

GENERAL TERMS AND CONDITIONS OF FIRST INVESTMENT BANK AD FOR MY FIBANK ELECTRONIC BANKING

I. DEFINITIONS

1.1. For the purposes of these General Terms and Conditions (hereinafter the GTC), the Request for registration/change/termination of registration for electronic banking, the request for registration/deactivation of a Mobile Device in the electronic banking system My Fibank, as well as all requests, declarations, confirmations and other written agreements for use of My Fibank (hereinafter the Agreement), concluded between the Account Holder (User of payment services) and First Investment Bank AD with its headquarters and registered office in the city of Sofia 1784, 111 P Tsarigradsko shose Blvd., UIC 831094393, holding a universal license № PA22-2257/16.11.2009, issued by the Bulgarian National Bank, which supervises its activities (hereinafter the Bank or Fibank), as well as all appendices thereto, the terms listed below shall have the following meanings:

- a) „Digitized Card“ shall mean a digitized version of a plastic credit or debit payment card or Virtual Card. The plastic card or the Virtual Card and its digitized version are one and the same card with one (total) credit limit/overdraft to one account where all payment transactions are booked. The Digitized Card may be used in the country and abroad, through an NFC Mobile Device, at terminals allowing contactless payments;
- b) „Electronic Signature“ (ES) shall mean a means for signing electronic documents, electronic identification of Authorized Users, and authentication for online services, such as: 1) Transaction Authorization Number (TAN) generated by a Hardware/Software Token; 2) Personal Identification Number (PINt); 3) ID number of the registered Mobile Device; 4) Password; 5) code sent via SMS to a mobile phone number registered with the Bank 6) Fingerprint/Face ID; 7) public and private key; or a combination thereof;
- c) „My Fibank electronic banking“ or „My Fibank“ shall mean the automated system for electronic banking of First Investment Bank AD, through which the Account Holder or persons authorized by him/her (Authorized Users) are entitled to remote access via the Internet at <https://my.fibank.bg> to the electronic services offered by the Bank. The My Fibank service can be used on personal computers, portable devices (laptops, tablets, etc.), or via the My Fibank Mobile Application after downloading it from the link;
- d) „Electronic statement“ shall mean a verbal statement delivered in digital form through a common standard for transformation, reading and visual presentation of information. An electronic statement may also contain non-verbal information;
- e) „Statement“ shall mean „Account statement“ respectively „Card statement“ under the definitions set out in the General Terms and Conditions for opening and maintenance of bank accounts and provision of payment services, respectively, the General Terms and Conditions of Fibank regulating the issuance and use of bank cards;
- f) „Card“ shall mean a valid credit or debit bank payment card with the logo of VISA, VISA Electron, MasterCard or Maestro, issued by the Bank to the Authorized User, on which information is stored electronically and which is used repeatedly for identification of the Authorized User, or for remote access to the Account Holder's own funds, and subject to the other characteristics of the card as a payment instrument specified in the General Terms and Conditions of Fibank regulating the

issuance and use of bank cards;

g) „Qualified electronic signature“ (QES) shall mean an advanced electronic signature which was created by a device for creating qualified electronic signatures and is based on a qualified certificate for electronic signatures;

h) „Utility payment through the System“ shall mean a payment in BGN, including under predetermined conditions and parameters, of household or other obligations incurred on the territory of Bulgaria, which an individual Account Holder can pay through My Fibank ;

i) „Download Link for the My Fibank mobile application“: the application is available for free download over the Internet, and for installation from the online app stores for Mobile Devices using the respective operating system (AppStore, Google Play, AppGallery or other specified by the Bank);

j) „My Fibank Mobile Application“ (the Mobile Application, or the Application) shall mean a specialized application for Mobile Devices, through which the Account Holder or persons authorized by him/her shall have the right, subject to the presence Internet connection, to remote access to the My Fibank system;

k) „Mobile Device“ shall mean a portable electronic device (mobile phone, etc.) that can use a variety of applications through its operating system, is provided with various radio communications, and allows Internet connectivity. A Mobile Device with a camera can be used to scan QR codes. An NFC Mobile Device shall mean a Mobile Device with technology for contactless data exchange (Near Field Communication) for the purpose of making contactless payments;

l) „Blink instant transfer“ (Blink): a credit transfer in BGN under the Blink payment scheme of NCPS, BORICA AD, which can be executed 24 hours a day every calendar day of the year, with immediate or close to immediate processing and crediting the account of the Payee and confirmation to the Payer within seconds after acceptance of the order and its execution by the Bank;

m) „Transfer by mobile number“ (Blink P2P by mobile number or Blink P2P): Blink instant transfer between accounts of natural persons, carried out using a secondary payment account identifier - a registered mobile phone number linked to the account's IBAN;

n) „Operating system“: an essential part of the system software that manages and coordinates the work of the processor and other components of the Mobile Device. The Mobile Application is available for iOS, Android and Harmony OS operating systems. The Bank shall establish mandatory minimum requirements for the operating system version, and publish them on the Application page in the online app store;

o) „Authorized User“ shall mean an individual who is entitled, in the name and on account of the Account Holder, to access to My Fibank and the services offered through the System, depending on the rights granted, including the Account Holder when an individual;

p) „Password“ shall mean a predetermined combination of numbers, Latin letters and symbols, which is unique and known only to the Account Holder/Authorized User, serves to identify the Account Holder, respectively the Authorized User;

q) „Personal identification number“ (PINt) shall mean a combination of numbers which is used in combination with TAN and serves for identi-

fication and access to My Fibank, as well as for confirmation of electronic payment transactions;

r) „Username“ shall mean a combination of Latin letters or letters and numbers, predetermined by the Account Holder/Authorized User which, in combination with independent elements within the meaning of the LPSPS, serves for authentication of the Account Holder/Authorized User;

s) „User Session“ shall mean a period of time in which the Mobile Application allows access to its services, and after expiry of this period the session is automatically terminated. The Authorized User can specify the duration of the User Session in the Application settings. The Bank recommends that after use of the Mobile Application the session is terminated by pressing „Exit“. In order to start a new session in the Mobile Application, the means of access and identification need to be reintroduced again;

t) „Fingerprint/Face ID“ shall mean an independent element within the meaning of the LPSPS of the biometric data set used by the Mobile Device, including through Push Notifications, for identification of the User when performing operations remotely through the Mobile application, login at the Mobile application, as well as for confirmation of payment transactions over the Internet by the User's card, issued by Fibank. The Bank uses the functionality of the Mobile Device without storing the data.

u) „Working hours of My Fibank for execution of payment transactions“ shall mean an interval of time within the business day, after which the payment order shall be considered received by the Bank on the following business day;

v) „Business day“ shall mean every day on which the Bank carries out its activities necessary for the execution of a payment transaction. For payment transactions related to transfer of funds from/to other payment service providers Saturdays and Sundays when not announced as working days, as well as the official holidays in the Republic of Bulgaria, shall be considered non-business days;

w) „Charges“ shall mean all amounts due under the Tariff of Fees and Commissions (the Tariff), such as fees, commissions, expenses, regardless of their type;

x) „Tariff“ shall mean the Tariff of Fees and Commissions of First Investment Bank AD adopted by the Managing Board of the Bank, including the Bulletin of Interests accrued by the Bank on bank accounts in local and foreign currency (hereinafter the Interest Bulletin) to it, together with all of their annexes at the date of application;

y) „Account Holder“ shall mean an individual, a company, or another legal entity in whose name an account is kept with the Bank and which is entitled to dispose of the funds on this account in the capacity as a User of payment services. An individual Account Holder registered in the electronic banking system My Fibank may also act as an Authorized User of a Card when using the My Fibank services with a Card issued by the Bank;

z) „Transaction authorization number“ (TAN) shall mean a unique digital code, valid for single use only, which is generated through a specialized electronic encoding device: Hardware/Software Token;

aa) „Operating instructions for Fibank's electronic banking My Fibank“ or „Operating instructions“ shall mean the current instructions of the Bank for registration in My Fibank and use of the services offered by it, published on the System's website at <https://my.fibank.bg>, together with all annexes and amendments thereto;

ab) „Payment initiation service“ shall mean a service to initiate a payment at the request of the payment service user with respect to a payment account held at another payment service provider;

ac) „Account information service“ shall mean an online service to pro-

vide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with one or more than one payment service providers.

ad) „Hardware Token“ shall mean a specialized electronic encoding device for generating TAN. It is provided personally to the Authorized User by his request at an office of the Bank. It is registered for use by the Authorized User in My Fibank in his personal registration as well as in other registrations for which at the request of the Account Holder the Authorized User has been granted access to, following procedures specified by the Bank.

ae) „API Integration“ shall mean a functionality providing My Fibank electronic banking users with active banking rights to use services through a secure channel for real-time integration of data and documents directly between the user's information system and My Fibank electronic banking;

af) „ID number of a registered Mobile Device“ shall mean a combination of numbers and letters generated by the Mobile Application, depending on the Mobile Device and the version of the operating system used. The Mobile Device of the Authorized User is registered in the Mobile Application under this ID number. In combination with other independent elements, the ID number serves as means of access and identification to the application, as well as for confirmation of electronic transactions. Upon activating the Mobile Application with built-in Software Token, the ID number of the registered Mobile Device is associated with the built-in Software Token and the TAN codes generated by it;

ag) „QR (Quick Response) code“ shall mean a matrix code in the form of a square with black modules on a white background, with encoded information that is displayed when scanning the code with a Mobile Device camera. In My Fibank, QR Code is used for encoding information and its deciphering;

ah) „Software Token (Fibank Token)“ shall mean a specialized Mobile Device application that generates a single use transaction authentication number (TAN), respectively a 3D-Secure dynamic password for online payment transactions with cards issued by the Bank. Upon activation of the My Fibank Mobile Application under item 4.9. of these General Terms and Conditions, the Software Token is built into the Mobile Application and shall be used together with it;

ai) „Push Notification“ shall mean an electronic message with payment transaction data (including payment amount and recipient) and/or other reference information sent through My Fibank, including through the Mobile Application which can also facilitate the access to My Fibank or the confirmation of payment transactions, including online card transactions, by enabling the authentication of the payer through Fingerprint/Face ID or entering a PIN code.

