Privacy Policy of the Mobile Application for Individual Customers AKIB «Ipoteka Bank»

Last updated: March 24, 2026

This Privacy Policy (hereinafter — the Policy) of the mobile application for individual customers (hereinafter — the Application) has been developed by Joint-Stock Commercial Mortgage Bank "Ipoteka-Bank", a legal entity registered under the laws of the Republic of Uzbekistan (State registration No.: 55/25; registration date: 26.03.1999; TIN: 202858483) (hereinafter — the Bank), conducting banking activities under License No. 74 issued by the Central Bank of the Republic of Uzbekistan on 25.12.2021, and in accordance with the legislation of the Republic of Uzbekistan, including the Law "On Personal Data" dated 02.07.2019 No. ZRU-547, the Law "On Informatization" dated 11.12.2003 No. 560-II, and other regulatory acts.

The Policy defines the procedure and conditions for processing personal data of Users that the Bank may receive during their use of the Application. The User's consent to provide personal information given in accordance with this Policy extends to all affiliated persons of the Bank.

Processing of personal data is carried out on the basis of the User's consent through explicit actions in the Application (including confirmation of consent), as well as on other grounds provided by the legislation of the Republic of Uzbekistan.

If the User disagrees with the terms of this Policy, they must refrain from using the Bank's mobile Application.

1. TERMS AND DEFINITIONS

Personal Data — information recorded on an electronic, paper, and/or other material medium relating to a specific individual or enabling their identification;

Subject of Personal Data (User / Client / Subject) — a natural person to whom personal data relates;

Personal Data Database — a database in the form of an information system containing personal data;

Processing of Personal Data — the implementation of one or a set of actions for collection, systematization, storage, modification, supplementation, use, provision, distribution, transfer, anonymization, and destruction of personal data;

Third Party — any person who is not a User or the Bank, but is associated with them through circumstances or relationships related to the processing of personal data;

Automated Processing of Personal Data — processing of personal data using computing technology;

Mobile Application of the Bank — software of the Bank designed for remote banking services for individuals.

2. DATA PROCESSED BY THE BANK

2.1. When using the Application, the Client provides, and the Application (Bank) may collect and process the following types of information:

2.1.1. Identification data:

- Full name of the User (last name, first name, patronymic);
- Client's gender (male/female);
- Identity document data (passport or ID card), including series and number, issue date, and validity period;
- Date of birth;
- Personal Identification Number (PINFL);
- Permanent and/or temporary registration address;
- Place of birth;
- Phone number;
- Email address;
- User's photograph (biometric data, including face data) — obtained via the device camera solely for identification and authentication purposes.

2.1.2. Financial data for conducting financial operations:

- Credit history data and other financial data;
- Transaction information;
- Balance and transaction data for cards of other banks.

2.1.3. Automatically collected data when using the Application:

- IP address;
- Device language;
- Device model;
- Application performance information, including errors and technical data;
- Operating system and its version;
- Unique device identifiers;
- User actions within the Application.

2.1.4. Access to device Contacts (when applicable):

- The Application may request access to device Contacts solely during the loan application process and strictly with the User's explicit permission.
- The Application does not upload or store the User's Contacts list on Bank servers and does not share Contacts data with third parties.
- Only the phone number of the contact selected by the User is used, solely to auto-fill the relevant form field.
- Granting access to Contacts is not mandatory — the User may enter any phone number manually without providing Contacts access.

2.1.5. Access to the device camera:

- The Application requests access to the device camera solely to capture the User's photograph during identity verification and authentication.
- Images obtained via the camera are used only for the stated purposes; no covert or background recording is performed.
- Camera access is granted explicitly by the User and may be revoked at any time in the device settings.

2.1.6. Geolocation data (when User permission is granted):

- Approximate or precise location of the User's device.
- Geolocation data is used exclusively for fraud prevention and the protection of the User's financial transactions (anti-fraud system).
- Geolocation data is not used to track the User for advertising or other non-declared purposes.
- The User may disable geolocation access at any time in the device settings; this may affect certain protective features.

2.2. The Bank processes only personal data necessary to achieve the purposes specified in this Policy and does not carry out excessive data collection.

2.3. The User is responsible for the accuracy and completeness of the personal data provided. The User undertakes to promptly notify the Bank of any changes to their personal data.

