling reporting obligations to government authorities;
- ensuring compliance with court decisions, requests, and orders of authorized bodies.

2.6. Protection of Rights and Legitimate Interests of the Platform and/or Third Parties

Personal data may be used for:

- investigating security incidents;
- preventing fraud and other abuses;
- ensuring compliance with the User Agreement, AML/KYC Policy, and this Policy;
- legal protection in case of claims, disputes, or other legal actions initiated by Users or third parties.

2.7. Sending Notifications and Technical/Legal Communications

Using contact information, the Platform sends Users:

- system notifications (service updates, changes to agreements and policies, maintenance notices);
- security alerts and notifications of suspicious activity;
- legal notices regarding their rights and obligations;
- informational messages within the scope of Platform functionality (e.g., transaction confirmations).

2.8. Improving Quality, Usability, and Security of the Platform

The Platform uses personal data for:

- improving the user interface;
- personalizing services based on User preferences;
- conducting behavioral analytics to optimize functionality;
- preventing technical errors and system failures;
- ensuring compatibility with various devices, browsers, and operating systems.

3. Categories of Personal Data Subject to Processing

In the course of providing services and operating the Platform, the Company processes the following categories of Users' personal data, depending on specific actions, transactions, services used, and applicable legal requirements:

3.1. Identification Data

Information that allows unambiguous identification of the User, including:

- full name (last name, first name, patronymic, if applicable);
- date and place of birth;
- gender;
- citizenship (including multiple citizenships);
- PIN, TIN, or similar identifiers in other jurisdictions (if required);

- tax residency status (where required under KYC/AML regulations).

3.2. Contact Data

Information required to communicate with the User and send legally significant notifications:

- email address;
- mobile or landline phone number;
- residential and/or registered address;
- country and city of residence;
- preferred language of communication.

3.3. Identity and Legal Status Documents

Data contained in official documents provided by the User as part of verification and AML/KYC compliance procedures:

- national passport, ID card, residence permit;
- driver's license (if used as an identification document);
- international passport or other identity documents;
- documents confirming residential or registration address;
- certificates of registration of sole proprietorships or legal entities, powers of attorney (in case of representation);
- other documents required under internal compliance procedures and applicable law.

3.4. Photo and Video Materials, Biometric Data

For identification, security, and fraud prevention purposes, the following may be processed:

- facial photographs provided for comparison with identity documents;
- video recordings confirming the User's presence during verification (including "video with a code phrase");
- biometric templates (e.g., facial recognition data), if processed using relevant technologies (subject to separate User consent);
- images or scans of documents uploaded via the Platform interface.

3.5. Financial and Transactional Data

Information generated during the use of the Platform and execution of virtual asset transactions:

- data on deposits and withdrawals of funds;
- trading history, orders, and transactions on the exchange;
- information related to payment infrastructure (crypto wallet addresses, transaction identifiers);
- information on the source of funds (where required);
- related financial information, including User risk profile, transaction volumes, and activity frequency.

3.6. Technical Information and Behavioral Data

Data automatically collected by the Platform for functionality, security, and analytics purposes:

- IP addresses and their geolocation;
- date, time, and duration of sessions;
- information about the device used, operating system, and browser type;
- login history and actions performed on the Platform;
- behavioral indicators (navigation patterns, time spent on pages, click sequences);
- technical identifiers (including cookies, session IDs, user agent).

3.7. Other Data Provided Voluntarily by the User

The Platform may also process:

- information contained in support requests;
- data submitted through feedback, claims, or review forms;
- information from publicly available sources (e.g., social media or public databases), if the User provides links during verification;
- information collected through surveys, events, or promotional activities;
- business-related information if the User acts on behalf of a company or principal.

4. Legal Grounds for Processing

The processing of Users' personal data by the Platform is carried out exclusively on lawful grounds in compliance with the legislation of the Kyrgyz Republic, including the Law of the Kyrgyz Republic "On Personal Information," as well as international data protection standards. In particular, such grounds include:

4.1. Consent of the Personal Data Subject

The User provides informed, voluntary, and specific consent to the processing of their personal data:

- upon registration on the Platform;
- when completing verification procedures;
- when using specific services that require the provision of additional data (e.g., uploading documents, biometric images, photos);
- when confirming acceptance of this Privacy Policy and the User Agreement.

Such consent may be withdrawn by the User at any time, unless processing is required on other lawful grounds (e.g., AML/KYC obligations or contractual requirements).

4.2. Necessity for the Performance of the User Agreement

Personal data is processed where necessary for:

- registration, activation, and maintenance of the User account;
- providing access to the Platform's functionality;
- processing transactions, orders, and other User actions;
- ensuring interaction with technical and legal support services;

- fulfilling all obligations arising from acceptance of the User Agreement.

Without such processing, the Platform would be unable to fulfill its obligations to the User.

4.3. Necessity for Compliance with Legal Requirements

The Platform is required to process personal data in order to comply with legal obligations established by the legislation of the Kyrgyz Republic and other applicable regulations, including international agreements relevant to the Platform's activities.

Such processing is mandatory, and refusal by the User to provide data for these purposes may result in the inability to use the Platform's services.