1.2. For the terms connected to payment services which are not explicitly stated in these GTC the definitions set in the Glossary of the terms used in the General Terms and Conditions for opening and maintenance of bank accounts and provision of payment services of First Investment Bank AD shall be applicable.

II. SUBJECT

2.1. These GTC shall regulate the relations between the Bank and the Account Holder regarding the registration and use of the services provided through the Electronic banking of First Investment Bank AD: My Fibank, and shall form an integral part of the Agreement.

2.2. At the request of the Account Holder and depending on the method of registration, the Bank shall provide the Account Holder with access, through My Fibank, to one or more of the following services:

2.2.1. Passive (reference) banking transactions and a limited number of active transactions for which the Account Holder may also register Au-

thorized User/s specified by him:

- a) the Bank provides information by electronic means, allowing its reproduction in an unchanged way, convenient for archiving and storage, about the balance and transactions on bank accounts, and/or payment cards (account reports, statements and/or other report information) in volume and frequency under the terms of the respective service;
- b) information about the branches of the Bank, Fibank ATMs, exchange rates of the Bank, news, and current promotions;
- c) a limited number of active transactions: transfers between accounts kept in the name of the Account Holder in the Bank, utility payments, purchase of electronic vignettes;
- d) applying for credit products of the Bank intended for individuals and legal entities;
- e) other reference information.

2.2.2. Active banking related to the execution of payment or other transactions – active banking:

- a) opening and closing of bank accounts in BGN or in foreign currency: current, deposit, or other bank accounts (excluding joint accounts, basic payment accounts, or other accounts with special conditions for disposal or interest payments, expressly agreed at an office of the Bank), subject to the terms of the selected account announced by the Bank and accepted by the Account Holder;
- b) transfer of funds (in national or foreign currency) from/to an account of the Account Holder to/from another account kept with the Bank, or to/from another payment service provider, including utility payments, mass transfers, transactions through payment cards issued by the Bank or other similar instruments, repayment of obligations under credit cards and/or loans provided by the Bank, as well as other services subject to the terms, conditions and requirements of the Bank for the respective service;
- c) Blink instant transfer from/to an account with another payment service provider;
- d) applying and entering into agreements for, and use of retail credit products offered by the Bank as well as applying for credit products intended for legal entities;
- e) issuance of debit card to individuals, including in the name of minors: Debit MasterCard PayPass kids/teen;
- f) purchase/sale of currency or dematerialized gold from/to an account;
- g) submitting orders for cash transactions;
- h) API integration allowing creating transfers, as well as receiving information about the Account Holder's accounts, account statements and information about specific transactions.

2.2.3. My Fibank Mobile Application, with options for:

- a) use of passive banking as specified in item 2.2.1. above;
- b) use of passive banking as specified in item 2.2.1., letters „a“, „b“ and „e“ above;
- c) use of active banking as specified in item 2.2.2., letters „a“, „b“, „c“, „d“, „e“, „f“ and „g“ above, subject to the limits determined by the Bank, or selected by the Account Holder;
- d) card digitization;
- e) access to payment accounts of the Account Holder, maintained at other Account servicing payment service providers and provision of Account information and Payment initiation services according to items 5.10. – 5.14. from these GTC;
- f) making transfers by mobile number;
- g) confirmation of cash transfers and other payment transactions initiated at the request of the Account Holder or the Authorized User at bank offices;

h) entering into General Terms agreements, or annexes to agreements for brokerage in financial instrument transactions, as well as placing transaction orders – for individual Account Holders with active banking rights in the Mobile Application.

2.2.4. Providing Third Party Provider (TPP) with access to payment accounts of the Account Holder, maintained in the Bank and accessible online /current accounts/ for performing of Payment initiation and Account information services;

2.2.5. Other services.

2.3. The circumstance that the Account Holder operates with his accounts through My Fibank does not limit his ability to dispose of these accounts by any other means agreed upon with the Bank.

2.4. The Account Holder agrees, in connection with the use of the payment services and other related services offered by the Bank through My Fibank, that the opening and maintenance of bank accounts and the authorization and execution of payment transactions shall be carried out subject to the made registration, these GTC, the General Terms and Conditions for opening and maintenance of bank accounts and provision of payment services (GTCPS), and under the specific terms and conditions provided on the website of My Fibank at <https://my.fibank.bg> and/or on the Bank's website at www.fibank.bg.

2.5. The Bank shall have the right to expand or limit the scope of services offered through My Fibank, to set additional requirements, including procedural ones, to change the terms, including the price, the way of registration, the means of access and identification, their use, as well as the execution of certain operations based on changes in the current legislation, for security reasons or due to improvements in the respective service, as well as to impose other restrictions arising from the normative requirements of the current legislation. The Bank shall notify the users of the changes, new services and special terms and conditions for their use, by publishing them on the website of My Fibank at <https://my.fibank.bg>, and shall not be responsible for any damages or lost profits resulting from changing the scope of the services.

III. TERMS OF USE

3.1. My Fibank shall be accessible via the Internet at <https://my.fibank.bg> for Account Holders who have requested and received confirmation for their registration or for the registration of the Authorized Users specified by them under the terms and conditions determined by the Bank, and have registered means for access and identification as specified by these GTC.

3.1.2. The My Fibank mobile application shall be available for use after installing it from the My Fibank mobile application Download Link.

3.2. For the use of My Fibank and the services offered through it, the Bank shall set (and with respect to the Mobile Application – also publish on the Application page in the app store) the minimum technical requirements which the Account Holder and the Authorized User need to ensure.

3.2.1. In order to improve the quality of the service provided, the Bank reserves the right to make changes in the computer programs which perform it. Should any of these changes require a modification of the necessary equipment, operating system, or speed of the Internet connection, the Bank shall notify the Account Holder to that effect by a message made available to him through My Fibank, the Mobile Application, or on the Bank's website at www.fibank.bg prior to implementing the change.

Preliminary information

3.3. The Bank shall make these GTC, the Operating instructions for the My Fibank system, the Tariff, the GTCPS, as well as the special conditions and instructions for use of the specific service, available to the Users in an accessible way and allow sufficient time for making an informed

decision for the use of the service concerned, respectively for entering into an agreement, including through announcing them on the website of the System at <https://my.fibank.bg>, and/or on the website of the Bank at www.fibank.bg, or in another accessible manner, on a durable medium, in the form of intelligible text in Bulgarian language.

3.3.1. At the request of the Account Holder, the Bank may provide the preliminary information in a manner different than those indicated in item 3.3., subject to charges as per the Tariff.

3.3.2. For the convenience of the Users - foreign persons, the Bank shall provide these GTC, the Operating instructions, the Tariff and the GTCPS also in English language. In case of an inconsistency or contradiction, the original text in Bulgarian language shall prevail.

3.4. Before using the services offered by My Fibank, the Account Holder/the Authorized User shall be obliged to acquaint themselves with the specific rules for their use.

3.5. When using My Fibank, the Account Holder/the Authorized User shall be obliged to comply with the security measures, requirements and guidelines of the Bank published on the website of My Fibank.

IV. REGISTRATION, ACCESS AND IDENTIFICATION

My Fibank electronic banking

Registration with confirmation at an office of the Bank

4.1. Registration shall be performed personally by the Account Holder, by filling a registration form in My Fibank, respectively in the My Fibank Mobile Application, or a Request for registration at an office of the Bank, with the necessary data such as names, valid electronic address for receiving information, username, password and others as per the Operating Instructions.

4.1.1. The registration shall be confirmed and activated at an office of the Bank, based on a signed Request for registration/change/termination of the registration (the Request) and after presentation of all documents required by the Bank. The confirmation of the registration of a legal entity Account Holder, as well as of the Authorized Users, may also be performed by a person authorized by the Account Holder with a notarized power of attorney drawn up in accordance with the requirements of the Bank.

4.1.2. In the Request, the Account Holder may specify one or more individuals – Authorized Users who in his name and for his account may use My Fibank, determine their access rights to the selected services, and the limits of disposal in the presence of a notarized power of attorney. In case of granting rights for passive banking only, when the Account Holder is a company or another legal entity, the authorization of the Authorized User may be done in an office of the Bank in the presence of Bank's employee and the legal representative of the Account Holder.

4.1.3. The Account Holder may at any time unilaterally revoke the rights granted by him to the Authorized Users.

Registration with confirmation by a card

4.1.4. When registering through My Fibank or the My Fibank Mobile Application, the individual Account Holder shall identify himself before the Bank by entering his national ID number and the details of the Card issued in his name by Fibank: names (as printed on the Card), term of validity, type of Card, CVC/CVV (personalizing features of the card), as well as by using the provided personalized security features. By confirming his Request for registration, he shall confirm that he has read and understood these GTC, accepts their application in governing the relationship with the Bank in connection with the use of My Fibank, and instructs the Bank to enable his registration and debit the account to which the Card is issued (whose personalizing features they have

entered) with the fee payable under the Tariff.

