

GENERAL TERMS AND CONDITIONS OF EUROBANK BULGARIA AD FOR ELECTRONIC BANKING SERVICES "INTERNET BANKING" FOR INDIVIDUAL AND CORPORATE CLIENTS

I. SUBJECT

1. (Amended, in force as of 12 September 2018) These General Terms and Conditions (hereinafter "General Terms and Conditions") regulate the relations between Eurobank Bulgaria AD, registered with the Commercial Register, UIC 000694749, having its seat and registered office at: 260 Okolovrasten Pat Str., Vitosha District, Sofia, website: www.postbank.bg, e-mail: info@e-postbank.bg, holder of License No. Б 05 / 2 April 1991, issued by the competent supervisory authority, namely: Bulgarian National Bank (www.bnb.bg), and the Account Holder, to whom access is provided through the Service, as well as the relations between the Bank and the Authorized Holder in the course of the provision and use of the Service, in compliance with the terms and conditions of the Agreement for the Provision and Use of Internet Banking Service entered into by and between the aforementioned parties.

2. (Amended, in force as from 12 September 2018) These General Terms and Conditions shall constitute an integral part of the Agreement for the Provision and Use of Internet Banking Service. For the avoidance of any doubts, for all cases not settled in these General Terms and Conditions and the Agreement for the Provision and Use of Internet Banking Service, the relevant general terms and conditions of the Bank for the specific account and the concluded agreement for the bank account requested to be accessed through the use of the Service shall apply.

II. DEFINITIONS

1. (Amended, in force as of 14 September 2019) "**Internet Banking Service**" or "**Service**" only – provision by the Bank to the Authorized Holder of access to the funds maintained on the Account(s) by technical means of communication used by the Authorizations Holder and described in these General Terms and Conditions, as well as provision of an option to perform other operations and/or transactions ordered by the Authorized Holder, including by electronic bank payment order, and described in these General Terms and Conditions.

2. "**Agreement for the Provision and Use of Internet Banking Service**" (hereinafter referred to as the "Agreement") – a written document (including a contract, request, data and other documents bearing the signatures of the parties and specifying their rights and obligations under the Internet Banking Service, including the annexes and addenda thereto), signed by the Bank and the Authorized Holder, who is also the Account Holder, or between the Bank, the Authorized Holder and the Account Holder, when the Account Holder entitles the Authorized Holder to dispose of the cash on the Account Holder's account(s) by using the Internet Banking Service.

3. **The "Bank"** – Eurobank Bulgaria AD, registered with the Commercial Register, UIC 000694749, with seat and registered office at: 260, Okolovrasten Pat Street,

Vitosha District, Sofia, providing the Service pursuant to the concluded Agreement and these General Terms and Conditions.

4. (Amended, effective as of 16 July 2018) "**Account Holder**" – a natural person with legal capacity or legal entity that has concluded an agreement with the Bank for any of the following services: bank account; bank payment card and/or loan agreement. In case the Account Holder is a legal entity acting through a proxy, the actions to be performed by it pursuant to these General Terms and Conditions shall be performed by its legal representative(s) or natural persons - proxy(-ies), respectively, according to their relevant scope of representative power.

5. "**Authorized Holder**" – a natural person with legal capacity, who, according to the Agreement, is entitled to access and/or dispose of the funds available on the Account, up to the available amount and the limit set on the Account by using the Service. In the cases where pursuant to the Agreement (including any concluded annexes/addenda thereto) the Account Holder has indicated more than one Authorized Holder, the provisions of these General Terms and Conditions concerning the Authorized Holder shall apply to each of the Authorized Holders accordingly.

6. (Amended, in force as of 12 September 2018) "**Account**" – any account opened with the Bank under a bank account agreement concluded with the Account Holder, the access to which the Account Holder has explicitly specified in the Agreement. With regard to the rights and obligations of the Parties in relation to each specific Account, the rules of the respective bank account agreement shall apply, including the respective general terms and conditions of the Bank thereto.

7. (Amended, in force as of 8 May 2021) "**Digital Certificate**" - a technical means, issued by the Bank, certifying the authorship of electronic documents for the purposes of the electronic identification of the Authorized Holder when using the Service. As of 8 May 2021 the Bank does not issue or accept digital certificates as means of certifying the authorship of electronic documents.

8. (Amended, in force as of 12 September 2018) "**Qualified Electronic Signature (QES)**" – electronic signature within the meaning of Article 3(12) 12 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("Regulation 910/2014");

9. (Amended, in force as of 8 May 2021) "**Activation code**" - code for the activation of the Service upon signing up to the Bank's Internet Banking System.

10. (Repealed, in force as of 8 May 2021).

11. "**Access code**" combination of username and password for access to the "Internet Banking" system.

11.a. (Amended, in force as of 14 September 2019) "**Website**" - the Bank's website available at:

www.postbank.bg or <https://e-postbank.bg>, through which the Bank provides access to the Authorized Holder to the Service.

12. (Amended, in force as of 14 September 2019) "**Mobile banking**" ("**m-Postbank**") - special application for mobile devices, providing access to an Authorized Holder to the Service via a mobile device.

13. (Amended, in force as of 8 March 2019) "**Mobile banking code**" – Personal Identification Number (PIN code) generated by the Authorized Holder. It should be entered to log in to the Mobile banking application and is equivalent to "Access code" and "Biometric data".

14. (Amended, in force as of 14 September 2019) "**Biometric data**" – personal data related to physical, physiological or behavioural characteristics of the Authorized Holder, registered as a result of specific technical processing through the capabilities of the operating system of the mobile device used (fingerprint, facial recognition), which allow or confirm its biometric identification, and can therefore be used to log in and access the functionality of the Mobile banking ("**m-Postbank**") application, which is equivalent to "Access code" and "Mobile banking code", as well as for unlocking and providing access to the functionalities of the **m-Token Postbank** application.

15. The "**Parties**" – the Bank and the Account Holder, in the cases where the latter is also an Authorized Holder; or the Bank, the Account Holder and the Authorized Holder, in the cases where the Account Holder entitles the Authorized Holder to dispose of the funds available on the account by using the "Internet Banking" service.

16. (New, in force as of 14 September 2019) "**Software Token**" ("**m-Token Postbank**") is an application for mobile devices (smartphones) with Android or iOS operating system, which serves to verify the identity of the Authorized Holder and to confirm the consent for the execution of electronic remote payment and non-payment transactions performed through the "Internet Banking" Service and/or through other digital channels for remote access. It is activated at the request of the Authorized Holder through the "Internet Banking" Service, including through the Internet Banking Basic Functionality. The access to the application is provided by means of a PIN defined for the Software Token by the Authorized Holder or using Biometric data. The Software Token is not possible to be installed on more than one device at a time. The activation of the Software Token on a new device automatically deactivates the Software Token on the device currently used.

17. (Amended, in force as of 8 May 2021) "**Personalized Security Tool**" (**PST**) – additional method of identification (*in addition to the basic ones - Access code, Mobile banking code or Biometric data*) - Software Token, Qualified Electronic Signature (QES), one-time code received via SMS or other electronic message to a mobile phone number) provided to the Bank under the Agreement, or a combination of two or more of the above methods.

18. (New, in force as of 14 September 2019) "**Push Notification**" is a notification in the form of a short

message sent by the Bank to the Authorized Holder and displayed on the screen of the mobile device on which the m-Token Postbank application is installed and activated. It informs the Authorized Holder that a transaction is being executed that requires the confirmation of the Authorized Holder and the latter has to unlock m-Token Postbank and confirm it. The notification contains information about the transaction required to be confirmed.

19. (New, in force as of 14 September 2019) "**QR Code**" is a matrix barcode in the form of a square with black modules on a white background, which encodes information that is visualized when scanning the code with a mobile device equipped with a camera. The QR code is used to encode the information for a specific transaction performed through e-Postbank and for its reading by m-Token Postbank.

20. (New, in force as of 14 September 2019) "**Internet Banking Basic Functionality**" – a service provided by the Bank, allowing remote online access to information on balances and transactions on payment accounts and information on other products and services provided by the Bank, without the option to initiate and execute remote electronic payment transactions. It is provided upon online registration in compliance with the Bank's General Terms and Conditions for opening, keeping and closing bank accounts of n p.

21. (New, in force of 30 August 2021) "List of Trusted Recipients" – a list of names of persons and their payment account/card number, which can be created after login and identification in Internet Banking Service ("e -Postbank") with an Access Code, or respectively login to Mobile Banking ("m-Postbank") with a Mobile Banking Code or Biometric Data, strong authentication via Software Token ("m-Token Postbank"), and then the execution of electronic remote payment transactions to persons on the list shall be without the need for confirmation with Software Token or in any other manner provided for in these General Terms and Conditions.

22. (New, in force as of 30 August 2021) "Low-value transactions" – remote electronic payment transaction, the amount of which does not exceed the equivalent of BGN 58, as well as where the cumulative sum of previous remote electronic payment transactions initiated by an Authorized Holder does not exceed the equivalent of BGN 195 as from the time of the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions or the number of previous consecutive remote electronic payment transactions initiated by an Authorized Holder does not exceed five as from the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions.

