Privacy policy for usage of mobile application Zapad mBank

To be able to provide the high quality and timely service, in line with regulations and good business practice, Zapad Bank JSC (hereinafter: the Bank) gives utmost significance to the protection of personal data of our users. Through this Privacy Policy (hereinafter: the Policy) the Bank provides for all important information related to personal data processing, such as the information on the purpose of processing, type of data being collected, as well as the rights the user may exercise in relation with personal data processing.

By accepting General Terms and Conditions of Operations together with this Privacy Policy, you agree to the collection, use, processing, storage and disclosure of data in accordance with this Privacy Policy. The personal data that the Bank collects, uses, processes and storages are only used for providing and improving the Service. We shall neither use, share nor disclose your personal data to any third party, except as described in General Terms and Conditions of Operations and this Privacy Policy.

For more information in relation to collection, processing and protection of your personal data, kindly please contact us at: info@zapadbanka.me

Legal basis for data processing

The Bank shall use the Client's data exclusively for performance of the contract the Bank has with the Client. Data processing is required for performance of the contract in which the Client is each party towards which the Bank shall provide services, such as the registration of M – Banking application and mobile payment service.

Which data are being collected and/or processed?

Through mobile application the Bank collects and processes those data required for the application to be used and function completely, as well as for the purpose of protecting user's data and funds, as well as in preventing the abuse.

In line with current regulations, the Bank may automatically collect the following data:

- IP address
- Cell – phone number
- Time of registration
- Time of application
- Information on mobile device: manufacturer, model, OS version, IMEI number, HW serial number.

Using permissions on a mobile device

Mobile application requires the access to data and components of a mobile device to function properly. The following are data and components to which the access is allowed:

- Fingerprint/face-recognition on the device. The application requires this permission to enable the authentication through a fingerprint/ face – recognition if this option is chosen for login.

APPLICATION LOGIN

By accessing and using the mobile application it is considered that they have understood and accepted the General Terms and Conditions of Operations, that they are familiar to them and agree to them, including this Policy.

HOW DOES THE BANK USE THE DATA IT COLLECTS?

The Bank shall use the data through mobile application for:

- Securing User security from unauthorized usage of the application or potential attempts of abuse.
- Checking the authenticity of mobile application access
- Implementation and monitoring of payment transactions;
- Provision of services in accordance with the Agreement and General Terms and Conditions of Operations.

DATA ON ACTIVITIES AND USAGE

To improve the mobile application and service available to the user via the application, the Bank may collect data on the manner of usage of the mobile application. These data are not personal, but exclusively aggregate and statistical data that are not to be linked with a specific user.

WHO HAS THE ACCESS TO USERS' PERSONAL DATA BESIDE THE BANK?

The Bank uses the User's personal data collected in accordance with the Agreement exclusively for the purpose of providing the e-banking service and implementing the security measures.

The Bank and the User commit to take high level of security measures to secure less risk of access to data, change of data and loss of data.

WHERE WILL THE USER DATA BE PROCESSED?

User's personal data shall be processed within Montenegro.

HOW LONG THE USER DATA WILL BE KEPT?

The Bank shall process personal data only for the period required in relation to the purpose of data processing.
Data required for activating the mobile application are kept the whole time the application is active, exclusively locally on a mobile device.

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.

USER RIGHTS CONCERNING DATA PROCESSING

Individuals whose data are being used have certain rights under the General Regulation od Data Protection, which implies:

- the right to be informed within a month from the date of receipt of Bank's request, which is obliged to provide such information free of charge, electronically, in a form compatible for machine reading;

- the right to access personal data, including the purpose of processing, category of given personal data, recipients to whom those data are submitted, suggested period for keeping those personal data;
- right to correction of irregular personal data concerning the individual (entity);
- Right to deletion / „right to be forgotten“;
- Right to limit the processing;
- Right to transferability of data based on which the user has the right to receive their own personal data in a structured form suitable for machine reading and that such data may be transferred to another controller;
- Withdrawal of consent when the processing relies on consent;

SECURITY

The Bank has established special organizational and technical mechanisms securing the high level of personal data security. The Bank tries to use physical and electronic systems enabling protection of user personal data from unauthorized and illicit processing, unintentional loss, destruction or damage.

The Bank is held liable to secure that the Client's personal data are safe. Aiming to prevent the unauthorized access or disclosure of data that are being transferred, stored or processed otherwise, the Bank keeps physical, technical, electronic, organizational and procedural protection measures in line with current regulations.

Communication between the mobile application and Bank's server is encrypted.

When logging in Zapad mBank, two – factor authentication is used.

The Bank provides for the security of user identification by having the parameters for log in unambiguously connected to the User, meaning that potential disclosure of such information to third parties may not lead to compromising the data.

FINAL PROVISIONS

The Bank reserves the right to change this Policy

All changes will be published on Bank's official website and on Store for mobile applications.