4.1.4.1. Upon registration through My Fibank, the acceptance of these GTC, the confirmation by the Account Holder of the registration under item 4.1.4. and the sending by the Bank of a confirmation for the registration made, shall have the effect of conclusion of an agreement with the Bank.

4.1.5. Upon registration of Authorized Users who are minors, access to passive banking transactions shall be provided according to item 2.2.1, letters „a“, „b“ and „e“. In cases where an express request has been submitted at an office of the Bank, limited access may be provided to active transactions via the Mobile Application from a registered Mobile Device, allowing internal bank transfers from/to a Savings Account for teenagers to/from an account with a Debit MasterCard PayPass teen, if both accounts are registered in the name of the Authorized User, as well as the option to digitize debit cards.

4.2. Upon completed registration under item 4.1.4. above, individual Account Holders shall receive access to passive banking under item 2.2.1. above, except for transfers between accounts kept in the name of the Account Holder with the Bank. For any additional service or change in access, they need to submit a request to the Bank. Upon entering an agreement for active banking rights and after activating the Mobile Application with built-in Software Token, Account Holders shall also receive access to active banking in accordance with these GTC.

Registration via the My Fibank Mobile Application with confirmation using a third party qualified trust service provider

4.3. The Bank provides individuals with Bulgarian citizenship with the option to enter into agreements for banking packages including the use of My Fibank with active banking rights, opening of bank accounts (current or deposit), applying for debit cards and/or other products/services, or switching from passive of active banking under already existing agreements electronically, via the My Fibank Mobile Application.

4.3.1. Registration is made in person, by filling the necessary details such as full name, valid email address, mobile phone number, username, password, selection of desired product/s and providing required confirmations.

4.3.2. In the process of registration, applicants confirm their consent with the applicable General Terms and the Information on processing of personal data, including with those of the third party provider. Upon registration, video identification is performed by a third party provider and a one-time qualified electronic signature /QES/ is issued for signing the required documents such as a general terms agreement, declarations, and documents for the services selected by the customer and/or included in the package. The applicant needs to provide a copy of their identity card (front and back). After the applicant enters the one-time password sent to the mobile phone number specified by them, the request for a package/service, respectively for active banking, is considered made. Upon sending of a confirmation notice by the Bank, the agreement for the products/services requested by the applicant is considered entered into.

4.3.3. The Bank shall not be responsible for actions or inactions of the respective third party provider (e.g. delay in the transmission of data or documents, termination of service, interrupted access, communication failure due to problems with Internet or other electronic communication networks), nor for any resulting losses or damages. Fees charged by third party providers are separate from fees charged by the Bank.

Registration of businesses and legal entities (together businesses), verified by a third party qualified trust service provider

4.3.4. The Bank provides businesses (ET, OOD, EOOD) registered in Bulgaria, owned and represented by individuals with Bulgarian citizenship,

with the option to open current accounts or to enter into agreements for banking packages, including for use of My Fibank with active banking rights, remotely, via its website at: <https://fibank.bg>.

4.3.5. Requests for opening current accounts or for entering into agreements for banking packages/use of My Fibank can be submitted online, by individuals with Bulgarian citizenship legally authorized to represent the business or employees/authorized persons, by filling in the required data such as name, valid e-mail address, and mobile phone number, as well as details of the business including name, UIC, and registered address. Upon submission of the request, video identification of the applicant is performed by a third party qualified trust service provider. The applicant needs to provide a copy of their identity card (front and back).

4.3.5.1. The Bank sends a link via SMS to the mobile phone number of the legal representative indicated by the applicant. The link is used to confirm the data entered in the application by the applicant, the products (accounts/packages) requested, and to provide the required data and documents.

4.3.6. Entering into agreement for the requested products and services is carried out by the legal representative with a one-time QES issued by the third party qualified trust service provider. The procedure under items 4.3.2 and 4.3.3 above applies for video identification of the legal representative, respectively for remote entering into the agreement.

4.4. The initiation of any active transaction through My Fibank before expiry of 14 days from the conclusion of the distance Agreement shall be considered as express consent of the Account Holder for the Bank to begin implementation of the Agreement before expiry of the term under item 15.7. of these GTC.

4.5. The Account Holder shall be obliged to immediately notify the Bank in writing of any changes in the data or documents submitted by him, including with respect to the Authorized Users, regardless of whether or not the circumstances concerning such changes, including with respect to the representation of a legal entity, are subject to registration or disclosure in a public register.

4.5.1. The changes in the data/documents or representative powers shall have effect with respect to the Bank from the moment the Bank was notified by the Account Holder of such changes in writing, by depositing the relevant documents in an office of the Bank, and for updating mobile phone numbers – also following the procedure under item 4.5.2. below.

4.5.2. Authorized users may update their mobile phone number via My Fibank. For customers with active banking access, change and confirmation of the updated phone number is done through My Fibank, depending on the means of access and identification used by the Authorized User. Authorized users with passive banking access who hold a card issued by the Bank may change and confirm their updated mobile phone number by entering the authorization code of an ATM transaction and the ATM ID number, as printed on the ATM slip, within 24 hours of the transaction performed with such card.

Means of access and identification

4.6. The Account Holder/Authorized User may use one or any combination of the following means of identification and access to My Fibank, depending on the services requested:

4.6.1. Username and password in combination with a one-time code sent via SMS message to the Authorized User's mobile phone number registered with the Bank, providing access to My Fibank electronic banking. Upon registration made through My Fibank or the My Fibank Mobile Application, the Authorized User shall personally specify his username and password, and if the registration is made in an office of the Bank he shall have the right to specify his username, while a one-time password, for security purposes, shall be automatically generat-

ed by the Bank's information system and sent to the Authorized User's e-mail address specified in the Request. The Authorized User should then change the one-time password, determining a login password for My Fibank consisting of a combination personally selected by him.

4.6.2. Username and password in combination with TAN – by entering a username and password, followed by entering a TAN generated by a Hardware or Fibank Token, My Fibank electronic banking can be accessed;

4.6.3. Combination of TAN and PINt – all active and passive banking transactions in My Fibank, in accordance with the granted permissions, can be performed using a valid PINt and a TAN generated by a Hardware/Software Token together with one-time code, sent through SMS to the registered in the Bank number of mobile phone of the Authorized User (when using a Hardware Token).

4.6.3.1. The PINt used with a TAN from an activated My Fibank Mobile Application with built-in Software Token, shall be determined personally by the Authorized User in the process of activation, after identification through a combination of username, password and the one-time activation code of the Mobile Application. It shall be used to perform all active banking transactions, including 3D Secure card payments.

4.6.3.2. The Hardware Token does not require a computer installation or any other special settings. When receiving a Hardware Token, at an office of the Bank, the Authorized User shall also be provided with a PINt that shall serve for personal identification. For security purposes, the PINt shall be automatically generated by the Bank's information system and sent to the Authorized User's e-mail address specified in the Request.

4.6.3.3. Software Token (Fibank Token)

To unlock the Fibank Token application, the Authorized User chooses whether to use his biometric data, or a password known only to him. It shall be considered that, by submitting a Request for a Software Token, the Authorized User selects the Software Token as means of authentication before the Bank when using My Fibank, and that by activating it the Authorized User instructs the Bank to deregister any another active means of authentication – QES or PINt and TAN generated by a Hardware Token – should such means be present in his registration/s.

4.6.4. Password or Fingerprint/Face ID in combination with TAN from an activated My Fibank Mobile Application with built-in Software Token can be used for access and identification to perform all active banking transactions;

4.6.5. Public and private key used to access My Fibank through API integration.

My Fibank Mobile Application

4.7. To use the My Fibank Mobile Application, Account Holders should have a valid registration in My Fibank, and after activating the new version of the Mobile Application under item 4.8.1. – also an activated Mobile application on their registered Mobile Device (for active transactions).

4.8. To perform active transactions under item 2.2.2. letters „a“ „b“ „c“, „d“, „e“, „f“ and „g“ and under item 2.2.3., letter „f“ above, Authorized Users need to activate the Mobile Application and register the Mobile Device with which they will access it, stating their request through the Mobile Application under conditions and parameters determined by the Bank.

4.8.1. As of 15.08.2022, Fibank provides a new version of the My Fibank Mobile Application, allowing users who activate it to use a Software Token built into the Mobile Application.

4.8.1.1. Upon activation, the means of access and authentication that Authorized Users have used so far (PINt and TAN from a Hardware To-

ken/Fibank Token) shall be automatically deregistered. The PINt of the activated Mobile Application and TAN generated by the built-in Software Token shall become valid for all accounts where the customer is Account Holder and/or Authorized User (including as a representative).

4.8.1.2. With the activation of the new version of the Mobile Application with a built-in Software Token, all preset limits for execution of payment transactions with a registered Mobile Device shall be terminated, except for limits for transfers between accounts kept in the name of the Account Holder. The limits announced on the Bank's website at www.fibank.bg, or individually agreed between the Bank and the Account Holder, shall become active. The Bank shall enable Account Holders to change limits as provided by item 5.2.1. of these GTC.