III. GENERAL PROVISIONS

1. (Amended, in force as of 8 March 2021) The Account Holder who wants to use the Service shall enter into a Service Agreement after reviewing these General Terms and Conditions. Where the Account Holder is a natural

person, the Agreement, as well as any additional agreements or annexes thereto, if any, shall be signed only in person by the Account Holder. Where the Account Holder is a legal entity, it may be represented through its legal representatives or through their proxy, in which case the Bank shall accept only the following powers of attorney:

1) Power of attorney with notarized signature or signature and content certified by (a) Bulgarian Notary Public after May 2016 or (b) certified by a Bulgarian diplomatic or consular mission abroad and submitted to the Bank for the first time within 1 (one) year since the date of its certification;

2) (Amended, in force as of 14 September 2019) Power of attorney in the form provided by the Bank, signed simultaneously by the legal representatives of the Account Holder and the authorized person before a Bank's officer, for which a fee is due according to the Bank's Tariff.

A power of attorney, which is not in the form provided by the Bank, regardless of whether it is with notarized signature or signature and content or is signed before a Bank's officer, should contain an explicit statement of intent to use the Service on behalf of the Account Holder and the proxy must have at least the following powers: to conclude a Contract for the Internet Banking Service under the terms and conditions offered by the Bank and to fill in and sign all documents required by the Bank in this regard, including, but not limited to: General Terms and Conditions for Electronic Banking Service, Application for Internet Banking Registration, Data of Internet Banking User, to determine bank accounts, limits, to state access rights, to specify an Authorized Holder (User) within the meaning of the Agreement, to specify rights for performing passive and/or active transactions, as well as to set other conditions or restrictions, to draw up, sign, submit and receive all necessary documents, as well as to perform any actions necessary for the conclusion, termination and/or change of any terms and conditions under an Agreement concluded with the Bank.

The power of attorney shall be presented by the proxy in original together with a valid identity document. The Bank shall be entitled to request to receive the explicit written confirmation for the validity of the power of attorney from the legal representatives of the Account Holder, as well as to check the power of attorney with any registers to which it has regulated access. The Bank is entitled to refuse to accept a power of attorney in case of non-compliance with its requirements for handling powers of attorney, such as, but not limited to: if, at its discretion, the scope of the representative power of the authorized person is not clearly and unambiguously defined; if the power of attorney stipulates a condition for the termination of the proxy's rights or a condition for performance that is beyond its control, or if, at its discretion, it creates difficulties beyond the usual for opening or servicing an account and/or for providing the Service; if it is not able to check the power of attorney with the respective registers to which it has regulated

access; if it is not able to receive an explicit written confirmation of the validity of the power of attorney from the legal representatives of the Client; in case of doubt about the regularity of the power of attorney or about illegal actions or similar issues.

The Bank shall refuse to accept a power of attorney for the purposes of concluding an Agreement if it is notified in writing in accordance with the procedure established by it that the powers of proxy have been terminated on any of the grounds specified by law or under the power of attorney itself, for example: upon withdrawal of the power of attorney by the Account Holder, upon a refusal by the proxy, upon the death of the proxy or upon the incapacitation of the proxy, in case of dissolution of the legal entity that is the Account Holder, as well as upon the expiration of the period specified in the relevant power of attorney and upon the realization of the powers authorized by the relevant power of attorney. Written notification for withdrawal of a power of attorney may be made by the legal representatives of the Account Holder by appearing in person at any financial center of the Bank.

2. (Amended, in force as of 12 September 2018) The Agreement should be signed by the Account Holder, in the cases where the latter is also an Authorized Holder; or by the Account Holder and the Authorized Holder, in the cases where the Account Holder entitles the Authorized Holder to dispose of the funds available on the account by using the Internet Banking Service, and by a representative of the Bank. In cases where the Account Holder entitles the Authorized Holder to dispose of the funds on the Account by using the Service, the Account Holder authorizes the Bank and gives consent to the Bank to provide the Authorized Holder with information on the relevant bank account agreement entered into by and between the Account Holder and the Bank and/or the Agreement, on the operations/transactions performed through the Service, as well as other information regarding the balances and the movement on the Account(s), which information represents bank, official, professional secrecy or other regulated information.

2a. (New, in force as of 8 March 2021) The Agreement for the Service, as well as the annexes/addenda thereto and/or any other documents according to the Bank's model, including those updating contact details, shall be signed by the Account Holder or, respectively, by the legal representative or by an explicitly authorized person (where the Account Holder is a legal entity), as well as by the Authorized Holder, where the latter is different from the Account Holder, in a financial center of the Bank.

2b. (New, in force as of 8 March 2021) In case (i) the Account Holder is a natural person or a legal entity belonging to the segment of Small Business Banking and (ii) the Account Holder or, respectively, the legal representative (where the Account Holder is a legal entity) is currently a client of the Bank with current client

data – they may sign the Service Agreement, respectively an annex/addendum to the Agreement and/or other documents according to the Bank's model, remotely through the possibility provided by the Bank for electronic identification and electronic signing using QES. In these cases the Bank shall notify the clients about the signing procedure through its website at www.postbank.bg. The Bank is entitled to impose restrictions and additional requirements with respect to remotely requested changes in order to avoid misuse or for other reasons at its discretion.

3. This Agreement shall enter into force when signed by the Parties.

4. (Amended, in force as of 8 May 2021) Upon signing the Agreement by the Parties, the Bank shall provide the Authorized Holder with an Activation Code for the purpose of initial access to the Service.

5. The Service enables the Authorized Holder to use products and services of the Bank through various access channels (through the technical means of communication used by the Authorized Holder, detailed in Article IV.3 of these General Terms and Conditions), namely through the Bank's Website and the Mobile banking application.

6. The Authorized Holder shall be able to use different services depending on the selected access channel, as follows:

6.1. Through the Website:

6.1.1 Passive rights:

a) To receive real-time information in electronic form about the balance of the Account(s) provided that the Authorized Holder has specified such rights when signing up for the Service.

b) In case the respective rights are available – to receive real-time information in electronic form about the fund movements on the Account, including operations/transactions in chronological order, whereby the Bank, depending on the respective request, may provide the information in the following formats: .pdf, .doc, .docx, .xls;

c) (Amended, in force as of 12 September 2018) To receive information in electronic form on the exchange rates;

d) (Amended, in force as of 8 May 2021) To change the Access code for the Service, to activate notifications via SMS or other electronic messages to the mobile phone number provided to the Bank under the Agreement or by e-mail, regarding any logins to the system, changes of input parameters and PST. By signing the Agreement, the Account Holder explicitly and unconditionally consents that the Authorized Holder may activate/deactivate the notifications referred to in the previous sentence, as well as declares agreement to and willingness to bear the payment of the fees and commissions due in this regard;

e) (Amended, in force as of 12 September 2018) To receive information about:

- Debit cards;

- Credit cards - status, cardholder, card number, validity, current card balance, limits, monthly statement and transaction history;

- Deposits - type, term, maturity date, etc.

- Loans - availability for utilization, purpose and currency of the loan, amount and date of opening, repayment plan (including final maturity and date of repayment instalment), notification of forthcoming credit line and overdraft renewals, insurance information.

6.1.2 Active rights:

a) To give electronically orders for credit transfers between accounts of the Account Holder with the Bank or with another bank(s) in the country and abroad;

b) To give electronically orders for credit transfers to third party accounts with the Bank or with another bank(s) in the country and abroad

c) To give electronically orders for transfers to the budget/execution and orders for direct debit;

d) To submit electronically orders for mass payments in BGN to a list of recipients with one payment order (this option is available only for Accounts of Account Holders who are legal entities). By signing the payment order, orders are submitted for all transfers contained in the input file for mass payment.

e) To buy and sell foreign currency (conversion) between Accounts of the Account Holder with the Bank;

f) To make requests for cash withdrawals at the offices;

g) (Amended, in force as from 8 May 2021) To make utility payments (payment of electricity, water supply, internet services, heating, cable/satellite TV and other similar payments) to certain providers of these services, as well as payments of local taxes and fees to certain municipalities, from an Account (payment or savings account) or by credit card, each payment being confirmed in accordance with the procedure set out in clause 9a of Section V. The available utility service providers as well as the respective municipalities are indicated in the respective menu on the Website. The Authorized Holder may also make a subscription to make payments to a specific utility provider and subscriber number, whereby the creation and change of the subscription is confirmed by a software token or a one-time code received via SMS or other electronic message to a mobile phone number provided to the Bank under the Agreement. The individual payments for a created subscription do not need to be confirmed according to the procedure set out in clause 9a of Section V.

h) To receive an electronic statement about the transactions on the Account executed using the Service, including amount, type of currency, date and time, status, type of transfer, recipient, reason, payment order, value date, as well as an option to print the report in the following formats: .pdf, .doc, .docx, .xls

i) To submit electronically applications for online (remote) opening of account(s) for which the Bank has provided such an option.

j) To utilize/repay the loan granted by the Bank in compliance with the terms and conditions of the relevant loan agreement.

k) To submit electronically requests for online change of account limits – maximum amount of single transfer (transaction limit) and maximum total amount of transfers that can be made within one day (daily limit).

l) (Transferred, in force as of 12 September 2018) To perform currency transactions - exchange of currency or currency transfers between the accounts of the Account Holder and to accounts of third parties with the same or with another bank at the relevant applicable exchange rate – specified in the system and on the Website or, where applicable, as expressly agreed between the Parties. The service is available for legal entities.