2.4. Age restriction and minors' data

The Application is intended for use by persons aged 18 (eighteen) years or older. The Bank does not knowingly collect personal data of persons under the age of 18. If the Bank becomes aware that data of a minor has been submitted without the consent of their legal representative, the Bank will take immediate steps to delete such data.

3. PURPOSES OF COLLECTION AND PROCESSING OF USERS' PERSONAL DATA

3.1. The Bank processes only those personal data and requests access only to those device functions and data that are necessary for the proper provision of services and fulfillment of agreements with the User.

3.2. The Bank processes personal data for the following purposes:

- 3.2.1. Providing banking services to the User;
- 3.2.2. Identification and authentication of Users;
- 3.2.3. Providing the User with personalized services;
- 3.2.4. Communication with the User, including sending notifications and information, as well as processing appeals and applications from the User;
- 3.2.5. Improving quality, usability, and developing services;
- 3.2.6. Compliance with the requirements of the legislation of the Republic of Uzbekistan;
- 3.2.7. Prevention of fraud and financial crimes;
- 3.2.8. Other purposes specified in this Policy.

3.3. The User's biometric data (including face data) may be used exclusively for identity confirmation, secure login to the Application, transaction confirmation, and fraud prevention.

4. CONDITIONS FOR PROCESSING USERS' PERSONAL INFORMATION AND ITS TRANSFER TO THIRD PARTIES

4.1. The Bank processes Users' personal information in accordance with this Policy, the terms of specific services, and the Bank's internal regulations.

4.2. Processing of personal data is carried out in the following cases:

- User's consent to the processing of such data;
- Necessity to perform a contract to which the User is a party, or to take pre-contractual steps at the User's request;
- Necessity to fulfill the Bank's legally defined obligations;
- Necessity to protect the legitimate interests of the User or another person;
- Necessity to exercise the Bank's rights and legitimate interests to achieve socially significant goals, including protecting User rights and ensuring banking system security;
- Processing for statistical or research purposes, subject to mandatory anonymization.

4.3. The User may refuse to grant access to certain data (e.g., geolocation, camera, Contacts, and other device functions), but this may affect the availability of certain Application features.

4.4. The Application does not carry out covert data collection and does not access data without the User's knowledge.

4.5. The Bank respects the User's privacy settings and does not attempt to bypass or forcibly change them.

4.6. The Bank has the right to transfer the User's personal information to third parties in the following cases:

- 4.6.1. The User has given consent to such actions;

- 4.6.2. The transfer is required under the procedure established by the legislation of the Republic of Uzbekistan;
- 4.6.3. For compliance with information security requirements established by the legislation of the Republic of Uzbekistan;
- 4.6.4. Within the framework of legally established interactions with banking infrastructure organizations (payment systems, interbank settlements);
- 4.6.5. Providing technical and service support.

4.7. All third parties undertake to ensure a level of personal data protection no lower than that established by this Policy and applicable legislation.

4.8. Third-party software components (SDKs) used

The Application uses the following third-party SDKs, which may process certain User data within the scope of their functionality:

- Firebase / Firebase Crashlytics (Google LLC, USA) — application performance analytics and technical error logging;
- Amplitude (Amplitude, Inc., USA) — analysis of user interactions to improve services;
- MyID (MyID LLC, Uzbekistan) — User identity verification;
- Wultra (Wultra s.r.o., Czech Republic) — secure authentication;
- Threatmark (Threatmark s.r.o., Czech Republic) — threat detection and fraud prevention.

All the above partners undertake to process data solely in accordance with their respective privacy policies and to the extent necessary to perform the relevant functions.

4.9. User tracking (App Tracking Transparency)

The Application does not perform cross-site or cross-app tracking of User actions for advertising purposes. The Bank does not share device identifiers (including IDFA) with advertising networks or data aggregators for targeted advertising purposes.

4.10. Cross-border transfer of personal data

Due to the use of certain international software components (Section 4.8), certain technical data about Application performance (performance metrics, error data, aggregated analytics) may be processed by servers located in the USA and the

European Union. Transfer is carried out under standard contractual data protection instruments. Users' personal identification and financial data are stored exclusively on servers located in the Republic of Uzbekistan.

