

INFORMATION

REGARDING THE PROCESSING OF PERSONAL DATA

(according to Art. 13 and Art. 14 of Regulation (EU) 2016/769)

As a personal data controller, First Investment Bank ("Fibank" or "the Bank") strictly adheres to the legal and regulatory provisions regarding the collection and processing of personal data. Customer satisfaction in all its aspects is a priority for us, especially when it comes to your data. Therefore, we consider our duty to exercise due diligence in the processing of your personal data and to take all possible measures for their protection from unlawful actions.

We hereby inform you of the processing of your personal data, of the rights you have in relation to data protection, and provide you with the information under Art. 13 and Art. 14 of Regulation (EU) 2016/679 of the EP and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR).

The content and scope of the data processed are in line with the type of products and services you wish to use, or are already using. As a credit institution with a universal license for banking activity on the territory of Bulgaria and abroad № РД22-2257/16.11.2009, issued by the Bulgarian National Bank, Fibank offers a variety of banking products. It is our aim, through recognized standards and advanced technologies, to offer innovative and secure solutions to our customers, as well as to protect the information and data entrusted to us.

INFORMATION ABOUT THE PERSONAL DATA CONTROLLER AND CONTACT DETAILS

Controller – First Investment Bank AD (Fibank), UIC 831094393

Headquarters and registered office:

111 P, Tsarigradsko shose Blvd.

1784 Sofia

Phone: (02) 817 11 00; (02) 9 100 100

BIC/ SWIFT: FINVBGSF

Website: www.fibank.bg

Data Protection Officer of First Investment Bank AD:

Dimitar Hristov

First Investment Bank AD

111 P, Tsarigradsko shose Blvd.

1784 Sofia

E-mail: dpo@fibank.bg

FOR WHAT PURPOSE AND ON WHAT GROUNDS DO WE PROCESS YOUR PERSONAL DATA?

The Bank processes your personal data on the following legal grounds:

(In certain cases, processing may be based on more than one grounds)

A. Performance of a contract

In the performance of an existing contract between you and the Bank, as well as in taking pre-contractual steps. Processing is done so that we may provide you with the product or service you have applied for, as well as for their use during the term of the contract. This includes:

- ❖ Performing transactions, provision of the requested products and services;
- ❖ Performing analyzes;
- ❖ Notifications on the performance;
- ❖ Notifications on important changes in the transactions or terms of use of the product/service.

B. Legal obligation

Compliance with our legal obligations such as:

- ❖ identifying you, as well as verifying your identification in accordance with the Law on Measures against Money Laundering;
- ❖ performing automatic exchange of financial information under the Tax and Social Insurance Procedure Code;
- ❖ providing information to state bodies and institutions such as BNB, NSSI, NRA, courts, prosecution, SANS and others, in compliance with the relevant legal procedures;
- ❖ performing creditworthiness assessment, and risk assessment and management in the Bank and the Group of First Investment Bank AD.

As a credit institution, we comply with a number of regulations that, in addition to the above, include laws such as the Law on Credit Institutions, the Markets in Financial Instruments Act, the Law on Consumer Credit, the Law on Consumer Real Estate Loans, the Payment Services and Payment Systems Act, the Law on Measures Against the Financing of Terrorism, the Law on Obligations and Contracts, the Civil Procedure Code, the tax and accounting legislation, as well as the regulations related to the supervision of the activity, e.g. by the BNB and FSC.

C. Legitimate interest

We process your personal data for the purposes of the legitimate interests pursued by the Bank or by a third party, for example in cases such as:

- ❖ review and optimization of analytical needs and procedures for direct customer access – e.g. testing the achieved goals and ways to improve products in line with customer requirements, improving customer service;
- ❖ market research, advertising and polls conducted when you have not objected to the use of your data;
- ❖ video surveillance to collect evidence of criminal acts, or to provide proof of transactions (for example ATM transactions) and to protect clients and employees;
- ❖ phone records (e.g. of alerts, notifications of lost payment instruments, provision of information, contact center inquiries);
- ❖ sending communications about the products and services used through SMS, letters, emails, telephone calls and others, not related to marketing purposes;

- ❖ measures related to business management, improvement of services and products and customer retention;
- ❖ measures to protect employees, clients and the property of the Bank (such as the Bank's access regime);
- ❖ prevention and investigation of fraud and criminal acts;
- ❖ ensuring the IT security and IT operations of the Bank;
- ❖ complaints and claims, disputes, including in court proceedings;
- ❖ Risk Management in First Investment Bank AD (e.g. management of operational risk in carrying out transactions, credit risk in determining total exposures, etc.).

D. Task carried out in the public interest

In case we carry out tasks in the public interest or in the exercise of official authority vested in the controller. In such situations, the Bank may assist a public authority by sharing personal data for the purpose of preventing or detecting a criminal offence.