6.1.3. (Repealed, in force as of 9 December 2019)

6.1.4. (Amended, in force as of 14 September 2019) Online account opening (remote opening).

a) For some accounts, the Bank provides for the option of online (remote) opening;

b) The right to online (remote) opening of account(s) shall be provided to the relevant Account Holder, when the latter is a natural person and is the Authorized Holder. The newly opened online (remotely) account shall always be with active rights in the cases where the Account Holder is a natural person (including acting as a sole proprietor or a member of the profession) and is the Authorized Holder.

c) (Amended, in force as of 8 March 2021) The right to online (remotely) opening of account(s) by companies and sole proprietors registered with the Commercial Register and the Register of Non-Profit Legal Entities (CRRNPLE) and by members of the professions shall be provided to the Authorized Holder(s) at the explicit written request of the Account Holder, respectively by its legal representative or by a person explicitly authorized, made in any of the Bank's financial centers in compliance with clause 2a, Section III. When determining the rights of the Authorized Holders on accounts to be opened online (remotely), two options are possible:

ca) (Amended, in force as of 12 September 2018) The Account Holder shall determine the rights by choosing between the rights granted to already existing Account Holder's accounts of the same type subscribed to the Service. The rights of the Authorized Holder on accounts to be opened online shall be identical to the rights on the existing account of the same type selected by the Account Holder.

cb) When there is no existing account of the same type, the rights that can be granted to Authorized Holders who have a right declared by the Account Holder to open accounts online (remotely) on these newly opened accounts can only be passive.

d) (Amended, in force as of 14 September 2019) The agreements and documents required for online (remote) account opening shall be in accordance with the Bank's model and shall be signed electronically by the following means of electronic identification: The account holder shall sign with QES, the legal force of which according to the applicable legislation is equivalent to a handwritten signature, and the Bank shall sign by electronic signature for a software or information object with holder Eurobank Bulgaria AD and with author - administrator being an

authorized person, and agreed by the Parties to have the effect of a handwritten signature in their relations, or by means of QES.

e) An account opened online (remotely) shall be considered opened after the relevant agreement is signed electronically by both Parties through the electronic methods of identification and signing specified in these General Terms and Conditions.

f) Opening an account online (remotely), which requires cash depositing is only possible in the cases where the Account Holder has the amount required on another existing account with the Bank in the same currency, may dispose of it without restrictions (including no seizures, blockades, etc. have been imposed), the account has been added to the Account Holder's Internet Banking profile and an order has been made to debit the amount for online (remote) transfer to the new account opened simultaneously with its opening.

g) The Bank shall be entitled to impose a limit on the number of requests for opening accounts online (remotely) on a monthly basis in order to avoid misuse or for other reasons at its discretion.

h) For all issues unsettled in these General Terms and Conditions regarding online opening of accounts (opening of accounts remotely), the provisions of the General Terms and Conditions for opening, keeping and closing bank accounts of Natural Persons with Eurobank Bulgaria AD or respectively the General Terms and Conditions for opening, keeping and closing bank accounts of Business Entities and Other Legal Entities with Eurobank Bulgaria AD, the applicable Bank's Tariffs and its Interest Rate Bulletin shall apply.

6.1.5. (New, in force as of 9 December 2019) Recurring payments

a) The Authorized Holders shall be able to set up in their e-Postbank profile recurring payments for a certain period, with the same amount, recipient, recipient's account, with or without the need for additional confirmation.

aa) Recurring payment with additional confirmation is set up automatically in the interval determined for it and its execution shall also require additional confirmation by the Authorized Holder by means of PST as specified in clause 9a of Section V.

ab) Recurring payment with automatic execution shall not require additional confirmation. It shall be confirmed once by the Authorized Holder by means of PST as specified in clause 9a of Section V, and then it shall be executed automatically within the interval specified.

b) When setting up a recurring payment, the Authorized Holder must also determine:

ba) the period within which it is to be executed or for indefinite term;

bb) the Account (current or savings account) from which to be executed.

c) The Bank shall make each recurring payment in accordance with the parameters specified by the

Authorized Holder until the time when the Authorized Holder refuses it or the period set expires.

d) Recurring payment may be refused by the Authorized Holder at any time through the Authorized Holder's e-Postbank profile.

e) The recurring payments shall be executed when there is sufficient availability on the Account, and all other conditions pursuant to these General Terms and Conditions and the agreement for the Account from which they are ordered shall apply thereto.

6.1.6. (New, in force from 30 August 2021) List of Trusted Recipients:

(A) Right to create a List of Trusted Recipients shall be vested in:

(aa) The Account Holder, when the latter is a natural person and coincides with the Authorized Holder.

(ab) Where the Account Holders are companies and sole proprietors registered with the Commercial Register and the Register of Non-Profit Legal Entities (CRRNPLE) and members of the professions, the right shall only be vested in the Authorized Holder(s) at the explicit written request of the Account Holder, respectively by its legal representative or by a person explicitly authorized, stated in any of the Bank's financial centers in compliance with clause 2a, Section III.

(b) The creation and modification of the List of Trusted Recipients shall be performed by an Authorized Holder, entitled to create/modify such a list according to the preceding paragraph (a) after login and identification in the e-Postbank Service with Access Code, strong authentication and confirmation with a Software Token.

(c) The list of Trusted Recipients is available to all Authorized Holders who, according to clause 6.1.6(a) are entitled to create and modify it for the respective Account Holder.

(d) Strong authentication of the Authorized Holder and confirmation through Software Token shall only be required for the creation and modification of the List of Trusted Recipients. Any electronic remote payment transactions to a person on the List of Trusted Recipients shall be performed without the need to confirm the payment transaction with m-Token Postbank or otherwise as provided for in these General Terms and Conditions, provided that the Authorized Holder has logged in to e-Postbank with an Access Code.

6.1.7. (New, in force from 30 August 2021) Low-value transactions:

(a) remote electronic payment transaction initiated after login and identification of an Authorized Holder in the e-Postbank Service with an Access Code, without requiring its confirmation with a Software Token or otherwise as provided for in these General Terms and Conditions.

(b) to exercise the option under (a), the following prerequisites must be met:

the value of the transaction should not exceed the equivalent of BGN 58, as well as the cumulative sum of the previous consecutive remote electronic payment transactions initiated by the Authorized Holder should not to exceed the equivalent of BGN 195 as from the time

of the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions or the number of previous consecutive remote electronic transactions initiated by the Authorized Holder should not exceed five as from the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions.

6.2. Through the Mobile banking application:

a) Free access to general information about the Bank, banking products, services, current promotions, etc. Upon free access, the Authorized Holder will not receive information about the balance and the movement of the funds on the accounts and information on other banking products used by the Account Holder.

b) (Amended, in force as of 8 May 2021) After identification by Access code or Mobile banking code or by Biometric data, the Mobile application will provide information about all registered accounts and products of the Account Holder in the Internet Banking with the passive rights within the meaning of clause 6.1.1 above (except for the rights referred to in clause 6.1.1(d));

In some cases, in addition to the identification under the previous sentence, the Bank may require further identification by a one-time code sent via SMS or another electronic message to the mobile phone number provided by the Authorized Holder / Account Holder to the Bank under the Agreement.

c) (Modified, in force as of 8 May 2021) After identification by Access code or Mobile banking code or by Biometric data, the Authorized Holder will be able to perform the following transactions:

ca) To submit electronically orders for credit transfers between the Account Holder's accounts with the Bank, including for repayment of credit card obligations of the Account Holder.

cb) (Amended, in force as of 8 May 2021) To make utility payments (payment of electricity, water supply, internet services, heating, cable/satellite TV and other similar payments) to certain providers of these services, as well as payments of local taxes and fees to certain municipalities, from an Account (payment or savings account) or by credit card, each payment being confirmed in accordance with the procedure set out in clause 9a of Section V. The available utility service providers as well as the respective municipalities are indicated in the respective menu on the m-Postbank application. The Authorized Holder may also make a subscription to make payments to a specific utility provider and subscriber number, whereby the creation and change of the subscription is confirmed by a software token or a one-time code received via SMS or other electronic message to a mobile phone number provided to the Bank under the Agreement. The individual payments for a created subscription do not need to be confirmed according to the procedure set out in clause 9a of Section V.

d) (Amended, in force as of 8 March 2021) After identification by Access code or Mobile banking code or

by Biometric data, and after confirming with a software token the consent to perform the specific transaction, the Authorized Holder will be able to electronically order credit transfers in BGN and foreign currency to third party accounts with the Bank or in BGN to accounts with (an)other bank(s) in the country from each Account to which access is requested through the Service, up to the amount specified in the limit set under this procedure (transaction limit, daily limit or monthly limit).