4.8.2. An Authorized User can only have one activated Mobile Application with built-in Software Token. Upon activating the Mobile Application on another Mobile Device, the Mobile Application installed on a previous Mobile Device shall be deactivated.

4.8.3. Upon attempt for activation of the Mobile Application with built-in Software Token on a new Mobile Device, the Bank shall send an SMS to the registered mobile number of the Authorized User. For security reasons, the message shall contain a personalized link, allowing the Authorized User to activate the application on a new Mobile Device, or to block the activation process in case of suspected fraud or unauthorized action.

4.9. Activation of the Mobile Application with built-in Software Token shall be confirmed by the Authorized User remotely, following a step-by-step process determined by the Bank, which includes strong customer authentication. A one-time activation code for the My Fibank Mobile Application shall be sent via SMS to the Authorized User's mobile number registered with the Bank. The code shall be generated upon entering a combination of username and password, and shall serve for authentication in the activation process.

4.9.1. When the Mobile Application is activated, the built-in Software Token shall generate unique one-time codes (TAN) that can be used for access and identification purposes, as well as for confirmation of all electronic payment transactions through My Fibank, including online card payments.

4.9.2. The Authorized User may remove (uninstall) the Mobile Application from their Mobile Device at any time, as well as deregister the Device. In case of re-installation of the Mobile Application on an already registered Mobile Device, regardless of the reason for that, as well as in case of changing the version of the operating system with which the Device operates that was not imposed not by the manufacturer of the Mobile Device, the Authorized User needs to activate the Mobile Application again, under item 4.9 above.

4.10. Means of access and identification when using the Mobile Application, valid until activation of the Mobile Application with built-in Software Token under item 4.8.1 above:

1) Username and Password are the ones determined by the Authorized User for use with My Fibank. They serve for access and identification, and in case of existing registration for active banking – also for placing orders of payment transactions up to the predetermined limits.

2) Combination of PINt and TAN – by entering a valid PINt and a TAN generated by a Hardware/Software Token together with one-time code, sent through SMS to the registered in the Bank number of mobile phone of the Authorized User (when using Hardware Token) all active and passive banking transactions can be performed when using the services of the Mobile Application.

3) ID number of registered Mobile Device – is used in combination with a Username and Password or with Fingerprint/Face ID and/or TAN and PINt generated by a Hardware/Software Token for identification and access to the Mobile Application..

4) Fingerprint/Face ID – functional options of a Mobile Device, allowing the Authorized User to verify his identity through biometric data, which he uses to access the My Fibank Mobile Application, as well as to order payment transactions up to the preapproved limits – in case of registration for active banking. Through the use of the biometric data under the current Item and from a registered Mobile Device, the User may confirm his identity and the execution of payment transactions with a card, kept in his name and issued by the Bank.

Means of access and identification, valid after activation of the Mobile Application with built-in Software Token under item 4.8.1 above:

1) Combination of PINt and TAN – by entering a valid PINt and generating a TAN from the built-in Software Token, the Mobile Application can be accessed. The combination of PINt and TAN generated by the built-in Software Token serves to access the Mobile Application and perform all active and passive banking transactions when using services through the Application.

2) Combination of Fingerprint/Face ID and TAN – by using a Fingerprint/Face ID and generating a TAN from the built-in Software Token, the Mobile Application can be accessed and all active and passive banking transactions can be performed when using services through the Application.

4.11. When the Account Holder has determined one or more Authorized Users, each one of them shall use individual means of access and of identification. The Account Holder shall accept that the means of access and of identification used by the Authorized Users are secure enough for the purposes of transactions and the specific terms agreed with the Bank, and shall be used to personalize the Authorized Users before the Bank when they are acting in the name and for account of the Account Holder.

4.12. The Bank and the Account Holder agree that use of any of the ES specified in item 1.1., letter „b” of these GTC, independently and/or in combination between them and/or with other personalized security features such as Username, Password, PINt, ID number of a registered Mobile Device, TAN, Fingerprint/Face ID shall be used by the Authorized Users and accepted by the Bank for giving authorizations, placing orders, and making electronic statements through My Fibank and the Mobile Application for carrying out active banking transactions for the account of the Account Holder. The electronic statements submitted after logging into My Fibank or the Mobile Application shall be accepted and executed by the Bank as submitted and signed by the Authorized User, who has identified himself before to the Bank and is acting in the name and for account of the Account Holder.

4.12.1. The Bank and the Account Holder agree that the use, individually or in combination, of any of the electronic means for access and authentication listed in item 1.1, letter “b” above by the Account Holder or the Authorized User upon access and identification in My Fibank, including the Mobile Application, respectively the use of electronic signatures by the Bank (including advanced electronic signatures), shall have the force and meaning of legally valid electronic signatures within the meaning of Art. 13, para 4 of the Electronic Document and Electronic Certification Services Act. In their relations with each other, the parties shall equate them to handwritten signatures certifying the veracity and authenticity of electronic statements when ordering transactions, signing agreements and/or electronically confirming other actions/operations performed by the respective party.

4.13. The Bank reserves the right to change the permissible means of access and identification, or to set requirements for combinations thereof, in which case it shall inform Users by notification on the website of My Fibank at <https://my.fibank.bg> or in another appropriate manner.

Measures to protect the Means of access and identification

4.14. The Authorized User shall:

4.14.1. Keep secret the personal identification characteristics of his/her Means of access and identification, such as Username, Password, PINt, including of the Mobile Device (when using the My Fibank electronic banking, including My Fibank or Fibank Token Mobile Applications, as well as in case of operations through TPP), and take all necessary precautions against their becoming known to third parties, as well as protect the devices used for access (such as a computer, tablet, mobile phone, etc.). The PINt/Password selected by the Authorized User, including for unlocking the Fibank Token, should not consist of easily ascertainable combinations (such as phone number, date of birth, car registration number, etc.).

4.14.2. Keep responsibly the Means of access and identification, e.g. the Mobile Devices and take all necessary measures against their damage, destruction, loss, alteration, theft, or use in any illegal way;

4.14.3. Take the necessary measures when storing biometric data in the Mobile Device (such as Fingerprint/Face ID) in order to prevent their unauthorized use, e.g. fraudulent use, by:

4.14.3.1. Use the Mobile Device only personally without giving it for use by third parties, e.g. children, parents, spouses, e.g. for use of biometric data functionalities;

4.14.3.2. Not keep biometric data of third parties in the Mobile Device and deleting all biometric data of third parties if any. In case of executed transaction with the biometric data of third party apart from the Authorized User, kept in the Mobile Device, the Bank shall deem the operation ordered by the Authorized User and shall not bear responsibility for any losses or damages caused thereby.

4.14.4. Check the address of the website accessed. If, upon entering the My Fibank electronic banking, the web address (URL) does not start with <https://my.fibank.bg> or the icon indicating secure connection is not displayed in the browser window, this means that the Authorized User has not accessed the site of My Fibank. In such case, there is a risk of coming across a website that aims to retrieve personalized security features or other identifying data (so-called phishing). The Authorized User should then immediately terminate access to that website and, if one or more of the personalized security features have already been entered, notify the Bank using the phone numbers listed in item 11.5.

4.14.5. In case the Authorized User has written down, or stored his/her personal means of authentication on an electronic, or another durable medium, thus creating prerequisites for their becoming known by third parties, or has communicated them to a third party, including to a family member or a relative, or has entered them on websites or through means of communication other than those specified in item 14.4. of these General Terms and Conditions, or has allowed use of the services provided through My Fibank by a third party other than the Authorized User, it shall be deemed that the Authorized User has acted intentionally or with gross negligence and the Bank shall not be responsible for any illegal actions of third parties involving unauthorized access to My Fibank that have caused damage to the Authorized User.

4.14.6. read and abide by the storage rules and security measures provided upon registration of the two keys – public and private, when using the API Integration service.

4.15. The personalized security features such as Username, Password, PINt, can be changed through My Fibank repeatedly by the Authorized User with new combinations, known only to him/her. The Bank recommends that the Username, Password, and PINt are changed periodically.

V. PERFORMANCE OF SERVICES AND TRANSACTIONS THROUGH MY FIBANK

5.1. The Account Holder/Authorized User, duly registered for access to passive, respectively active banking, can receive information and details on balances and transactions of the accounts registered in My Fibank, as well as initiate and authorize (by placing orders/requests, etc.) active transactions through My Fibank without limitation, 7 days a week, 24 hours a day.

5.2. The Bank shall be entitled to determine limits for execution of payment transactions through My Fibank and the Mobile application as well as for operations initiated through TPP – accessible on the internet site of Fibank at www.fibank.bg. The Bank may introduce other restrictions, apply exceptions, as well as establish additional requirements, including procedural ones, when necessary due to requirements of the current legislation, or for the purpose of maintaining a level of security according to the technical standards, conditions and policies for electronic and mobile banking.

5.2.1. The Bank provides the option and recommends that Account Holders set limits for execution of payment transactions (per transaction, daily and weekly) by submitting a change request at an office of the Bank or through a third-party app.

Third party providers (TPPs)

5.3. In the event that the User uses payment initiation and/or account information services when his/her account is available online via other payment service providers (third party providers), including when giving consent for the execution of a payment transaction or a series of payment transactions through such providers, the User is informed in advance that by giving such consent he provides the TPP with the same access as if the account is accessed by the User himself.