5. DATA STORAGE

5.1. Data retention periods

The Bank retains Users' personal data for the following periods:

- Financial and banking data (contracts, transactions, credit history) — 5 (five) years after termination of the contractual relationship, in accordance with banking legislation of the Republic of Uzbekistan;
- Personal identification data — for the duration of the User's agreement and 3 (three) years after its termination;
- Technical data (logs, device identifiers, error data) — no more than 12 (twelve) months;
- Geolocation data — no more than 90 (ninety) days.

Upon expiry of the specified periods, data is permanently deleted or anonymized, unless a longer retention period is expressly required by the legislation of the Republic of Uzbekistan.

5.2. The Bank does not store the User's biometric data (including face data) on its servers. Face data is used exclusively during the authentication session for identity verification purposes. Face data is NOT retained and is NOT transferred to any permanent storage — it is immediately and permanently deleted upon completion of the verification process.

5.3. Where trusted third-party identity verification providers are engaged, such providers process face data solely during the verification session. Third parties do NOT store or retain face data after the verification process is completed. The use of face data is strictly limited to identity verification purposes only.

6. PROTECTION OF PERSONAL DATA

6.1. The Bank takes legal, organizational, and technical measures to protect personal data, which include:

- use of modern data encryption algorithms and secure transmission protocols (TLS);
- strict control and differentiation of employee access rights to information;
- round-the-clock monitoring of systems to detect suspicious activity;
- regular data backups and other protective measures.

The Bank ensures full compliance with the legislation of the Republic of Uzbekistan and international standards (PCI DSS) and regularly undergoes external security audits. User data is stored in a secure perimeter and is not transferred to third parties except in cases expressly provided by law (e.g., by court order) or based on the User's consent.

6.2. Security incident notification

In the event of a personal data security incident that may pose a risk to the rights and freedoms of Users, the Bank shall promptly notify the competent government authority within the timeframes established by the legislation of the Republic of Uzbekistan. The User will be notified if the incident directly affects their personal data and poses a high risk to their rights.

7. USER RIGHTS

7.1. The User has the right to:

- obtain information from the Bank about the processing of their personal data upon request;
- withdraw consent to the processing of personal data;
- appeal to an authorized government body or court regarding the protection of rights in relation to their personal data;
- request clarification, update, or deletion of data (within the framework of legislation).

The User also has other rights provided for by the legislation of the Republic of Uzbekistan, in particular the Law "On Personal Data" dated 02.07.2019 No. ZRU-547.

7.2. The User may at any time withdraw consent to the processing of personal data by submitting a request to the Bank at the contact details on the Bank's official website. The request is considered within thirty days, unless a different period is established by law.

7.3. Account deletion

The User may delete their account in one of the following ways:

- In the Application: 'Profile' section → 'Settings' → 'Delete Account';
- By contacting the Bank's Contact Center at (+78) 150-11-22 or at info@ipotekabank.uz.

Requests to delete an account are processed within 30 (thirty) days. After account deletion, the Bank retains data the storage of which is required under banking legislation of the Republic of Uzbekistan (in accordance with the periods specified in Section 5.1). Data not subject to mandatory retention requirements is permanently deleted.

7.4. The Bank may continue partial processing of data, in particular archiving and storage, in cases provided for by the legislation of the Republic of Uzbekistan (including for fulfilling obligations and legal requirements).

8. USER MODIFICATION OF PERSONAL INFORMATION

8.1. The User may at any time modify (update, supplement) the personal information they have provided or part of it.

9. CHANGES TO THE PRIVACY POLICY. APPLICABLE LAW

9.1. The Bank has the right to make changes to this Policy at any time, indicating the date of such changes. In the event of changes to the purposes of personal data

processing, the Bank notifies Users of such changes and, where required, requests new consent for the processing of personal data in accordance with the amended purposes.

9.2. The new version of the Policy is posted in the Application or on the Bank's website and comes into force from the moment of its posting, unless otherwise provided.

9.3. The Bank recommends that Clients regularly refer to this Policy to familiarize themselves with the most current version.

9.4. The laws of the Republic of Uzbekistan apply to this Policy and to the relations between the Client and the Bank arising from or in connection with the Policy.

10. CONTACT INFORMATION

Joint-Stock Commercial Mortgage Bank «Ipoteka-Bank»

Address: Republic of Uzbekistan, 100000, Tashkent, Shahrisabz Street, 30.

TIN: 202858483 | MFO: 00937

License: No. 74 dated December 25, 2021

Contact Center: (+78) 150-11-22

Website: www.ipotekabank.uz | E-mail: info@ipotekabank.uz