(e) (New, in force as of 30 August 2021) After login and identification in Mobile Banking ("m-Postbank") with a Mobile Banking Code or Biometric Data, the Authorized Holder, in the cases where the latter is also the Account Holder or where the latter has been granted a right under clause 6.1.6(a)(ab) of Section III, shall be allowed to create and modify a List of Trusted Recipients subject to successful strong authentication and confirmation via Software Token. Electronic remote payment transactions to a person on the List of Trusted Recipients shall be performed without the need to confirm the payment transaction with Software Token, provided that the Authorized Holder has logged in and been identified in m-Postbank with a Mobile Banking Code or Biometric Data.

(f) (New, in force from 30/08/2021) Low-value transactions:

(fa) remote electronic payment transaction, initiated by an Authorized Holder after having logged in and been identified in Mobile Banking ("m-Postbank") with a Mobile Banking Code or Biometric Data, without need for its confirmation via Software Token.

(fb) to exercise the option under (a), the following prerequisites must be met: the value of the transaction should not exceed the equivalent of BGN 58, as well as the cumulative sum of the previous consecutive remote electronic payment transactions initiated by the Authorized Holder should not to exceed the equivalent of BGN 195 as from the time of the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions or the number of previous consecutive remote electronic transactions initiated by the Authorized Holder should not exceed five as from the latest strong authentication through Software Token or otherwise as provided for in these General Terms and Conditions.

7. (Amended, in force as of 8 March 2021) The active and/or passive access rights when using the Service under clause 6 above shall be determined in respect of the Authorized Holder and the Account by the Account Holder or, respectively, by its legal representative or by a person expressly authorized by the Account Holder when concluding the Service Agreement in a financial center of the Bank or remotely, in compliance with clause 2a or clause 2b, Section III. Any change of the active and/or passive rights may be requested by the Account Holder or, respectively, by its legal representative or a person expressly authorized by the Account Holder, by signing an annex / addendum to the Service Agreement in a financial center of the Bank or remotely, in compliance with clause 2a or clause 2b, Section III.

7.1. (Amended, in force as of 8 March 2021) When requesting access through the Service to a credit card(s) issued by the Bank, the option to execute active transactions is only provided if the Authorized Holder of the Service is the Cardholder of the respective credit card, unless the Cardholder of the credit card has declared when concluding the Agreement that he/she wants to perform only passive credit card operations through the Service. Authorized Holders in connection with the Service who are not Cardholders of the respective credit cards may not have active rights on these cards.

8. (Amended, in force as of 8 March 2021) The Account Holder should specify in the Agreement (in the annexes / addenda thereto, respectively) the natural persons - Authorized Holders who shall be entitled to access the Service, the Account(s) to which each of them will have the right of access, the respective scope of access for each Authorized Holder - passive and/or active rights, their ability to create, sign and send transfers, as well as the total maximum amount of non-cash transfers, which the respective Authorized Holder or group of Authorized Holders, respectively, may perform for a certain period of time (limit for Authorized Holder / limit for a group of Authorized Holders), if determined. The amount of the limits for an Authorized Holder under the previous sentence may not exceed the daily limits and/or transaction limits and/or monthly limits determined / changed herein.

9. Clients who are Account Holders of accounts with the Bank or Cardholders of credit cards issued by the Bank shall be allowed to sign up for the Internet Banking Basic Functionality without concluding an Agreement for the Provision and Use of the Internet Banking Service, according to the procedure and under the terms and conditions described in detail in the General Terms and Conditions for opening, keeping and closing bank accounts of Natural Persons with Eurobank Bulgaria AD and the General Terms and Conditions of Eurobank Bulgaria AD for the issue and use of VISA, Mastercard and American Express credit cards, respectively.

10. The Account Holder shall be required to individualize in the Agreement (respectively in the annexes/addenda thereto) the Authorized Holders, indicating their full names and a PINs and, respectively, to indicate similar data for the Authorized Holders - foreign individuals.

11. The Service may only be used in respect of the Account(s) explicitly specified in the Agreement and under the terms and conditions specified in the Agreement. When active rights are also included in the scope of the Service, the transactions shall be accepted and performed insofar as they are applicable to the specific Account (in particular, deposit or savings account) according to the agreement for the respective bank account concluded by the Account Holder.

12. (Amended, in force as of 8 March 2021) The termination of the registration for the use of the Service in respect of Authorized Holders, as well as any changes in and/or cancellation of their rights, scope and access limits, as well as exclusion of access to products, may be

performed by the Account Holder or by its legal representative or a person expressly authorized by the Account Holder, respectively, by signing and submitting to the Bank the necessary documents according to the Bank's model, and/or (as appropriate) by signing the relevant annex / addendum to the Service Agreement in any financial center of the Bank in compliance with the provisions of clause 2a, Section III. Each Authorized Holder may terminate its registration for the use of the Service after signing and submitting to the Bank the relevant documents according to the Bank's model in any financial center of the Bank in compliance with the provisions of clause 2a, Section III. In the cases referred to in the previous sentences and (according to the case) after concluding the necessary additional agreements / annexes, respectively, after submitting the necessary documents to the Bank, the Agreement shall be considered amended regarding the above circumstances.

13. (Amended, in force as of 8 March 2021) In order to increase the security of the Service and limit the risk of an unauthorized transaction, the Account Holder or, respectively, its legal representative or a person expressly authorized by the Account Holder, may set a maximum amount of a single transfer (transaction limit), a maximum total amount of transfers that can be made within one day (daily limit), as well as a maximum total amount of transfers that can be made within one calendar month, by signing and submitting to the Bank the necessary documents according to the Bank's model, and/or (as the case may be) by signing the respective annex / addendum to the Service Agreement in any financial center of the Bank or remotely, in compliance with clause 2a or clause 2b, Section III.

In order to achieve the objectives referred to in the previous sentence, the Bank is entitled to unilaterally introduce and/or change (including, but not limited, to increase at its discretion upon request by the Account Holder) daily limits, transaction limits or monthly limits, provided that the limits set by the Account Holder may not exceed the limits introduced / changed by the Bank. Where the Account Holder has not specified a daily limit and/or a transaction limit in compliance with sentence 1 herein, the maximum limits shall be the daily limit and/or the transaction limit set by the Bank, as specified in the Service Agreement.

The Bank shall notify the Account Holder and the Authorized Holder of the size of the limits introduced by it in compliance with Section XIII of these General Terms and Conditions.

14. (Amended, in force as of 8 March 2021) The determination / change of a certain daily limit, transaction limit, and/or monthly limit at the request of the Account Holder shall become effective for all parties (including the Authorized Holder) after the Account Holder of the account has signed and submitted the respective documents according to the Bank's model, respectively, in the applicable cases after the Account Holder of the

account has signed the necessary addenda / annexes (without the need for the documents to be signed by the Authorized Holder) and, respectively (if applicable), after the Bank has taken a decision at its discretion to make the requested change of the relevant daily limit and/or transaction limit, and/or monthly limit, for which the Bank shall notify the Account Holder and the Authorized Holder according to the procedure specified in Section XIII of these General Terms and Conditions.

15. The Bank shall provide an option for requesting a change of the limits (transaction limit and/or daily limit) online as well.

15.1. The Authorized Holder has the right to change the limits online when he is a natural person and coincides with the Account Holder.

15.2. (Amended, in force as of 8 March 2021) The right to make online changes in limits of companies and sole proprietors registered with the CRRNPLE and members of the professions shall be granted to the Authorized Holder(s) at the express request of the Account Holder or, respectively, by the legal representative or a person explicitly authorized by the Account Holder, by signing and submitting the relevant documents in accordance with the Bank's model in any financial center of the Bank in compliance with clause 2a, Section III.

15.3. (Amended, in force as of 8 March 2021) The request for making online changes in limits should be made through the Service in the profile of the Authorized Holder entitled to do so according to the preceding clause 15.1 or 15.2, after accessing the system through the Site and being identified by entering the relevant Access code. The request shall be started after correctly entering a one-time code received via SMS or another electronic message or by voice call to the mobile phone number specified in the Agreement. Then the Authorized Holder should set the specific limits (transaction limit and/or daily limit) for a selected account within the scope of limits set by the Bank, available in the respective menu in the Authorized Holder's profile in the system of Internet Banking. Finally, the request should be confirmed via Software Token or QES.

15.4. The Authorized Holder is able to monitor the status of the request in the Authorized Holder's profile in the Service.

15.5. The change of limits online shall become effective after the Bank approves it and notifies the Authorized Holder thereof.

15.6. The Bank is entitled to refuse to approve the request for online setting/changing limits without giving any reasons.