5.4. By giving consent/instructions to a TPP, including for online transactions as part of the online payment process, or for payment initiation or retrieval of information about account balances and/or transactions (under the procedure established by the TPP), the User gives his express consent that this TPP, subject to the conditions under which it has identified itself and implements the legal requirements in its activity, accesses the User's accounts in Fibank accessible online and initiates payment transactions from them for the account of the User. In such cases, Fibank will accept any instruction/order received from the TPP as placed by the User.

5.4.1. By confirming in My Fibank of initiated by TPP request for consent through the used by the Account Holder means of access and identification, the Account Holder gives consent before the Bank that the accounts /current accounts/ chosen by him are to be accessible by TPP for the purpose of performing the Payment initiation and/or the Account information service.

5.4.2. Based on the consent of the Account Holder, the Bank provides the option TPP to be able to access information including on the balances and transactions on the account as well as to initiate payment on his behalf.

5.5. Users, before giving consent and/or instructions for initiating payments or retrieving information from their accounts, should take the due care and make sure that the TPP has the right to perform the Payment initiation and Account information services.

5.5.1. TPPs should provide Users in advance with information on their registration, office address, authorization, identify themselves as payment service providers, specify the supervising authority that supervises their activity. Each TPP should be duly registered or licensed to provide account information and/or payment initiation services. Users can obtain such information from the public registers maintained on the website of the Bulgarian National Bank at www.bnb.bg, respectively from the Register on payment and electronic money institutions

maintained on the website of the European Banking Authority (EBA) at <https://euclid.eba.europa.eu/register/>.

5.5.2. To facilitate making informed decisions on the use of third party service providers for account information and/or payment initiation purposes, Fibank shall provide Users with additional information on its website at www.fibank.bg.

5.6. Users normally have the right to withdraw their consent given to a TPP, and in some cases this can be done following the instructions of the Bank and the TPP. In case of doubt regarding the security of their accounts, Users should immediately contact the Bank pursuant to item 11.5. of these GTC.

5.7. The Bank shall not be responsible for any actions or inactions of the TPP (such as interruption or termination of the provision of the service), nor for any resulting damages. The Bank is not a party to the relationship between the User and the TPP. The fees charged by TPP are separate from the fees charged by the Bank.

5.7.1. If the payment transaction is initiated through a Payment initiation service provider, the burden shall be on the Payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

5.8. The Bank may deny the TPP access to the account/s of the User when unauthorized access or fraud is suspected, to which effect the User shall be advised in an appropriate manner, unless this is prohibited by law or for security reasons.

5.9. In case of failure to fulfill its obligations to the Bank, Users may not make objections based on their relations with third parties, including with TPPs.

Provision of Payment initiation and Account information services

5.10. Fibank provides the Account information service for the customers of My Fibank with rights for passive banking, as the customers with rights for active banking may use the Payment initiation service as well.

5.11. By choosing the Account information service and/or the Payment initiation service and by determining of an account (IBAN), serviced by other payment service provider the User gives his explicit consent Fibank to access the chosen by him account/s for the purpose of providing the requested services, confirmed by the provision of access by the Account servicing payment service provider.

5.12. When using the Account information service for an account maintained at other payment services provider, in the registration of the Account Holder in the electronic banking My Fibank a consolidated information for that account is displayed, including availability, transactions performed for certain period of time and other information, as it is provided by the Account servicing payment service provider. Fibank shall not be liable for the completeness nor the actuality of the provided information.

5.13. The Payment initiation service for an account, maintained by other payment service provider is performed as Fibank initiates payment on behalf and for an account of the User under indicated by the latter data and information (payee, IBAN, amount, etc.) up to the limits for transaction executions, established by the Account servicing payment service provider.

5.13.1. Fibank shall not be liable for Payment initiation, containing indicated by the User inaccurate or invalid data – IBAN, amount, payee, etc.

5.14. The Bank shall not be responsible for any actions or inactions of the Account servicing payment service provider (such as interruption or termination of the activity, inability to perform the services, technical difficulties or other), nor for any resulting damages. The Bank is

not a party to the relationship between the User and the Account servicing payment service provider. The fees charged by the Account servicing payment service provider are separate from the fees charged by the Bank.

API Integration Service

5.15. The Bank allows My Fibank users with active banking rights to register for the API Integration Service. Registration is made and confirmed by the Account Holder (for legal entities by the Authorized User – director/director materially responsible person), with the means of access and identification used for My Fibank. Upon registration, the Bank provides a pair of keys (public and private) for identification of the Account Holder/Authorized User upon each login (access) to the service. The keys can only be used by the Account Holder/Authorized User having made the registration above.

5.15.1. Authorized Users create transfer orders in their information system in the form of API requests. Before submitting requests to My Fibank, they should ensure that all data entered accurate and complete. Confirmation of transactions is made in My Fibank electronic banking, via the Authorized Users' means of access and identification, and subject to the rights granted to them.

5.15.2. Deregistration – Authorized Users may at any time deregister from the API Integration service by performing the following two steps:

- 1) deactivate the keys issued;
- 2) erase the same keys.

VI. BANK ACCOUNTS AND CARDS

6.1. A bank account can be opened through My Fibank in the name of the Account Holder, by him personally or by the Authorized User.

6.2. The Account Holder shall be entitled to perform active banking transactions on his accounts registered in My Fibank, regardless whether they were opened in an office of the Bank or through My Fibank .

6.3. Opening and maintenance of banks accounts, including opening of deposits through My Fibank , shall be carried out subject to the terms and conditions of the Bank for the respective account or deposit product, announced on the website of My Fibank and/or of the Bank, with which the Account Holder shall be required to acquaint himself before opening the account/deposit.

6.3.1. The Bank and the Account Holder agree that, on the order of the Account Holder and after confirmation by the „Sign“ feature, the requested account/deposit shall be opened in his/her name through My Fibank , according to the applicable policies and procedures of My Fibank , and shall be maintained subject to Bank's terms for the respective type of account/deposit and the applicable regulatory requirements. The account shall be considered opened under a valid agreement between the parties. At the discretion of the Bank, additional documents may be required under items 4.2 - 4.4. of the GTCPS.

6.3.2. By opening an account/deposit subject to the procedures of My Fibank and the conditions for access, identification and confirmation by electronic signature, the Account Holder confirms that he is familiar with the contractual terms of the Bank applicable to the account/deposit opened in his name, including with the terms and conditions for changing them, and the consequences of violating them, accepts them, and shall be bound by them under the electronically signed agreement.

6.4. Closing of a bank account at the request of the Account Holder shall be done by submitting a written order at an office of the Bank, under the terms and conditions of the GTCPS, or through My Fibank, according to the type of account and subject to the current conditions of the Bank, provided that all charges due to the Bank have been paid, and there are no other special provisions for closing the respective account.

6.5. Through My Fibank electronic banking, including through the Mobile

Application, Individual Account Holders with active banking rights may submit debit card applications, including for the issuance of Debit MasterCard PayPass kids/teen to the account of a parent in the name of a minor (with optional wearables), credit card applications (including for virtual cards) and enter remotely into agreements for the respective products. Debit cards may be issued to an existing account, or to a new account opened in a currency selected by the Account Holder.

6.5.1. Debit/credit card applications and agreements for the respective card or credit products shall be signed using the Hardware or Software Token used by the Account Holder in My Fibank electronic banking.

6.5.2. After following the My Fibank procedures for access, identification and confirmation by electronic signature and after confirming by the Account Holder that they are familiar with these GTC, the GTCPS, the General Terms and Conditions for the respective product and the procedure for change thereof, as well as with the consequences of violating them, that they accept them and shall be bound by them, the agreement for debit/credit card or for another credit product between the Account Holder and the Bank shall be considered concluded.

6.6. Unless otherwise provided in these GTC, the relationship between the Bank and the Account Holder in connection with opening, maintenance and closing of bank accounts, as well as in connection with the conclusion of agreements for debit cards and their use, shall be governed by the GTCPS as well as by the current specific General Terms and Conditions and agreements for the respective services.

Deposit Insurance

6.7. The funds in all accounts of the Account Holder, including in those opened through My Fibank, shall be insured by the Bulgarian Deposit Insurance Fund up to the amount and under the conditions provided in the Law on Bank Deposit Guarantee.

Active banking

6.8. All requested transactions (including payment orders in national and/or foreign currency) shall be performed under the terms and conditions set by the existing legislation, the GTCPS, and according to the specific arrangements with the Account Holder.

6.9. The Authorized User may order payments from the accounts of the Account Holder, provided that the Authorized User has a level of access with rights to dispose of the account, in accordance with the defined limits, if any, and up to the amount of funds available in the account.

6.10. To execute a payment transaction, the Authorized User shall submit a payment order drawn up in electronic form, with correctly entered unique identifier/IBAN identifying the account of the Payee and, if necessary, the business identification code of the payment service provider for the Payee (BIC), as well as any other information and details required for execution of the respective payment service. In case the data is derived from an automated information exchange system, the Account Holder shall be obliged to make sure in advance that such data is correct.

6.10.1. The Authorized User shall be obliged to double check the correctness and completeness of the data, to verify the recipient's name and account information, the amount and currency of the transaction, ensure that they are correct and match the order placed, and then confirm the requested transaction by signing the payment order with his chosen ES.

6.10.2. The Bank shall not be responsible for non-execution or incorrect execution of a payment transaction in case of inaccuracy of the unique identifier/IBAN of the Payee, and/or of other data required for its implementation, indicated in the payment order by the Authorized User.