4.4. Legitimate Interests of the Platform

The Platform may process personal data based on its legitimate interests, provided a balance is maintained between such interests and the User's rights. These interests include, in particular:

- ensuring reliable and uninterrupted operation of services;
- protection against unauthorized access, fraud, and other abuses;
- maintaining information and financial security;
- conducting internal analytics (e.g., performance monitoring, interface adaptation, functionality improvement);
- protecting the Platform's rights and interests in the event of legal disputes or claims.

5. Data Storage and Protection

5.1. The processing of the User's personal data is carried out on an ongoing (indefinite) basis using all methods permitted by law, including automated, semi-automated, and non-automated processing, with or without the use of computing equipment, within personal data information systems or outside such systems.

5.2. The User's personal data may be disclosed or transferred exclusively in cases and in the manner expressly provided for by the legislation of the Kyrgyz Republic, including upon a reasoned request from authorized government authorities, provided there is a valid legal basis (e.g., a court order, regulatory directive, or obligations arising from international agreements).

5.3. The Platform implements all reasonable and necessary organizational, technical, and software/hardware measures to protect Users' personal data from unauthorized or accidental access, alteration, destruction, blocking, copying, distribution, as well as from any other unlawful actions by third parties. Such protection is ensured in accordance with legal requirements, the current level of technological development, and an assessment of potential risks.

5.4. The Platform shall not be liable for any disclosure of personal data resulting from the User's own actions, including intentional sharing of information with third parties or negligent handling of account access credentials that leads to unauthorized access. The Platform recommends that Users follow best practices in digital security and maintain the confidentiality of their authentication data.

6. Transfer to Third Parties

The Platform ensures a strictly limited and controlled access regime to Users' personal data. Transfer of such data to third parties is permitted only to the extent necessary to achieve the purposes of processing and where a valid legal basis exists.

In particular, personal data may be transferred to the following categories of recipients:

6.1. Authorized Government Authorities

The Platform may disclose the User's personal data:

- in response to official requests made in accordance with the legislation of the Kyrgyz Republic;
- based on a court decision, order of an investigative authority, or directive of another authorized government body;
- as part of mandatory reporting stipulated under the laws "On Virtual Assets," "On Personal Information," "On Counteracting the Financing of Terrorism and the Legalization (Laundering) of Criminal Proceeds," etc.;
- in cooperation with the Financial Market Regulation and Supervision Service, financial intelligence units, or tax authorities.

6.2. Affiliates and Partner Organizations

To ensure uninterrupted operation of the Platform, improve service quality, and fulfill contractual obligations, personal data may be transferred to:

- subsidiaries, parent companies, and other entities under common control with the Company;
- partners ensuring technological interoperability of services;
- external service providers involved in technical and operational support, subject to the principle of minimum necessary access.

6.3. Supporting Service Providers

Processing and transfer of data may be required for interaction with third parties providing the Platform with the following services:

- technical and hosting solutions, including cloud storage, content delivery networks, and analytics platforms;
- legal support (including litigation, claims handling, advisory on international sanctions regimes, etc.);
- payment infrastructure and money transfer operators, where the User initiates transactions requiring third-party payment providers;
- auditors, consultants, and compliance providers assessing regulatory compliance and security standards.

All such third parties are required to maintain confidentiality and use the personal data solely within the scope of delegated functions.

6.4. Cross-Border Transfer of Personal Data

In certain cases related to technical support, storage, backup, or provision of ancillary services, personal data may be transferred to or accessed by third parties located outside the Kyrgyz Republic, including jurisdictions:

- where servers or data centers of partner providers are located;
- where contractors providing cloud, hosting, legal, or analytical services are registered;
- within data transfers between affiliated entities of the Company operating in other countries.

Such cross-border transfers are carried out only if one or more of the following conditions are met:

- the recipient country ensures an adequate level of personal data protection recognized under international or national law;
- standard contractual clauses (SCCs) or other agreements ensuring sufficient data protection safeguards are in place;
- the User has provided explicit and informed consent, where required by law;
- the transfer is necessary for the performance of a contract between the Platform and the User or to fulfill the User's request;
- the transfer is carried out upon request of an authorized authority in accordance with applicable law or international agreements.

The Platform undertakes to ensure that cross-border transfers provide a level of protection not lower than that required under the legislation of the Kyrgyz Republic and, where necessary, to conduct legal and technical risk assessments related to such transfers.

7. User Rights as a Personal Data Subject

A User whose personal data is processed by the Platform is entitled to all rights of a personal data subject stipulated by the legislation of the Kyrgyz Republic, including, but not limited to, the following:

7.1. Right to Access Personal Data

The User has the right at any time to request:

- confirmation of whether their personal data is being processed;
- the categories of personal data being processed;
- the purposes and legal grounds for processing;
- retention periods or criteria used to determine them;
- sources from which personal data was obtained;
- information about third parties to whom the data has been disclosed;
- a description of the data protection measures in place;
- clarification of the consequences of refusing to provide mandatory data.

