Privacy Policy

IBT24 Mobile Application

This Privacy Policy (hereinafter - Policy) of IBT24 mobile application (hereinafter - Application) applies to information, which International Bank of Tajikistan CJSC (hereinafter - Bank) may obtain from a user's device when they uses the Application.

The use of the Application means the user's unconditional consent to this Policy and to the terms for processing of the information received from the user's device as specified therein. In case of any disagreement with the Policy the user must refrain from using the Application.

The Application and the services provided thereunder shall be sold to the user on the basis of contracts and agreements with the Bank, which, *inter alia*, regulate all the issues related to processing and storage of the user's personal data by the Bank.

This Policy shall be solely applicable to the Application. The Bank does not have control over and shall not be responsible for the information (and the consequences of its transfer) transmitted by the user to a third party, if such transfer was performed on a third party resource, which the user could have accesseed through the links from the Application.

The Bank has the right to amend this Policy by posting a new version of the Policy on the Bank's website and/or in the Annex. It is the the user’s respnsibility to familiarize himself/herself with the current version of the Policy.

Conents of the information that can be obtained from the user's device when they use the Application and the purposes for which it can be obtained (hereinafter "User Information")

1.1. Information about phone numbers from the address book on the device. Purpose: Phone numbers from the address book on the user's device shall be used in the Application to facilitate money transfer operations by the users. When installing the Application, the user shall be additionally informed about the purpose of using the phone numbers from their address book in the Application. When used in the Application, the data on phone numbers shell be copied to the Bank's servers and may be periodically updated.
1.2. Information about the location of the user's device (based on the data of the mobile network operator and GPS signals) Purpose: informing the user when using the Application about the location of the Bank's units and self-service devices, as well as about additional services available to the user and conditioned by their location.
1.3. Photo images taken with the device's camera. Purpose: Obtaining and using photo images as part of the services provided by the Application, including for creating and saving photo images in the user's profile in the Application, obtaining photo images of payment documents and bar codes in order to recognize them and use them for funds transfer operations in the Application.
1.4. Information about the version of operating system and the device model. Purpose: analysis of possible errors in the operation of Application and improvement of the Application’s operation. For the purpose of analysis, the Bank may pass the information about the operating system and the device model to third parties in an anonymized form.
1.5. Information about user's IP-address and connection point address. Purpose: to increase user security when using the Application and making financial transactions.
1.6. Information about SMS messages on the user's device. Purpose: saving and using the SMS messages received from the Bank in the Application.
1.7. Audio data received using the device's microphone (implemented in the Application if technically possible) Purpose: making audio calls to the Bank by the User using the Application.
1.8. Use of the Application’s built-in antivirus software.

1.8.1. Purpose: to increase the level of operational protection:

- information about the installed software, including the unique identifier of the software installation on the device, the identifier and version of the software used, the unique identifier of the device, the unique identifier of the user in the services of the right holder;
- information on the URLs being checked, including the URL about which reputation is requested and the URL of the page from which the checked URL was obtained, the connection protocol identifier and the number of the ports being used;
- information about the URLs being inspected, including the URL and IP address of the site being inspected, the serial number and contents of the URL and the certificate type and checksum (MD5);
- information to obtain the reputation of the file being checked, including its checksum (MD5), as well as the detection type, identifier of the record used in the threat database, and the type and time the record was created;

1.8.2. Purpose: identification of new and difficult to detect information security threats and their sources, intrusion threats, as well as increasing the level of protection of information stored and processed by the user on the device:

- information about the installed software, including the unique identifier of the software installation on the device, the identifier and version of the software used, the unique identifier of the device, data about the type of device and the OS and OS service packs installed on it;
- information on network spoofing attacks, including the URL, where the spoofing was detected, the version of the threat database used, the ID of the database entry corresponding to the detected threat, the name, the checksum (MD5) and the file size of the application that requested the spoofed URL, the client type, the attack weighting, the attack target name, the detection reliability level, the Silent detection flag;
- information about the files inspected, including the file name and checksum (MD5), its path and path pattern code, file type code and identifier, executable file identifier, name of the threat according to the rightsholder classification, time of issue and time of last update of the anti-virus database, identifier and type of the database entry used, debugging detection feature, vulnerability identifier and its hazard class, identifier of the software task within which the scan was performed, file check or signature feature.

1.8.3. 3 Purpose: to improve the quality of the software operation and software update:

- information on the results of the software update, including the type and unique identifier of the device on which the software is installed, unique identifier of the software installation on the device, identifiers of the software and the update task, identifier and version of the software update, identifier of the software update settings, result of the software update, identifier of the condition of the transferred statistics, identifier of the software settings, identifier and name of the partner for which the software is released, language of the software localization, unique identifier and type of the license installed;
- information about errors in operation of the software components, including the type and time of the error, as well as the ID of the software component and the task that caused the error, a copy of the area of RAM of the device that caused the error, the type and time of creating the copy of RAM area, dates of creation, activation and expiration of the license key being used, the number of computers the license is designed for, the name of the primary update file, date and time of the primary files of the previous and new update.

1.8.4. Purpose: to protect the user from fraud when visiting the pages of the Bank's website:

- Identifier and version of the software used, unique identifier of the computer, information about the status of the browser used, identifier of the software settings.

1.8.5. Purpose: to increase the level of protection of information stored and processed by the user on the device:

- Identifier and version of the software used, unique device identifier, type and version of the installed OS, type and version of the browser, time of the last update of the anti-virus databases;
- information about attacks involving network spoofing, including the URL where the spoofing was detected, the name of the target and the attack detection method;
- Information about certificates being scanned, including the URL and IP address of the site being scanned, the checksum (MD5) of the scanned certificate, and the reason it is not valid;
- information about detected threats and vulnerabilities, including the name of the threat and the result of its elimination, sign of OS vulnerability detection, the identifier of the threat detected at browser launch, the sign of detection of loading of an untrusted module;
- information about the level of protection against screen shots The above data on the built-in anti-virus can also be used to generate reports on information security risks. Additionally, under this Policy, the Bank may use additional software tools (including the Bank's partners) and cookies to collect and process impersonal statistical information about the user's use of the Application and services within the Application for the purposes of improving the Application;

2. Terms of processing of User Information

2.1. In accordance with this Policy, the Bank shall process only that information and only for the purposes defined in clause 1.

2.2. The anti-virus built into the Application processes the received information, excluding the data relating to the identified or identifiable on the basis of such information (personal data subject), and does not associate the processed information with the personal data of the user in any way.

2.3. The Bank shall take all organizational and technical measures depending on the Bank to protect the user's Information from unauthorized access by third parties, use, copying and distribution.

2.4. For the purposes set out in this Policy, the Bank may engage partners with whom the Bank has concluded appropriate confidentiality agreements for the processing of User Information. The Bank's transfer to the partners of the impersonal data on the use of the Application for the purposes of improving the Application is carried out on the basis of agreements with partners.

2.5. The user's information may be stored on the resources of the Bank and its partners during the term of the contractual relations between the Bank and the User regarding the Application, as well as within 5 years after the termination of such contracts.

2.6. The user's information may be provided to the state authorities in accordance with the requirements of the current legislation.