Transfers by mobile number (Blink P2P)

6.10.3. Natural persons that are Authorized Users of My Fibank Mobile Application with active banking rights may register for the Blink P2P

service, which is provided through the Blink Mobile Lookup centralized service of BORICA AD and connects the account's IBAN with a mobile phone number.

6.10.4. Upon registration, Authorized Users shall indicate a mobile phone number (registered by them in Fibank) and the IBAN of current account kept in their name with the Bank which shall be used for Blink P2P transfers. The IBAN and mobile phone number shall be provided to BORICA AD for the purpose of executing Blink P2P transfers. Authorized Users shall confirm registration using their means of access and identification. In addition, the Bank shall send an SMS with a one-time code to their mobile phone number.

6.10.4.1. By registering for the Blink P2P service, Authorized Users accept that payment documents (orders, account statements) will contain a recipient's mobile phone number, which shall uniquely identify the recipient's account IBAN.

6.10.5. After registration, Authorized Users can make Blink P2P transfers from any of their accounts with the Bank to mobile phone numbers of individuals registered for the Blink P2P service, but can only receive transfers to the current account linked to their mobile number registered with the Bank.

6.10.6. When making a Blink P2P transfer, Authorized Users can select the recipient of the transfer from the Contacts list of their Mobile Device registered with My Fibank, or enter the recipient's mobile number themselves. After that they need to correctly fill in the required fields (amount, currency and reason for payment).

6.10.6.1. By confirming a Blink P2P transfer, Authorized Users assume responsibility for the accuracy of all details contained therein. Therefore, before confirming they should: 1) check the correctness of the recipient's names and mobile phone number; 2) check the amount and currency of the transfer.

6.10.6.2. Transfers shall be executed subject to the limits set per day/transaction or others, and provided there are sufficient funds on the account for the transfer amount and for the fees due, announced in the Tariff and/or on the Bank's website at www.fibank.bg.

6.10.7. By registering for Blink P2P, Authorized Users agree to receive transfers from any person registered for the service and authorize the Bank to credit their account linked to the registered mobile phone number with the amounts of any such incoming transfers.

6.10.8. Upon change of the mobile phone number or the IBAN of the account registered for the Blink P2P service, Authorized Users need to make a re-registration. Authorized Users shall notify the Bank immediately of any such change. The Bank shall not be responsible for damages or lost profits arising from late notification or failure to notify.

6.10.9. By registering for Blink P2P, Authorized Users consent that the Bank may access the Contact list (Contacts) on their registered Mobile Device, and agree that their personal data (names, telephone number, IBAN, photo and other necessary for using the service), may be provided to third parties, such as other registered persons and participants in the payment process.

6.10.9.1. Upon registration and consent, the Blink or Fibank logo may be visible to other users of the service.

6.10.10. De-registration: Authorized Users can de-register at any time from Blink P2P via the My Fibank Mobile Application.

6.10.11. With respect to Blink P2P instant transfers, all terms and conditions shall apply set out in these GTC and in the GTCPS.

6.11. For execution of a payment order, the Account Holder/the Authorized User shall provide the Bank in advance with copies of all supporting documents for the order requested by the Bank and under the current legislation by e-mail, in the form of scanned documents. The Account Holder shall provide the Bank with the original documents or with attested cop-

ies thereof within 7 days of ordering the transaction.

6.12. The required documents (declarations and others) that need to be provided by the Account Holder for execution of the ordered transaction under the current legislation, shall be compiled electronically, and submitted in the manner provided for submission of payment orders through My Fibank and in accordance with the requirements of the Bank.

6.13. The Account Holder/the Authorized User may create, save and use templates of electronic payment forms, containing one or more commonly used details, in order to facilitate the completion of payment orders through the My Fibank system.

6.13.1. Upon registration for payment of tax and credit obligations, the individual Account Holder shall receive information about, and be able to pay only his own obligations. The information about them shall be periodically updated through an automated information exchange system.

6.14. The Account Holder shall be obliged to ensure sufficient available funds on the account for execution of the ordered payment transactions, and for payment of the charges due for their execution.

6.15. Payment orders shall be executed on the date of their receipt, unless another date for execution has been agreed, subject to the procedures, terms and value dates under the GTCPS.

6.15.1. Blink instant transfer orders (with „approved“ status) shall be executed immediately upon receipt, provided that the payment service provider of the Payee is accessible through the instant payment system.

6.15.2. The Bank shall not be responsible for transfers not executed due to inaccessibility of the respective payment service provider through the instant payment system or to processing failure by other participants in the payment process.

6.16. When payment of tax obligations is initiated, such obligations shall be paid, for each particular type, (e.g. taxes, fines, etc., along with the interest accrued thereon) in the order of their occurrence. Partial payments of tax obligations shall not be performed.

6.17. Payment orders received on behalf of the Account Holder/the Authorized User through My Fibank according to the rules and procedures established by the Bank shall be considered validly submitted written statements that unconditionally bind the Account Holder. The Bank shall not be responsible for any damages or lost profits resulting from their implementation.

6.18. The Account Holder/the Authorized User shall be obliged to check the status of implementation of the payment orders initiated by him, and give timely alert in case of any identified discrepancies. An order with „approved“ status shall be deemed accepted for implementation by the Bank, and may not be cancelled through My Fibank (the procedures for cancellation of orders referred to in GTCPS shall apply).

6.19. The Bank shall send Push Notifications in the Authorized User profile in My Fibank electronic banking, including in the Mobile Application, for all Blink instant transfers: executed, received or failed.

VII. REFUSAL FOR EXECUTION OF PAYMENT TRANSACTION

7.1. The Bank shall refuse the execution of a payment transaction ordered through My Fibank, if the requirements of these GTC, the GTCPS or the specific agreed terms with the Account Holder are not met. The Bank shall refuse the execution of payment transaction when invalid or incomplete identifier (IBAN) is indicated, when there is no sufficient available balance on the account for execution of the transaction and for payment of the charges due to the Bank.

7.1.1. The Bank shall not be responsible for damages resulting from non-execution of payment transactions due to insufficient funds, non-fulfillment of the applicable rules and requirements or the agreed terms, or in case of transactions inadmissible under current legislation,

including in connection with the measures against money laundering and terrorism financing.

7.2. The Bank shall notify the Authorized User of its refusal (by a “wrong” status in “Ordered documents” menu, e.g. by Push Notification message in “Notifications” menu – unless the option is explicitly deactivated by the Authorized User), and upon request of the Account Holder shall inform him of the reasons for the refusal and how to correct the errors (in case non-execution was due to errors), unless there is a ban on the provision of such information under a law or act of the European Union.

VIII. REPORTING

8.1. The Bank shall prepare and provide the Account Holder, as well as the Authorized Users specified by the Account Holder, with written account statements and other accounting information (statements, confirmations, etc.), with information on the transactions performed with bank cards, balances, and transactions on bank accounts, making them available through My Fibank.

8.2. The Account Holder agrees to receive the statements and other documents and information under item 8.1. above in the manner stipulated under these GTC, without the Bank having the obligation to provide them on paper.

8.2.1. The Bank shall make the statements available on the date of their preparation, indicated in the document, which parties shall accept as the date of their receipt.

8.2.2. The Bank shall provide the Account Holder/Authorized User with access to statements for past periods, storing them in the System for at least 6 (six) months after their preparation.

8.2.3. The Account Holder shall be obliged to archive the documents received on his own durable medium, for a period sufficient for his information purposes.

8.2.4. By registering into My Fibank, the Account Holder gives his express consent that the Bank ceases to provide him with paper statements (account statements), including in an office of the Bank, or by mail. Change regarding the above mentioned is possible by signing a request in an office of the Bank. The Account Holder could opt out of receiving bank card statements from the cards settings in the electronic banking My Fibank. At the request of the Account Holder, the Bank shall provide him with duplicates subject to charges under the Tariff.

8.3. The Account Holder shall be obliged to review the contents of the received reporting information immediately, and inform the Bank of any discrepancies found without undue delay, under the terms and conditions for submitting complaints pursuant to the GTCPS.

8.3.1. If the Bank does not receive a written objection within 45 days from the execution date of a transaction, it shall be considered that the Account Holder has received and approved the reporting documents and the payment services connected with that transaction. Notifying the Bank after this period shall be considered undue delay on behalf of the Account Holder.

8.4. The Account Holder/Authorized User may indicate in the System more than one email address for receipt of statements. The indication of addresses of third parties shall be entirely the responsibility of the Account Holder and shall be considered valid authorization of the Bank to send the data and information contained in the statements (representing banking secrecy and personal data) to the addresses indicated.

8.5. The Account Holder confirms that he is aware of, and assumes the risks associated with transmission of data in the Internet environment, of the possibility of unauthorized access and disclosure of information to third parties, of alteration of the contents or technical omissions in the transmission of data and information in unencrypted form, protected only by password.

IX. CARD DIGITIZATION THROUGH THE MY FIBANK MOBILE APPLICATION

9.1. The conditions for card digitization are: the Authorized User to be registered for active banking (e.g. banking with limited access to active transactions pursuant to item 4.1.5. of these GTC) in the My Fibank Mobile Application or to have activated Mobile Application with built-in Software Token; to hold a plastic card (except for Maestro and V PAY) issued by the Bank or Virtual Card in accordance with the General Terms and Conditions of First Investment Bank AD for issuance and use of revolving international credit cards Mastercard and VISA or the GTCPS; the Mobile Device to be registered with the Mobile Application (to have a registered ID number) or the Authorized User to have activated Mobile Application with built-in Software Token; the Mobile Device software to meet the technical requirements and to be standardized for work with a Digitized Card.