IV. CONDITIONS AND TECHNICAL MEANS REQUIRED FOR USING THE SERVICE

1. Except for the case specified in Article XIII.8 of these General Terms and Conditions, a precondition for using the Service is that the Account Holder should have one or more accounts opened with the Bank.

2. (Amended, in force as of 12 September 2018) By signing the Agreement, the Account Holder/Authorized Holder explicitly, irrevocably and unconditionally

declares to have been acquainted with the relevant applicable General Terms and Conditions of Eurobank Bulgaria AD to the agreements for bank accounts (of natural persons/legal entities) (published on the Bank's website at www.postbank.bg and/or available in the financial centers of the Bank), including the information that should be provided to the Account Holder / Authorized Holder under Article 60 et seq. of the Payment Services and Payment Systems Act (PSPSA), accepts and agrees that the provisions of the agreement(s) for bank account(s) should be applied in the relations between the Parties in connection with the opening, keeping and closing the Account(s), as well as with ordering, executing, contesting and correcting payment transactions through the use of the Service, with the responsibility of the Parties for unauthorized or incorrect transactions, and other applicable provisions, unless otherwise agreed in the Agreement.

3. The Authorized Holder may use the Service through the following technical means (according to the different access channels specified in Article III.6):

3.1. To access through the Website, a Computer configuration is required that allows for the installation of an operating system usable for the purpose of the service, Internet access and a usable browser;

3.2.1. (Amended, in force as of 14 September 2019) To access through Mobile banking, as well as to use the m-Token Postbank application for the purposes of verifying the identity of the Authorized Holder and for confirming the consent for execution of electronic remote payment and non-payment transactions, an Android or iOS mobile device is required that is usable for the needs of the Service and access to the Internet;

3.2.2. (Amended, in force as of 14 September 2019) To use the Biometric login data in the Mobile banking application, as well as to access and use the m-Token Postbank application, an Android mobile device is required with a fingerprint sensor or an iOS device that has a fingerprint sensor or facial recognition capability.

3.3. To use the Service, the Bank shall establish minimum technical requirements for the above technical means and publish this information on its website, specified in Article XIII.2 of these General Terms and Conditions.

4. The Bank shall reserve the right to technically change the procedure for providing the Service for the purposes of improving the quality and security of the Service, as well as to comply with the legal requirements. The Bank shall notify the Account Holder and/or the Authorized Holder of any amendments that require a change in the minimum technical requirements for using the Service, specified in Article IV.3 of these General Terms and Conditions, with a two months' written notice sent to the Authorized Holder and the Account Holder in accordance with the procedure referred to in Article XIII.3 of these General Terms and Conditions. A draft of the planned changes in the information regarding the minimum technical requirements shall also be submitted to the Account Holder and/or the Authorized Holder through the

Service and shall be published in their profile within the above-mentioned term.

V. ELECTRONIC IDENTIFICATION FOR THE USE OF THE SERVICE

1. (Amended, in force as of 8 May 2021) In order to access the Service, the Authorized Holder should initially sign up in the Bank's system. The Bank shall start the registration procedure after the Agreement is signed by the Parties and the Authorized Holder shall be provided in person an Activation Code to be used for the initial setting of an Access code. In the cases where the Account Holder is a natural person, the Activation Code shall only be handed over in person to the respective Authorized Holder. In the cases where the Account Holder is a legal entity, the Activation Code shall be handed over in person to the respective Authorized Holder or to a person authorized by the Account Holder under a power of attorney in compliance with the Bank's requirements under clause III.1 of these General Terms and Conditions, containing an explicit authorization to receive an Activation Code. In the cases where the Account Holder is a legal entity, by accepting the General Terms and Conditions and signing the Agreement (respectively any annexes / addenda thereto), the Authorized Holder declares that the authorization of a third party to receive an Activation Code will mean that Authorized Holder also assumes all risks of non-receipt of the Activation Code due to the fault of the proxy, as well as the risk of unauthorized operations performed by the proxy or a third party, and accepts that the transfer of the Activation Code by the Bank to the proxy does not constitute disclosure of personalized security tools to a person other than the Authorized Holder.

2. (Amended, in force as of 8 May 2021) The initial login to the electronic banking system in order to use the Service shall be carried out through the Website, and for this purpose the Authorized Holder should enter the provided Activation Code, after which the Bank will send an initial username to the e-mail address specified in the Agreement and the initial password via SMS or other electronic message to the mobile phone specified in the Agreement. After the initial login to the system, additional identification will be requested by a one-time code sent via SMS or other electronic message or by automatic voice call to a mobile phone specified by the Authorized Holder in the Agreement. Upon successful initial login, the system requires a mandatory change of the initial password. The Authorized Holder is able to determine a username and password (collectively referred to as "Access code") at the discretion of the Authorized Holder, subject to the requirements of the system for the length and complexity of the password.

3. (Amended, in force as of 8 May 2021; previous Article V.2.1, amended, in force as of 14 September 2019) To access and use the Service through the Website, the Authorized Holder shall be required to perform electronic identification at each login in the system, by entering of the relevant username and password (Access code), after manually entering in the browser one of the Internet

addresses for access to the Website. In some cases, in addition to the identification under the previous sentence, the Bank may require further identification by a one-time code sent via SMS, by another electronic message or by automatic voice call to the mobile phone number provided by the Authorized Holder / Account Holder to the Bank under the Agreement.

4. The Authorized Holder shall be required to periodically change the password when using the Service.

5. (Amended, in force as of 8 May 2021; previous Article V.3, amended, in force as of 14 September 2019) In case of forgotten password and/or username for access to the Service, the Authorized Holder may receive a new Activation Code in any financial center of the Bank. A new access password can also be requested entirely online through the Website, and the Authorized Holder should enter a username and data for the mobile phone number and the e-mail provided to the Bank under the Agreement.

6. (Previous Article V.2.2, amended, in force as of 14 September 2019) To access and use the Service through the Mobile banking application, the Authorized Holder shall be required to perform electronic identification at each login in the application by entering an Access code or by entering a Mobile banking code or by using Biometric data, in case the latter have been requested in compliance with Article V.7 or V.8 herein.

a) (Amended, in force as of 12 September 2018) identification and login through Access code shall be performed as specified in Article V.3 above;

b) (Amended, in force as of 12 September 2018) identification and login through Mobile banking code shall be performed as the Authorized Holder enter a personal identification number (PIN code) generated in compliance with Article V.7 herein.

c) (Amended, in force as of 8 March 2019) identification and login through the "Biometric data" functionality shall be performed using biometric data registered with the operating system of the mobile device. If the login in the Mobile banking application using the biometric data is enabled, the access to the application will be considered authorized/enabled by the Authorized Holder when using any of the biometric data registered in the operating system of the mobile device.

7. (Previous Article V.2.3, amended, in force as of 14 September 2019) The Authorized Holder may request identification and login in the Mobile banking application by Mobile banking code after the initial login and identification in the application by Access code or Biometric data, explicitly activated option for access by Mobile banking code in the "Settings" menu of the application and generation of the corresponding personal identification number (PIN code);

8. (Previous Article V.2.4, amended, in force as of 14 September 2019) The Authorized Holder may request identification and login in the Mobile banking application using Biometric data after the initial login and identification in the application by Access code or Mobile banking code, explicitly activated option for access by Biometric data in the "Settings" menu of the application.

9a) (Amended, in force as of 8 May 2021; previous Article V.3.(a), amended, in force as from 9 December 2019) In addition to the data referred to in Article V.3 – V.8 above, for the purposes of electronic identification when using the Service and for performing active payment transactions to Accounts with a holder other than the Account Holder, as well as for making transfers to accounts with banks other than Eurobank Bulgaria AD, the Authorized Holder confirms consent to perform the specific transactions by means of a selected by the latter and registered PST - activated Software Token or QES in combination with a one-time code received via SMS or another electronic message on a mobile phone number provided to the Bank under the Agreement.

9b) (Repealed, in force as of 9 December 2019)

10. (Amended, in force as of 8 May 2021; previous Article V.3. (A), amended, in force as from 14 September 2019) As of 8 May 2021 the Bank does not issue or accept digital certificates as means of certifying the authorship of electronic documents. In the event that before the specified date, the Authorized Holder has selected and used a Digital certificate issued by the Bank as a Personalized Security Tool, the Authorized Holder shall confirm to be aware of the potential risks of using this access and identification tool and shall accept them, and that the latter has obtained the consent of the Account Holder in this regard. The Digital certificate only serves for identification when accessing the Bank's Service through the Website and may not be used for any other purposes. QES can be used for identification only when accessing the Service through the Website.

11. (New, in force as of 14 September 2019) In order to use the m-Token Postbank application as a Personalized Security Tool, the Authorized Holder must install and activate the application by submitting an online application through a dedicated section of the Website.

