Erste Bank AD Podgorica Privacy Policy For mBanking application

INTRODUCTION

Wanting to show transparency and accountability to all users of mobile applications, whose data is collected and processed, this Privacy Policy of the Bank (hereinafter: the Policy) provides all relevant information concerning personal data processing, such as information on the processing purpose, type of data collected, third parties, and the rights that the User may exercise concerning the personal data processing.

As the personal data collection handler, the Bank is aware of the importance of personal data for each individual. Therefore, it is essential for us to act following the applicable law governing personal data protection. Thus, the Bank is continuously working to maintain and improve your personal data and privacy's security.

It is necessary to understand specific terms having the following meanings to understand this Policy better:

Personal data – include all information of a natural person whose identity has been or can be established. They include name, surname, personal identification number, address, location data, photograph, employment data, income, etc.

Personal data processing - the act by which personal data is automatically or otherwise collected, registered, recorded, organised, stored, modified, withdrawn, used, inspected, transmitted, published or otherwise made available, sorted, combined, blocked, deleted, destroyed, or subject to any other action performed on personal data.

The Bank - The Privacy Policy issuer is Erste Bank AD Podgorica (hereinafter: the Bank), with registered office at Arsenija Boljevića 2A, Identification number 02351242, account number 907-54001-10, SWIFT code OPPOMEPG, Bank's website www.erstebank.me, info phone: +382 (0)20 / 440-440, e-mail: info@erstebank.me.

The body authorised to supervise the Bank's operations as a payment service provider is the Central Bank of Montenegro (CBCG).

Mobile application – is a software solution enabling contracting and using the Erste mBanking service via mobile devices (smartphones) supporting its installation and operation under the Minimum Technical Requirements of the Electronic Banking Service available at www.erstebank.me.

User - For the Privacy Policy purposes, the User is considered a natural person - a consumer who has concluded a Framework Agreement on Payment Services with the Bank for purposes not intended for activity, business or profession.

WHO IS THE PERSONAL DATA COLLECTION HANDLER?

The Bank is the personal data collection handler. As a handler, it collects, processes and uses the User's personal data. For all questions concerning personal data processing, the User may contact the Bank at the e-mail addresses info@erstebank.me or vasemisljenje@erstebank.me, via the Call Center at 19991 or +382 (0) 20440440, at the Bank's registered office, or in the Bank's branches.

The Bank has appointed a personal data protection officer. For all questions and information concerning personal data processing, the User may contact the Bank by sending an e-mail to dpo@erstebank.me or by mail to the address Arsenija Boljevića 2A, 81000 Podgorica (with reference: Attn. Personal Data Protection Officer).

WHAT DATA DO WE COLLECT AND PROCESS?

The Bank collects and processes the data necessary for the application to be used and fully functional through the mobile application. It may also collect and process the data to protect user data and financial assets and prevent misuse.

- Under applicable regulations, the Bank may automatically collect data on the User's device used to access electronic banking services and which in a broader sense can be considered the User's personal data: IP address, domain name, Android ID, IFV, Device ID, Installed applications, Serial number, Brand, Model, Manufacturer, Time zones, Wallpapers, SIM card serial number, Paired Bluetooth devices, Paired WIFI networks. The Bank may collect this information for secure use of the mobile application and prevention of misuse.

- The mobile application collects the User's geolocation data exclusively for the application's secure use. Location permission is recommended, but not required to use the application.
- The mobile application requires the User's consent to use the camera on a mobile device to use the PhotoPay functionality. Without the specified permission, the application will not access the specified functionalities. This permission is not required to use the application.
- For a direct call to the Bank (Call Center), the mobile application requires the User's consent to access the calling application. Acceptance of this permission is mandatory in order to identify and prevent potential threats that could lead to security misuse of the user's phone and account.
- For activation of mBanking service for the existing users of NetBanking service (Display card used as the authentication means), the mobile application requires entry of phone number which will be collected in our system, in accordance with the General conditions of usage of electronic banking services for the natural persons.
- User may change his/her contact phone number, which will be collected in our system, within the appropriate section in the application, only after logging in to the application.

APPLICATION LOG IN

Each User has to get acquainted with the General Terms of Use of the application to protect its own rights and interests. By accessing and using the mobile application, it is considered that the Users have understood and accepted the General Terms and Conditions. They are familiar with and agree with them, including this Policy.

The procedure for logging in to the mobile application is described in the application's General Terms of Use.

HOW DO WE USE THE DATA WE COLLECT?