9.2. By selecting a card from the list in the My Fibank Mobile Application and confirming the request for card digitization with an ES, the Authorized User places an express Request to the Bank to digitize the selected card, which card shall be used under the Agreement for the card, entered into between the user and the Bank under General Terms: the GTCPS (for digitized debit cards), these GTC, respectively the General Terms and Conditions of First Investment Bank AD for issuance and use of revolving international credit cards MasterCard and VISA (for digitized revolving international credit cards), and fees and commissions under the current Tariff, which the Account Holder has read and understood and accepts their application in governing his relations with the Bank in connection with the request for and use of the Digitized Card.

9.3. By sending by the Bank to the Authorized User, through the Mobile Application, of a notification that the Request has been executed and the card has been digitized, the Digitized Card Agreement shall be considered entered into.

9.3.1. In the case of a Digitized credit card, the Agreement under the preceding paragraph shall form an integral part of the Agreement for issuance of a revolving international credit card (including Virtual Card) and granting of a credit limit (overdraft) on a current account, and in the case of a Digitized debit card (including Virtual Card) – of the Agreement for granting of a bank credit-overdraft on a current (card) account to individuals, when such an agreement has already been concluded.

9.4. The Digitized Card shall have the same personal identification number (PIN) as the plastic card or the Virtual Card. The PIN is a combination of at least four digits and is used to identify the Account Holder when performing transactions with the Card.

9.4.1. In the case of loss, theft, destruction, damage or sale of the Mobile Device, the Authorized User may submit a new card digitization request, which shall be considered by the Bank subject to charges under the Tariff.

9.4.2. In the case of loss of the plastic card, the Bank shall issue the Authorized User a new plastic card with a new PIN, respectively digitize it, upon request by the Authorized User.

9.5. For any matters not settled in this section, as well as regarding the conditions for use, maintenance, management and termination of the Digitized Card Agreement, the GTCPS (for digitized debit cards), respectively the General Terms and Conditions of First Investment Bank AD for issuance and use of revolving international credit cards MasterCard and VISA (for digitized revolving international credit cards) shall apply.

9.6. The Bank may refuse card digitization, including where the Mobile Device has the necessary technical parameters, without giving a reason for that.

9.7. The ordering of a payment, or of any other transaction with the Digitized Card before the expiry of 14 days from the conclusion of the Agreement for it, shall be considered as express consent of the Account Holder for the Bank to begin implementation of the Agreement.

X. BLOCKING OF ACCESS

10.1. The access to My Fibank, including to the Mobile Application and the API Integration service, may be blocked by the Bank in the following cases:

10.1.1. at the request of the Account Holder or the Authorized User, pursuant to item 11.5. below, without them having to specify a particular reason for that;

10.1.2. on the initiative of the Bank – for objective reasons related to the security of the identification data, or in case of reasonable suspicion of payments submitted through My Fibank, including through the Mobile Application, which have not been authorized by the Account Holder, or in case of significantly increased risk that the Account Holder may not be able to meet their obligations to the Bank;

10.1.3. on the initiative of the Bank – for the Account Holder/the Authorized User who, with their actions, violates the requirements of the existing regulations, of these GTC and/or the GTCPS, who threatens the security and proper functioning of the System, or threatens or obstructs the use of the services by other customers;

10.1.4. automatically - following a series of wrong attempts to enter a TAN, PINt, Password, or other personalized security features as specified in the Operating instructions.

10.2. In the cases under item 10.1.1. the Bank shall block the access within the time necessary for processing the request, but not later than 2 hours from its receipt, unless for objective reasons a longer period is required.

10.3. The Bank shall notify the Account Holder of the blocking of access in the cases under items 10.1.2. and 10.1.3. and of the reasons for that prior to the blocking if possible, or at the latest immediately thereafter, unless giving such information is not allowed for security reasons or due to compliance with regulatory requirements.

10.4. Unblocking of access shall be made by the Bank after elimination of the grounds for blocking, and where the blocking was made upon the initiative of the Account Holder/the Authorized User – based on a request for unblocking submitted by the Account Holder, after fulfilling the requirements in the Operating instructions and payment of a fee according to the Tariff.

10.5. The Bank shall not be responsible for damages arising as a result of blocking of access under this section.

XI. RESPONSIBILITIES

11.1. The Bank shall not control the purpose, nor shall it monitor the lawfulness of the transactions underlying the payments executed under these GTC, unless otherwise provided by law, nor shall it be responsible for damages, or for resolving of disputes arising in connection with such transactions.

11.2. The Account Holder/the Authorized User shall be responsible for damages caused by them directly or indirectly to the Bank, related to unauthorized access to information or making of payments through My Fibank, to non-compliance with the banking requirements, or to use of My Fibank services in a way that is improper, illegal, or contrary to these GTC.

11.3. In case of breach of his/her obligations to the Bank in connection with the use of My Fibank, the Account Holder may not make objections based on their relations with third parties, including TPPs.

11.4. The Account Holder/the Authorized User shall be responsible for any attempts on their part to gain unauthorized access to other customers' registrations or information.

11.5. The Account Holder/the Authorized User shall be obliged to immediately notify the Bank upon doubt that a third party has learned, or might learn their Username and Password/PINt and/or the personalized secu-

city features of a means for access and identification, and request blocking of access to My Fibank or of the means for access (if the means allows blocking). The notification shall be made in person at an office of the Bank, or by calling the following telephone numbers:

0700 12 777

+359 2 800 2700

+ 359 2 818 0003

In case of change of the above telephone numbers, the Bank shall notify Account Holders/ Authorized Users by an announcement on the Bank's website at www.fibank.bg and through My Fibank, at <https://my.fibank.bg>.

11.5.1. The Bank shall not be responsible for any damages if it has received an incorrect notification by a person who, on the basis of unambiguous circumstances, has been authorized to make it, and the Bank, acting in good faith, has taken the necessary measures to protect the interest of the Account Holder by blocking the access and not executing payment transactions ordered through My Fibank .

11.6. The Account Holder shall bear all losses, regardless of their size, relating to unauthorized payment transactions resulting from improper use of My Fibank in the cases of item 4.14. above, as well as all losses caused by him, or by an user authorized by him, through fraud or through failure to fulfill of one or more of the provisions of these GTC, the security measures set out in the Operating instructions, including the measures for protection of the means of access and identification, which shall be considered gross negligence.

11.6.1. Until receipt of the notification under item 11.5. the User, who is a consumer, shall bear limited liability pursuant to GTCPS, and after receipt of the notification and blocking of the access, the User shall not be liable for any damages, unless he has acted fraudulently, in which case he shall be liable for all damages.

11.7. The Account Holder and the Authorized Users shall notify the Bank immediately upon detection of delay, malfunction, or failure to receive information, as well as provide assistance to the Bank for preventing and limiting damages in the way indicated by the Bank.

11.8. The Bank shall provide information on the website of My Fibank at <https://my.fibank.bg> on the appropriate measures to enhance security. The Authorized Users of My Fibank shall check regularly for information and warnings to enhance security, and implement them.

11.9. Bank shall not be responsible for damages and lost profits due to inaccuracies, errors or delays in the transmission of information due to force majeure, technical, communication or other reasons beyond the Bank's control, or for the continuity of access to My Fibank .

XII. INTERESTS, FEES AND COMMISSIONS

12.1. For the use of the Bank's services through My Fibank , the Account Holder shall owe fees and commissions as per the GTCPS and the Tariff.

12.2. The interest accumulated on the balances of the Account Holder's accounts shall be calculated and accrued under the GTCPS, and announced in the Interest Bulletin.

12.3. In connection with the registration and use of My Fibank , as well as the use of other banking services related to the implementation of rights and obligations of the parties under the Agreement and these GTC, the Account Holder shall owe the Bank fees and commissions under the GTCPS and the Remote Banking section of the Tariff effective on the due date.

12.4. The terms and conditions for amending and supplementing the Tariff and the appendices thereto shall be governed by the GTCPS.

12.4.1. Changes in interest rates and exchange rates shall be applied in accordance with the GTCPS.

12.5. The Bank shall have the right to officially collect all amounts due to

it by the Account Holder, including fees and commissions, from any account in the Account Holder's name kept with it, under the terms and conditions of the GTCPS.

XIII. COMMUNICATION

13.1. All communication, including notifications between the parties, shall be made in writing, including to the e-mail addresses of the parties specified in the registration, unless another way of notification is expressly provided by these GTC.

13.2. In case of change of the address and/or other details provided by the Account Holder, the latter shall be obliged to notify the Bank within 7 days of the change. Otherwise, all notices, invitations and messages sent by the Bank to the previous address of the Account Holder shall be deemed served.

13.2.1. In the event of legal proceedings in a dispute arising in connection with the conclusion, performance, interpretation, or termination of the Agreement or these GTC, the addresses of the parties stated in the Request shall be considered as addresses for service of summons and court messages within the meaning of the Civil Procedure Code, unless either party has expressly notified the other party of a change of address.

XIV. CHANGES IN THE GTC

14.1. The Bank shall provide Users with information about upcoming changes to these GTC, notifying them in advance, at least 2 (two) months before such changes take effect, and providing the full version of the new GTC. The Bank shall also provide Users with advance information about changes to the GTC within the above-mentioned period on its website at: www.fibank.bg, section „Upcoming changes to the Tariff and General Terms and Conditions”, as well as in My Fibank electronic banking, „Notices” menu.