12. (Amended, in force as of 8 May 2021) The authorized holder shall receive the activation codes for the m-Token Postbank application via SMS or another electronic message and via e-mail to the mobile phone number and e-mail address, respectively, registered with the Bank (the e-mail sent also indicates a link to download the application). The Bank shall not be liable for incorrectly submitted and/or not updated by the Authorized Holder mobile phone number and e-mail address. The mobile phone number and e-mail address can be updated at an office of the Bank.

13. (Amended, in force as of 8 May 2021) In order to ensure a sufficiently high level of protection of the channels through which the activation codes are received, the Authorized Holder should take measures to make sure that the access to the e-mail via the mobile device is by using a username and password, and the access to SMS messages or other electronic messages is carried out after entering the relevant identification data for unlocking the mobile device (PIN for mobile device or Biometric data).

14. (New, in force as of 14 September 2019) When using m-Token Postbank, the Authorized Holder should confirm his/her consent to execute a specific electronic

remote payment transaction through the Service in one of the following ways:

a) The Authorized Holder receives a Push notification on the mobile device on which the m-Token Postbank application is installed and activated with information about the specific transaction to be confirmed.

b) The Authorized Holder scans a QR code displayed on the Website, as a result of which information about the specific transaction to be confirmed is displayed in the m-Token Postbank application.

The Authorized Holder should unlock and access the m-Token Postbank application, identifying himself/herself in the pre-selected method, namely: with a PIN specified for m-Token Postbank or with Biometric data, and to explicitly confirm the transaction.

15. (New, in force as of 14 September 2019) The m-Token Postbank application is a personalized security tool with respect to the Service and the Authorized Holder is required to take all reasonable measures to protect it and prevent unauthorized access. In this regard, the Authorized Holder is required to take the necessary measures when storing Biometric data in the mobile device (fingerprint, facial recognition) to prevent their unauthorized use and/or use for fraudulent purposes, including: to use only the mobile device in person and not to transfer it for use by other persons (including children, parents, spouses), to protect the mobile device from damage, destruction, loss, theft, its use in another illegal way, not to register in the operating system of the mobile device any Biometric data of other persons.

16. (New, in force as of 14 September 2019) Upon logging in the Mobile banking and/or the m-Token Postbank application with Biometric data, the access to them will be considered authorized by the Authorized Holder when using any of the Biometric data registered in the operating system of the mobile device.

17. (New, in force as of 14 September 2019) Upon unlocking the m-Token Postbank application with a PIN code, the Authorized Holder shall bear all the obligations for its confidentiality, as provided in these General Terms and Conditions regarding the Access code, including, but not limited to obligations to keep it secret by taking all necessary measures to prevent other persons from knowing it, not to communicate it to anyone, not to record it in the device or on any other means, as well as to take any other necessary measures to protect the secrecy of the PIN code for m-Token Postbank. Allowing any third party to know the PIN code, disclosing or recording it on any medium shall constitute gross negligence of the Authorized Holder, and the list is not exhaustive. The PIN code can be changed repeatedly by the Authorized Holder through the m-Token Postbank application.

18. (Repealed, in force as of 8 May 2021; previous Article V.5, amended, in force as of 14 September 2019)

19. (Amended, in force as of 8 May 2021) By activating the m-Token Postbank application, the Authorized Holder is deemed to have chosen the same as a means of identification before the Bank and to confirm his/her consent to perform electronic remote payment and non-

payment transactions through the Service, as well as through other digital channels for remote access, including when making online payments by bank cards issued by the Bank. By activating the m-Token Postbank application, the Authorized Holder orders, in the presence of an active QES registered in the system, to be deregistered by the Bank for the purposes of confirming electronic remote payment transactions.

20. (Amended, in force as of 8 May 2021; previous Article V.7, amended, in force as of 14 September 2019) All statements made on behalf of the Authorized Holder electronically shall be considered validly signed written statements (electronic documents) binding on the Authorized Holder and the Account Holder, unless otherwise provided by the applicable legislation and/or these General Terms and Conditions. Upon access to the Service, from the time of access to the end of the user session, the Authorized Holder shall be responsible for and bound by all statements, the author of which is identified in the system through the use of the relevant PST of the Authorized Holder, unless otherwise provided by the applicable legislation and/or these General Terms and Conditions. The electronic use of a software token ("m-Token Postbank") or QES of the Authorized Holder shall have the effect of a legally valid signature of the Authorized Holder within the meaning of Article 13(4) of the Electronic Document and Electronic Certification Services Act (EDECSA).

The orders submitted via the Mobile banking application through a trusted mobile device after login and identification in the application through the Access code or Mobile banking code of the Authorized Holder or through Biometric data registered in the operating system of the mobile device will be considered permitted by the Authorized Holder and signed with a legally valid signature within the meaning of Article 13(4) EDECSA.

21. (New, in force as of 14 September 2019) The Bank, the Authorized Holder and the Account Holder agree that for the purposes of performing electronic remote payment and non-payment transactions through the Service, the confirmation with m-Token Postbank shall represent a valid identification of the Authorized Holder and confirmation and consent to perform the respective transaction. When ordering a payment transaction, the consent of the Authorized Holder shall refer to the size of the specific amount and the payee and the Bank will consider it ordered and authorized by the Authorized Holder and will perform any transaction confirmed by m-Token Postbank.

22. (Amended, in force as of 8 May 2021; previous Article V.3.(b), amended, in force as from 14 September 2019) It is not necessary to submit a request to the Bank for issuance/registration of a Software token, in case the Authorized Holder declares (i) the use of the Service with passive rights only within the meaning of Article III.6.1.1 and Article III.6.2(a) and Article III.6.2(b) above, and (ii) when performing payment transactions between

Accounts of the Account Holder with the Bank (including in case of payments from the Account for covering liabilities of the Account Holder on a credit card issued by the Bank and the access to which the Account Holder has explicitly stated in the Agreement). In these cases, the Authorized Holder shall only be identified by entering the Access code when accessing through the Website or, respectively, by entering an Access code, a Mobile banking code or by using Biometric data when accessing through Mobile banking. In some cases, in addition to the identification under the previous sentence, the Bank may require further identification by a one-time code sent via SMS, by another electronic message or by automatic voice call to the mobile phone number provided by the Authorized Holder/Account Holder to the Bank under the Agreement.

VI. MAKING PAYMENTS

1. The Authorized Holder shall have access to the Service every day, 24 hours a day, and the Bank shall process and execute payment orders in accordance with the terms and conditions specified in the General Terms and Conditions for bank accounts applicable to the respective bank account agreement and in compliance with the current legislation:

1.1. 24 hours a day – for transfers between bank accounts opened with the Bank in the same currency, as well as for transfers between bank accounts opened with the Bank in different currencies (provided that the accounts from which the transfer is ordered and received are in BGN or EUR);

1.2. Within its working hours – for interbank transfers, as well as for transfers between bank accounts opened with the Bank in different currencies (provided that any of the accounts from which or on which the transfer is ordered is in a currency other than BGN or EUR). The Account Holder / Authorized Holder may also submit payment orders outside of the working hours of the Bank, in which case the payment order may be cancelled by the beginning of the next business day for the Bank (and in case of transfer to an account in another currency /conversion/ - by 09:30 a.m. on the next business day), and in case the payment order for transfer to an account in another currency (conversion) is not cancelled by 09:30 a.m. on the next business day, it shall be executed at the respective exchange rate of the Bank at the beginning on this business day, for which the Account Holder and the Authorized Holder give their explicit consent by accepting these General Terms and Conditions.

For the purposes of these General Terms and Conditions, the payment order shall be considered received by the Bank when the Authorized Holder has ordered (has given consent for) its execution in compliance with Article VI.2 herein and the data from the order have been entered in the accounting and information system of the Bank.

2. (Amended, in force as of 8 March 2021) The Authorized Holder shall order (agree to) execute payment transactions by submitting (filling in, signing

and sending) electronically orders in the form and according to the procedure specified on the relevant website of the Bank, respectively on the Mobile banking application and in compliance with the requirements of the effective Bulgarian legislation and other applicable provisions. In order to ensure the appropriate execution of a payment order, the Authorized Holder must provide (or fill in, respectively) clearly, accurately and correctly information about the payee, reason and amount of the transfer, as well as information uniquely characterizing the payee's account, including its unique identifier (including international bank account number - IBAN and international bank identification code - BIC). In case of inaccuracy of the unique identifiers indicated by the Authorized Holder, the Bank shall not be liable for the failure to execute or for any inaccurate execution of the respective payment transaction. The Bank shall only execute orders for transactions up to the amount of the available balance on the Account(s) and in compliance with the applicable General Terms and Conditions for the respective bank account. The Authorized Holder undertakes to regularly monitor the transactions in the electronic banking system ordered through the use of the Service, their status and successful reflection and accounting by the Bank. Upon rejection of a payment order entered in the electronic banking system, the Authorized Holder shall receive a systematic message with the number of the refused transfer, which shall be considered that the Bank has notified the Authorized Holder and the Account Holder that the payment order will not be executed. The Authorized Holder undertakes to use the Service in compliance with the limits for the use of the Service specified in the Agreement by the Account Holder, as well as with the daily limit and/or monthly limit and/or transaction limit set/changed pursuant to clause 11 and clause 12 of Section III. In case the value of the order submitted by the Authorized Holder is higher than the relevant limit, as well as when the transaction, according to the Agreement, needs to be ordered by a group of Authorized Holders, the Bank shall refuse to execute the transaction without constituting a breach of the Agreement and these General Terms and Conditions. The Account Holder undertakes to maintain sufficient funds on the Account(s) to cover all the obligations arising from the use of the Service.