7.2. Right to Rectification and Updating of Personal Data

The User has the right to request that the Platform:

- promptly correct outdated, inaccurate, or incomplete personal data;
- update personal data in case of changes (e.g., passport details, contact information, etc.);
- update data provided for identification purposes, including supporting documents.

7.3. Right to Restriction or Erasure of Personal Data

The User may request temporary suspension of processing (restriction) or full deletion of their personal data if:

- the data is outdated, inaccurate, or unlawfully obtained;
- further processing is no longer necessary for the purposes for which the data was collected;
- the retention period has expired or the User has withdrawn consent (provided no other legal grounds apply).

Important: deletion or restriction of personal data may result in the inability to continue using the Platform.

7.4. Right to Withdraw Consent

The User has the right to withdraw previously given consent to the processing of personal data at any time by submitting a corresponding request to the Platform.

Withdrawal of consent does not affect the lawfulness of processing carried out prior to such withdrawal and does not apply where processing continues on other legal grounds.

7.5. Right to Lodge a Complaint

The User has the right to:

- file a complaint with the authorized personal data protection authority of the Kyrgyz Republic if they believe their rights have been violated;
- request clarification from the Platform regarding specific actions or decisions related to data processing;
- seek judicial remedies, including filing claims to restore violated rights and recover damages.

7.6. Procedure for Exercising Rights

To exercise any of the above rights, the User may submit a request via:

- the Platform's support service (through the personal account or email);
- postal mail to the Company's registered address.

Requests shall be reviewed within 10 (ten) business days from the date of receipt, unless otherwise provided by law. In certain cases, the Platform may request additional identification of the User to verify their identity and prevent misuse.

8. Use of Cookies and Similar Technologies

To enhance the efficiency of the Platform, improve user experience, and ensure security, the Company uses automated data collection technologies, including but not limited to:

- cookies (text files stored in the User’s browser);
- web beacons (invisible pixels tracking User activity on the website);
- local storage, session storage, and other browser storage mechanisms;
- fingerprinting technologies (browser/device fingerprinting).

8.1. Purposes of Using Cookies and Similar Technologies

These technologies enable the Platform to:

- Authenticate Users — recognize registered Users, maintain session parameters, and prevent repeated login requests;
- Analyze behavior and preferences — track on-site activity, evaluate navigation patterns, identify popular sections/pages, and generate aggregated analytics reports;
- Improve usability and personalize the interface — store user preferences (language, layout, dark/light mode), and speed up content loading;
- Ensure information and financial security — detect suspicious logins and activity, monitor unauthorized access attempts, and prevent phishing and session hijacking.

8.2. Types of Cookies Used

The Platform may use the following types of cookies:

- Strictly Necessary Cookies — required for basic website functionality (e.g., authentication, CSRF protection, navigation). These do not require separate User consent;
- Functional Cookies — enable interface personalization and store User preferences;
- Analytics Cookies — collect aggregated statistics on User activity to optimize content and structure;
- Security Cookies — used to prevent fraud, detect suspicious activity, and protect data;
- Marketing Cookies (if applicable) — track interaction with advertising content and support targeted advertising (currently not used unless explicitly stated).

8.3. Cookie Management

The User has the right to manage the use of cookies and similar technologies, including:

- configuring or restricting cookies via browser settings (including deleting existing cookies and blocking new ones);
- using “incognito” or “guest” mode, where cookies are not stored after the session ends;
- disabling certain categories of cookies, where the Platform provides such options (e.g., via a cookie consent banner).

Please note that disabling cookies may affect the proper functioning of the Platform and limit access to certain features, including account login, transaction confirmation, and display of personalized content.

8.4. Storage and Security of Cookie Data

Information collected via cookies and similar technologies may be linked to the User's account and processed as personal data in accordance with this Privacy Policy.

All such data is protected using the Platform's technical safeguards, and access to it is strictly limited.

9. Amendments to the Privacy Policy

9.1. Right to Amend the Policy

The Platform reserves the right to unilaterally amend and supplement this Privacy Policy at any time without prior individual notice to Users, unless otherwise required by applicable law.

Such amendments may be driven by, including but not limited to:

- changes in the legislation of the Kyrgyz Republic or international practices;
- implementation of new technologies, services, and data processing methods;
- updates to regulatory requirements, including in the AML/KYC domain;
- internal initiatives to enhance security and transparency;
- the need to correct identified legal or technical inconsistencies.

9.2. Publication and Effective Date of Amendments

The updated version of the Policy shall become effective upon its publication on the Platform's official website at: <https://bitbanker.kg/ru>, unless otherwise specified in the updated version.

The Platform undertakes to publish the updated Policy in publicly accessible form, indicating the date of the latest revision, and, where technically feasible, to display a notification of changes upon the User's next login to their account.

9.3. Implied User Consent

Continued use of the Platform, including logging into the account, conducting trading operations, submitting orders, viewing content, or using any services after the updated Policy becomes effective, shall be deemed as the User's implied acceptance of its terms.

If the User does not agree with the amendments, they have the right to:

- discontinue use of the Platform;
- delete their account;
- submit a written objection or withdraw consent to personal data processing (to the extent permitted by law).