E. Your consent

In cases where we process your data based on your consent, processing shall be within the scope and for the purposes set forth in your consent. Any given consent may be revoked at any time under the terms of the document [Procedure for the exercise of rights related to personal data \(Appendix 1\)](#).

The Bank processes personal data after you have given consent, for instance, in cases of electronic signing of documents through specialized device in the Bank's office (biometric data – behavioral characteristics), in cases of remote identification, e.g. video identification, including performed by external qualified trust services provider (biometric data – facial characteristics). After consent, we process your data (e.g. list with names and telephone numbers) from your contacts list (Contacts) in your mobile device for the purpose of executing Blink P2P transfers by mobile number.

WHAT PERSONAL DATA DO WE PROCESS?

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The information we process depends on the product/service that you use or apply for.

General information we process for all products/services – personal information (e.g. names, address, date and place of birth, nationality, EGN, email address, phone number); identity verification data (e.g. signature specimen); identity document details (such as ID card number);

Depending on the type of product/service we process data on existing contractual obligations (such as financial information, bank account numbers); information about your financial status (e.g. data on your creditworthiness, scoring or rating, etc.); marketing data (advertising, sales); documented data (e.g. consultation records); recorded data, image and voice data (e.g. video or phone records);

biometric (behavioral, facial) data; data (including list with names and telephone numbers) from your contacts list (Contacts) in your mobile device; information from your electronic communication with the Bank (e.g. cookies); results generated by the Bank as a result of processing; data on compliance with regulatory requirements.

For users of credit products, additional information may be found in [Appendix 2](#).

For users of payment services, additional information may be found in [Appendix 3](#).

For users of investment services, additional information may be found in [Appendix 4](#).

The Bank uses automated decision making, including profiling in accordance with the requirements of Art. 22 of the GDPR to give you the best possible service. Evaluation of personal aspects is done to inform you about certain products and services. It is possible that, when considering applications for certain credit products, decisions are partially taken without human intervention on the basis of predetermined criteria for assessing creditworthiness.

Profiling is also done in implementation of mandatory regulatory provisions, such as the legislation on measures against money laundering, terrorist financing, investment services and activities.

SOURCES OF INFORMATION

We collect the data we process directly from you, when you apply for a particular product or service online or in a bank office, as well as in the course of our relationship. In cases where the personal data are provided by a representative, such representative must inform and provide to the person represented this document.

We also process information we have legally and legitimately obtained from institutional registers such as the Central Credit Register (BNB), the Register of Bank Accounts and Safe Deposit Boxes (BNB), the NSSI, the Chamber of Private Enforcement Agents, Register of Bulgarian Personal documents (MI), from publicly available sources such as the registers of the Registry Agency, from the media, or from officially published lists of persons to whom sanctions apply.

WHO MAY HAVE ACCESS TO YOUR DATA?

Within First Investment Bank AD, your data is received by those employees who need access to it for the performance of a contract, for obligations and regulatory provisions, or for the protection of legitimate interests.

Service providers, agents, contractors and subcontractors with whom we work and who have undertaken obligations and are responsible for the processing of personal data under current legislation, may also obtain the data, for example: companies operating in the field of banking services, qualified trust services providers, IT services, logistics, insurance companies, telecommunications, photocopying, debt collection, consultancy, sales and marketing, including companies from the Group of First Investment Bank AD for risk management purposes; correspondent banks, depositaries, exchanges, payment system operators, other participants in the payment process, information desks, depending on the services we provide to you.

The Bank also provides client personal data to third parties in compliance with legal obligations applicable to credit institutions, or for the purposes of measures against money laundering and terrorist financing, the automatic exchange of financial information, the prevention and investigation of fraud related to banking activity, as well as when necessary for the provision of a specific service.

STORAGE PERIOD OF YOUR PERSONAL DATA

First Investment Bank AD stores your personal data in compliance with the statutory provisions and protecting the legitimate interests of the Bank, the retention period depending on the type of documents and services used. For example, in the case of a general 5-year period, the Accountancy Act requires that data from accounting registers, including tax audit documents subject to subsequent financial inspections, are stored for 10 years. Retention periods may be extended further, for example in the case of litigation, extension of the limitation period due to interruption, as well as in the implementation of legal provisions and requirements of supervisory authorities.

HOW TO EXERCISE YOUR RIGHTS CONCERNING THE PROTECTION OF YOUR PERSONAL DATA?

For submission of request/statements regarding the processing of your personal data, please refer to the document ["Procedure for the exercise of rights related to personal data" \(Appendix 1\)](#).

ARE YOU OBLIGED TO PROVIDE US YOUR PERSONAL DATA?

Within our business relationship, you are obliged to provide the personal data required for the initiation, performance and termination of your relationship with the Bank, as well as for ensuring compliance with the applicable contractual obligations or legal requirements.

In the event you do not provide the necessary data and documents, we shall not be able to enter into contractual relationship with you, or continue such relationship.