3. The Account Holder/Authorized Holder may not cancel a payment order after it has been received by the Bank, except in the cases expressly provided for in these General Terms and Conditions. In case the Bank refuses to execute an order for a payment transaction, the Authorized Holder shall receive a notification, except for the cases where the provision of this information is not allowed according to the applicable legislation.

4. For the use of the Service, the Account Holder/Authorized Holder shall owe and pay fees and commissions according to the Bank's Tariff, an integral part of these General Terms and Conditions. By signing the Agreement (including the annexes/addenda thereto), the Account Holder and the Authorized Holder confirm that they have read the content of the Tariff and agree to

pay all fees and commissions due under the Tariff. By signing the Agreement (including the annexes/addenda thereto), the Account Holder/Authorized Holder gives their explicit and irrevocable consent and authorizes the Bank to collect ex officio from the balance on the Account, as well as from the balance of all their other accounts opened with the Bank, all its receivables arising from the use of the Service, including, but not limited to, receivables for fees and commissions due in connection with the Agreement. In this case, the Bank shall notify the Account Holder/Authorized Holder of the basis, the value date and the amount of the collected funds under the provisions of Article XIII.7.

5. When performing transactions, the Authorized Holder shall explicitly indicate in the field designated for this purpose whether the ordered transaction is intended for payment of wages, including advance payments, or not. The Bank shall not be responsible for electronic bank payment orders received through the Internet Banking system and automatically processed, which are intended for payment of wages, including advance payments, if the Authorized Holder has failed to explicitly indicate the reason for the transaction.

6. When providing and using the Service, the transfers between local and foreign persons, as well as cross-border transfers, shall be executed in compliance with the effective currency legislation.

7. By using the Service, no transfers from deposit accounts can be made.

8. The Bank is entitled to require the submission of additional documents in compliance with the requirements of the effective legislation. In the cases where, according to the effective legislation, for the implementation of the respective operation, additional documents should be submitted and/or filled in (including, but not limited to: document - reasons for the transaction, declarations, certificates), the Authorized Holder undertakes to provide/complete the relevant document on the day of the transaction before its execution. The Authorized Holder may compile/fill in and sign in electronic form or attach the relevant required additional documents in the manner provided for in the Internet Banking system or to present them in an office of the Bank.

9. After entering a transfer order in the Bank's system in the form of an electronic bank payment order, it shall be considered received and the Bank shall execute it, except if:

9.1. The payment order has not been entered in accordance with the standards of the systems for servicing interbank money transfers;

9.2. There are not enough funds in the Account(s);

9.3. (Amended, in force as of 12 September 2018) Seizure has been imposed on the respective Account, as a result of which there are not enough free funds on the Account to execute the payment transaction and pay the fees and commissions due to the Bank in connection with its execution;

9.4. There is no declaration submitted by the Authorized Holder or the other necessary documents required by the applicable legislation have not been provided.

10. The Account Holder unconditionally consents and authorizes the Bank, when providing the Service, to enter electronic messages for the respective payment orders in the payment systems for servicing interbank money transfers, on behalf and for the account of the Account Holder, in accordance with the data received by the Bank from the Authorized Holder electronically when using the Service.

11. All transactions performed while using the Service shall be automatically registered by the Bank chronologically through certain procedures and technical means that allow secure storage and accurate reproduction of the information and prevent any possibility for its subsequent change. The entries of all transactions are accounting documents within the meaning of the Accountancy Act and shall be considered to be true until proven otherwise.

12. (Amended, in force as of 12 September 2018) After performing an operation/transaction (related to debiting or crediting an Account), the Bank shall provide an option to the Authorized Holder and the Account Holder by using the Service to receive information about the respective operation/transaction (with content consistent with Article 65(1) and Article 66(1) PSPSA, as far as it is applicable).

13. (Amended, in force as of 8 May 2021) In order to prevent misuse that could lead to damage to the Account Holder and the Authorized Holder, provided that the Bank suspects that the execution of a particular operation/transaction is ordered by unauthorized access to the Service, it shall be entitled to request the Authorized Holder whose PSTs were used in the order of the operation/transaction and/or the Account Holder to provide additional confirmation of the ordered operation/transaction by a one-time code sent automatically upon the order of the operation/transaction by SMS or another electronic message to a mobile phone number specified by the Authorized Holder/Account Holder and registered with the Bank or in another way approved by the Bank, including by telephone, e-mail or other means of remote communication.

14. (Amended, in force as of 8 May 2021) In addition to the foregoing, if there are other cases where, in the opinion of the Bank, there is fraud or threat to the security of use of the Service or in case of suspicion of the existence of such circumstances, the Bank shall promptly notify the Authorized Holder thereof and if the ordered operation/transaction has not yet been executed, the Bank shall not execute it. The notification is sent through the Service via SMS or another electronic message to a mobile phone number specified by the Authorized Holder/Account Holder and/or in another way approved by the Bank, including by making a telephone call, e-mail or other method of remote communication.

The Parties shall make the necessary efforts to maintain and use these means and channels for notification in a manner that meets the modern standards of technological security, and shall prevent their use by unauthorized third parties and shall protect their integrity. The Bank shall notify the Authorized Holder and the Account Holder in an appropriate manner in the event of a significant operational or security incident concerning the Service which affects or may affect the financial interests of the Authorized Holder and the Account Holder, as well as of all measures undertaken to limit the adverse effects of the incident.

15. (Amended, in force as of 12 September 2018) In the cases specified in the preceding two clauses of this Section of the General Terms and Conditions, the deadline for the execution of the ordered operation/transaction by the Bank shall start to run as from the time of the confirmation of the operation/transaction by the Authorized Holder and/or the Account Holder, regardless of whether it is otherwise agreed in the General Terms and Conditions for bank accounts applicable to the respective bank account agreement.

VII. OBLIGATIONS OF THE ACCOUNT HOLDER / AUTHORIZED HOLDER WHEN USING THE SERVICE

1. (Amended, in force as of 12 September 2018) The Account Holder/Authorized Holder shall be required to use the Service only in compliance with the terms and conditions of the Agreement, these General Terms and Conditions and the provisions of the effective Bulgarian legislation, including but not limited to the Payment Services and Payment Systems Act, BNB Ordinance No. 3 of 18 April 2018 on the terms and conditions and the procedure for opening payment accounts, for executing payment transactions, and for using payment instruments ("Ordinance 3"), the Measures against Money Laundering Act, etc. The Authorized Holder and the Account Holder shall not be entitled to use the Service for purposes prohibited by the laws of the Republic of Bulgaria; the Bank shall not monitor the lawfulness of the transactions, unless otherwise provided by a relevant regulation. The Authorized Holder and the Account Holder shall be responsible for all unlawful transactions executed through the use of the Service under the provisions of the effective law.

2. (Amended, in force as of 14 September 2019) The Account Holder and/or the Authorized Holder shall be required to notify the Bank or a person authorized by it of the occurrence of any of the circumstances specified in Article VIII.2 herein.

3. (Amended, in force as of 14 September 2019) The Account Holder/Authorized Holder shall be required, after receiving access to the Service, to take all reasonable actions to keep the PST (Activation key, Access code, Mobile banking code, PIN for access to m-Token Postbank), including to remember the Access code, the Mobile banking code and their PIN for access to m-Token Postbank and not to record or keep

information about these characteristics on any media. The failure of the Account Holder/Authorized Holder to comply with the provisions of this Article shall constitute gross negligence on their part in respect with the use of the Service.

4. (Amended, in force as of 12 September 2018) Upon the provision of the Service, the Bank shall make available to the Account Holder and the Authorized Holder, depending on their rights, electronic information on the balance and availability on the Account(s) and/or on the movement of the funds on the Account (including chronological information on operations/transactions), whereby the content of the information shall be consistent with the provisions of Article 65(1) and Article 66(1) PSPSA, as far as it is applicable. The Account Holder and the Authorized Holder are required to get acquainted with the information referred to in the preceding sentence (including the balances and the executed payment operations on the Account(s) through the Service) at least once a month, whereby the failure of the Account Holder/Authorized Holder to comply with the provisions of this Article shall constitute gross negligence on their part in respect with the use of the Service.

5. If the Account Holder and the Authorized Holder fail to implement their obligation under the previous Article or the Bank does not receive a written objection from the Account Holder or the Authorized Holder (regarding the transactions ordered by the latter) within 60 days from the date of the execution of the respective payment transaction, the Account Holder and the Authorized Holder shall be considered to have read and approved the information under the preceding Article and the executed payment services and operations specified therein. The notification to the Bank after this period shall be considered unreasonable delay by the Account Holder and/or the Authorized Holder.