The Bank will use the mobile application data for:

- ensuring the User's security from unauthorised use of the application or potential misuse attempts; and

- providing services following the Agreement and the General Terms and Conditions.

DATA ON ACTIVITIES AND USE

To improve the mobile application and the services available to the User through the application, the Bank may collect information on way of usage of the mobile application. This data is not personal but exclusively aggregated and statistical data and is not associated with a specific User.

EXCEPT FOR THE BANK, WHO MAY ACCESS THE USER'S PERSONAL DATA?

The Bank uses the User's personal data collected under the Agreement exclusively to provide electronic banking services and implement security measures. The Bank and the User shall take a high degree of security measures to ensure the lowest possible risk of access to data, alteration and loss of data.

The User agrees that the Bank may make available his/her personal data, and other data that represent banking secrecy, to the Group members or third parties according to applicable regulations to protect the User's property interests.

WHERE WILL THE USER'S DATA BE PROCESSED?

The User's personal data will be processed within Montenegro and the European Union.

HOW LONG DO WE KEEP USER DATA?

The Bank must keep the User's data for a specific period. Applicable regulations determine the exact data keeping period.
The data required to activate the mobile application is stored exclusively locally on the mobile device during the application's activity.

The data entered by the User into the mobile application as additional, optional data, are located within the application while the application is active or until the application is uninstalled.

WHAT ARE THE USER'S RIGHTS CONCERNING DATA PROCESSING?

The User shall not use the mobile application in a manner contrary to the application's General Terms of Use or that could jeopardise its true purpose and proper functioning.

Under the applicable law governing the personal data protection concerning the User's personal data collected and processed by the Bank, the User has the following rights:

- **The right to information whether the Bank processes the User's personal data**

The User may request information on whether the Bank processes his/her personal data. If processed, the Bank will provide the User with additional information provided by the applicable law governing the personal data protection, such as basic data on the Bank as the personal data collection handler, the content of processed data, the purpose and legal basis for personal data processing, the source of data according to available information, and the third parties.

- **The right to supplement incomplete, amend or delete inaccurate data**

If the User's processed personal data are incomplete or inaccurate, the User may request the Bank to correct, supplement or delete them at any time. The Bank is obliged without undue delay to act upon the request if it is grounded. The User is responsible for providing correct data, and it will inform the Bank about relevant personal data changes.

- **The right to delete personal data**

The User has the right to request the Bank to delete data if he/she considers that the personal data processing is not following the law. The Bank is obliged to act upon the User's request without undue delay if it is determined that it is justified.
The User may exercise these rights by submitting an application in person at one of the Bank's branches.

If the User considers that its personal data processing is not following the provisions of the applicable law governing the personal data protection, it may file a complaint to:

- the Bank's Personal Data Protection Officer via the e-mail address dpo@erstebank.me or to the address Arsenija Boljevića 2A, 81000 Podgorica (with reference: Attn. Personal Data Protection Officer).
- Supervisory Authority, i.e. the Agency for Personal Data Protection and Free Access to Information, at the address Bulevar Svetog Petra Cetinjskog no. 147 or mail address: azlp@t-com.me.

SECURITY

The mobile application is designed as an electronic banking system with high-security standards. The Bank also implements a few technical, personnel and organisational protection measures to ensure an adequate security level of User data processing and privacy, using, inter alia, the following proven technologies and security measures:

- **Encrypted communication -** Communication between the mobile application and the Bank's server is encrypted (coded).
- **User identification -** By identifying the User, the Bank checks whether the person logging in to the mobile application is a real, authorised user. This at the same time ensures that no one else has access to his/her accounts and funds. User identification when logging in to the mobile application is based on the use of:
  - **Two-factor authentication –** When logging in, Erste Display card, username password, and/or mToken, mToken serial number and mPin are used to generate a one-time password (OTP) as an additional protection level. The user identification security also requires that the card owner does not disclose its username, password/mPin or card and specified parameters used in the identification to a third party. It means that the user should not give access parameters to other persons. Moreover, the username and password must be kept separate from the card.

- **Automatic logout -** If you have logged in to the mobile application and do not use it for 15 minutes, the user's login will expire. To continue working, the user must re-login or re-enter his/her username and OTP/mPin. It prevents unwanted access to accounts and transactions while the user is not using the mobile device.

The User's obligations and responsibilities are described in the application's General Terms of Use.

CLOSING REGULATIONS

The Bank reserves the right to change this Policy.

All changes will be published on the Bank's website and linked from the Store and the mobile application.

Applicable from 27 May 2022