14.1.1. The upcoming changes and the new GTC shall be provided in an accessible form that enables unchanged reproduction, allowing Users to store them for an unlimited period, as well as to print them out for record-keeping purposes and future reference.

14.2. Notifications of changes may be sent via email, SMS/Viber message, or letter, to the last correspondence/email address or mobile phone number of the User registered with the Bank, including by push notifications for Users of the My Fibank Mobile Application, or in another appropriate manner. The Bank shall provide information about upcoming changes, as well as the new General Terms and Conditions, to My Fibank electronic banking Users, in the „Notices” menu. Users can also receive them in paper form upon request, at an office of the Bank.

14.3. For Users that are not consumers it shall suffice that information about upcoming changes is provided, in the above form and timeframe, in the „Notices” menu of My Fibank electronic banking, and on the Bank's website: www.fibank.bg, section „Upcoming changes to the Tariff and General Terms and Conditions”, or in another agreed manner.

14.4. In case that an Account Holder, who is a consumer, disagrees with the changes, he/she shall have the right to immediately terminate the Agreement (without owing any penalties or compensation in connection with termination due to amendments in these GTC) prior to the date on which the changes are proposed to take effect, by a written request without notice, pursuant to Section XV, after having repaid in full their obligations to the Bank. If the Account Holder does not terminate the Agreement by the date of entry of the changes into force, it shall be considered that the Account Holder has accepted them and is bound by them. In its notifications, the Bank shall inform Users to that effect.

14.4.1. In the event that a User, who is not a consumer, disagrees with the changes, the Agreement shall terminate in accordance with Section XV below.

14.5. Changes in the GTC related to legislative changes or to extending the scope of the services, as well changes in the charges and/or conditions of the payment services provided, when more favorable for the users, shall apply immediately and without prior notice.

XV. TERM OF THE AGREEMENT, TERMINATION

15.1. The Agreement is concluded for an indefinite period of time.

15.2. The Agreement shall be terminated:

15.2.1. By written request of the Account Holder, without notice, provided that there are no unpaid obligations to the Bank and, in case of termination of the Agreement before the expiry of 6 months from the date of its conclusion – after payment of a fee under the Tariff; Account Holders who are not consumers shall be charged a fee under the Tariff;

15.2.2. At the request of the Bank – unilaterally, with 30 (thirty) days' notice, and when the Account Holder is a consumer – with 60 (sixty) days' notice, addressed to the Account Holder on paper or on another durable medium, after expiry of the notice.

15.3. Upon termination of the Agreement, the Account Holder shall be obliged to pay all charges due to the Bank. Monthly charges which are paid after the beginning of the month for which they were due, shall not be considered prepaid. Charges prepaid by an Account Holder who is not a consumer shall not be refunded.

15.4. The Bank shall be entitled to unilaterally terminate the Agreement without notice to the Account Holder due to occurrence or ascertainment of the occurrence of any of the circumstances indicated below, namely: upon inclusion of the Account Holder/Authorized User in sanctions lists, including of the UN Security Council, the European Union, the Office of Foreign Assets Control (OFAC) of the U.S. Treasury Department, the Ministry of Finance or the National Revenue Agency of the Republic of Bulgaria, or in other restrictive lists, including under the Law on Measures against Money Laundering or the Law on Measures against Terrorist Financing; due to use of the electronic banking for non-legitimate purposes or fraudulently, as well as when the Account Holder/Authorized User with its actions threatens or precludes the use of services of other clients, incl. for attempting to obtain unauthorized access to other clients' registrations and information, as well as for provision of false information for the registration for "My Fibank", when the provision of the correct information would have led to a refusal of registration. Upon termination of the Agreement under this item, the Bank shall not owe to the Account Holder a refund of any prepaid charges.

Upon termination of the Agreement under this item, the Bank shall not owe to the Account Holder a refund of any prepaid charges.

15.5. Termination of the Agreement shall not automatically lead to closure of the accounts, including the deposits, opened through My Fibank, unless the Account Holder expressly requests their closure under the terms and conditions specified by the Bank, or the Bank closes them on its own motion, pursuant to the GTCPS.

15.6. The Account Holder shall be entitled, without owing a compensation or penalty and without giving a reason, to withdraw from the Agreement for My Fibank and/or for the Mobile Application when they were concluded remotely, whereby the Account Holder shall be deemed also to have automatically withdrawn from the Digitized Card Agreement, or to withdraw only from the Digitized Card Agreement concluded remotely via the Mobile Application, by depositing at an office of the Bank, or sending by mail or courier a written notice to the Bank to the correspondence address indicated in the registration, or at the Headquarters of the Bank at 1797 Sofia, 37 Dragan Tsankov Blvd., within 14 calendar days from the date of conclusion of the Agreement.

15.6.1 The withdrawal of the Account Holder from the Agreement for My Fibank and/or for the Mobile Application shall enter into force

and the Agreement shall be terminated provided that notice was made within the period and under the conditions of item 15.6., and the Account Holder has paid the Bank the services provided and the fees due under the Agreement.

XVI. ADDITIONAL PROVISIONS

16.1. Unless otherwise provided in these GTC or the specific arrangements between the parties, the relations between the Bank and the Account Holder in connection with the use of the payment services and the other related services offered by Fibank through My Fibank, including the opening and maintenance of bank accounts, the issuance of bank cards, the provision of credit products, the authorization and execution of payment transactions, the cancellation of payment transactions ordered by the Account Holder, possibility for corrections, and the other rights, obligations and responsibilities of the parties, shall be governed by the GTCPS, the General Terms and Conditions for the respective product/service, the Tariff and the appendices thereto, which shall form an integral part of the Agreement.

16.2. The records kept by the Bank of the orders for execution of payment transactions or other transactions, and of the other information submitted in the form of electronic statements through My Fibank, shall be considered as definitive proof of their content, as well as of the time of their submission, or execution. The records made by the Bank of the transactions through My Fibank are accounting documents under the Accountancy Act, and shall be considered true until proven otherwise.

16.3. As a controller of personal data, First Investment Bank AD shall act in compliance with the legislation of the European Union (EU) and the Republic of Bulgaria, including with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR), effective 25.05.2018. Personal data of clients shall be lawfully processed in the presence of at least one of the conditions under Art. 6, para. 1 of the GDPR.

The Bank shall provide to each client a document containing the information on processing of personal data required by law and under Articles 13 and 14 of GDPR, as well as personal data protection information for users of payment services and bank cards. Where necessary, the Bank shall update the information provided. The latest version shall be made available on paper or other durable medium at any time in the Bank's offices and on the website of First Investment Bank AD at www.fibank.bg.

XVII. DISPUTE RESOLUTION. APPLICABLE LAW

17.1. Any disputes arising between the parties in connection with the execution or interpretation of the Agreement and these GTC shall be resolved by mutual consent. Fibank shall provide the option of filing a written complaint at any of its bank offices, as well as electronically, under the Client Complaint Procedure published on its website at www.fibank.bg. Any data and documents substantiating the merits of the complaint should be attached to it. With a view to objective handling of complaints, resolution of disputes and correction of any errors, the Bank may request additional data and documents.

17.1.1. The Bank shall process the complaint and notify the Account Holder in writing of its decision within 15 (fifteen) working days of receipt of the complaint, unless it becomes necessary to extend this period, to which effect the User shall be notified in writing.

17.1.2. In the event that the Bank does not issue a decision on the complaint within the prescribed period, including where such period is extended, as well as in the event the User disagrees with the Bank's decision, the User may refer the dispute to the Conciliation Commission for Payment Disputes to the Consumer Protection Commission at the following address:

1000 Sofia, 1 Vrabcha Street, floor 4, phone: +359 2 9330577, website: abanksb.bg/pkps

or, for agreements concluded online, use the Online Dispute Resolution (ODR) platform at:

<http://ec.europa.eu/odr>.

17.2. For any matters not covered by the Agreement, these GTC, the GTCPS and the terms and conditions for the specific payment service, the relevant regulations of the current Bulgarian legislation shall apply.

17.3. In the event that mutual consent cannot be reached, either party may refer the dispute for resolution to the competent Bulgarian court.

17.4. Should any provision of these GTC be, or become invalid, this shall not affect the validity of the remaining provisions of these GTC.

XVIII. FINAL PROVISIONS

18.1. All rights and obligations of the Bank and the Authorized User in relation to the Card used by the latter shall be governed by the General Terms and Conditions of Fibank applicable to the respective Card, regulating the issuance and use of bank cards.

18.2. The General Terms and Conditions for opening and maintenance of bank accounts and provision of payment services, the General terms and conditions of First Investment Bank AD for electronic deposit My Deposit, the Operating instructions for the My Fibank system, the Tariff of fees and commissions of Fibank, and the appendices thereto shall form an integral part of these GTC.

18.3. With regard to the existing agreements for use of Internet banking concluded with Unionbank EAD prior to its merger with First Investment Bank AD (04.03.2014), the Bank and the Account Holder accept that the persons authorized by the Account Holder under the conditions and requirements of Unionbank EAD will continue to operate and have the same rights as the persons authorized under item 4.1.2. of these GTC persons declared to the Bank for a period announced by the Bank.

18.4. These General Terms and Conditions have been drawn up pursuant to Art. 298 of the Commerce Act, amended and supplemented by resolution of the Management Board of First Investment Bank AD effective 04.03.2025.