6. The Account Holder is required to ensure available amount on the Account, including for the payment of all necessary fees and commissions under the Agreement.

7. The Authorized Holder is required to log out the Service using the "Exit" button of the application, otherwise when re-entering, the Authorized Holder may be restricted to access the Service for a period of 15 minutes.

8. The Account Holder and/or the Authorized Holder shall promptly provide the documents and information required by the Bank in connection with the implementation of the Bank's obligations under the Measures against money laundering Act and the regulations on its implementation.

VIII. SECURITY

1. (Amended, in force as of 14 September 2019) The Authorized Holder or the Account Holder, respectively, shall be required to keep secret their Access code, Mobile banking code, PIN for the access to m-Token Postbank, as well as to prevent the unauthorized use by third parties of the mobile device with installed application for Mobile banking (m-Postbank), the mobile

device with installed application m-Token Postbank, PST, as well as all other tools for their electronic identification before the Bank.

2. (Amended, in force as of 14 September 2019) The Authorized Holder or the Account Holder, respectively, shall be required to immediately notify the Bank or a person authorized by it on phone: 0 700 18 555 (+359 2 816 60 00 if dialled from abroad) or in any of its financial centers, in case of:

2.1. loss, theft or misappropriation of any of the PSTs or a mobile device on which the m-Token Postbank application or the Mobile banking application (m-Postbank) is installed;

2.2. knowledge or suspicion or assumption of unauthorized use of any of the PSTs or a mobile device on which the m-Token Postbank application or the Mobile banking application (m-Postbank) is installed, including, but not limited to the circumstance that the Access code, the Mobile banking code, PIN for access to the m-Token Postbank application or other PSTs have become known to third parties other than the Authorized Holder;

2.3. knowledge or suspicion or assumption of other unauthorized access to the Service, or of using the Service or the PSTs in another illegal manner;

2.4. knowledge or suspicion or assumption of an unauthorized or incorrect payment transaction executed through the Service.

After receiving the notification, the Bank shall take the necessary actions to block the access to the Service and in the cases where applicable - to deactivate the Software Token.

3. (Amended, in force as of 14 September 2019) The Bank shall not be liable for any adverse consequences arising as a result of third party becoming aware of the Authorized Holder's PST prior to the receipt of the notification, unless such liability is expressly provided for in the General Terms and Conditions for bank accounts and/or in the applicable Bulgarian legislation.

4. (Amended, in force as of 14 September 2019) The Bank is entitled to block the access of any Authorized Holder/Account Holder to the Service, and in cases where applicable - to deactivate the Software Token, for objective reasons related to:

- The security of the Service and/or the PST;
- Suspicion of unauthorized use of the Service and/or the PST;
- Suspicion of use of the Service and/or the PST for fraudulent purposes (suspicion may arise, including, but not limited to, upon the receipt by the Bank of a request for reverse/notification for fraudulently ordered transfer by or in favour of an Authorized Holder/Account Holder);

5. (Amended, in force as of 14 September 2019) In case of deactivation of the Software Token, the Authorized Holder may activate a new token according to the procedure under Article V.11 et seq.

6. The Bank shall temporarily suspend the access to the Service in the event of one of the following circumstances:

6.1. Receipt in the Bank of an attachment notice on the Account or on any/all accounts of the Account Holder with the Bank, in which case the access to the Service shall only be suspended regarding the execution of transfers and other transactions on the respective Account(s) for which the attachment notice has been received up to the amount of the imposed attachment;

6.2. Violation of the requirements of the effective regulations, the Agreement and/or these General Terms and Conditions or endangering the security of the system by the Authorized Holder / Account Holder;

6.3. At the request of the Account Holder or the Authorized Holder, when the request for blocking the access is made by phone call;

6.4. Upon the receipt of a written request from the Account Holder or the Authorized Holder.

7. In the cases under Article VIII.4-VIII.6, the Bank shall notify the Authorized Holder of the blocking and the reasons thereof as soon as possible (before the blocking and immediately thereafter), including by telephone, unless the provision of such information is prohibited for reasons for security or certain regulatory requirements.

8. The Bank shall restore the access to the Service in case the grounds for termination cease to exist. If the blocking has been performed on the grounds of Article VIII.5 and Article VIII.6.3 and 6.4, the Bank shall restore the access to the Service in case the grounds for blocking cease to exist and after a joint written request has been submitted by the Account Holder and in the Bank's financial center.

9. The Bank shall permanently terminate the access to the Service upon providing information and evidence of the death of the Authorized Holder.

IX. CHALLENGING OF PAYMENTS AND OBJECTIONS

1. (Amended, in force as of 12 September 2018) The Bank shall correct an unauthorized or incorrectly executed payment transaction from an Account only if the Account Holder and/or the Authorized Holder have notified the Bank in writing without unreasonable delay within the meaning and within the term of Article VII.5 of these General Terms and Conditions after becoming aware of the unauthorized or incorrectly executed payment transaction. The Bank undertakes to assist in resolving the cases of disputed transactions/operations and shall decide on the relevant objections according to the procedure and within the time limits provided for in the applicable law, the relevant internal rules and procedures of the Bank, as well as in this section of the General Terms and Conditions herein.

2. (Amended, in force as of 14 September 2019) In the cases where the Account Holder and/or the Authorized Holder notify(ies) the Bank of the existence of an unauthorized payment transaction executed by fraud by a third party or as a result of stolen or misappropriated PSTs and/or mobile device with installed m-Token Postbank application and/or m-Postbank application, the Authorized Holder or the Account Holder, respectively, shall notify the competent authorities of the Republic of

Bulgaria and provide evidence to the Bank thereof. By accepting these General Terms and Conditions, the Account Holder or the Authorized Holder, respectively, confirm(s) to be aware that upon failure to provide such evidence, the Bank may consider this fact, including if there are other circumstances in this regard, as an indication of the existence of reasonable suspicion of fraud and notify the competent authorities in the Republic of Bulgaria and refuse the reversal of the value of the unauthorized payment transaction under Article 79(1), sentence 1 of the PSPSA.

3. (New, in force as of 12 September 2018) Based on the written notification referred to in clause 1 above, received within the time limit referred to in Article VII.5 of these General Terms and Conditions, the Bank shall, in accordance with its internal procedure, initiate actions for resolving the cases of disputed payment transactions (including actions against the payment service provider servicing the payee of the executed payment transaction in cases where the payment order has been received through the payee and its provider).

4.1. (New, in force as of 12 September 2018) The Bank shall inform in writing the Account Holder and/or the Authorized Holder of its decision on the received objection immediately after the completion of the procedure for proving the authenticity and the exact execution of the disputed payment transaction.

4.2. (New, in force as of 12 September 2018) In case the procedure under the preceding clause has been completed within the business day following the day of the receipt of the written notification of unauthorized payment transaction and the Bank has found the written notification to be justified and the circumstances under Article X.3 herein are not present, it shall immediately reverse the value of the unauthorized payment transaction.

4.3. (New, in force as of 12 September 2018) In case the procedure has not been completed within the time limit specified in the preceding clause, the Bank shall immediately reverse the value of the unauthorized payment transaction not later than the end of the business day following the day of the receipt of the written objection, by blocking the reversed funds on the Account until the end of the procedure.

4.4. (New, effective of 12.09.2018) If after the completion of the internal procedure the Bank has found the written notification under clause 1 above to be well founded, it shall release the blocked funds immediately.

4.5. (New, in force as of 12 September 2018) In all cases of reversal, the value date for crediting the Account shall be no later than the date on which the Account was debited with the amount of the unauthorized payment transaction.

4.6. (New, in force as of 12 September 2018) In the cases where, after the completion of the internal procedure, the Bank has found the written notification under clause 1 above to be unfounded or in case the circumstances under Article X.3 below are present, the Bank shall refuse to reverse the funds / debit in its favour the Account with the amount of the reversed and blocked

funds on the Account, for which the Account Holder gives explicit consent under Article 21 of Ordinance 3 by accepting these General Terms and Conditions.

4.7. (New, in force as of 12 September 2018) The Bank shall refuse to reverse the amount of the disputed payment transaction in the presence of reasonable suspicions of fraud, after notifying the competent authorities in the Republic of Bulgaria.

4.8. (New, in force as of 12 September 2018) The Bank shall also reverse the amount of unauthorized transaction in other cases where there is such an obligation for the Bank in the applicable legislation.

5. (Amended, in force as of 12 September 2018) In case of inaccurate, including delayed execution of a payment transaction, the relations between the Parties shall be settled in compliance with the General Terms and Conditions for bank accounts applicable to the respective Account(s).

6. In case of unjustified dispute of a transaction/operation executed while using the Service, the party disputing the transaction/operation - the Authorized Holder or the Account Holder, respectively, shall be required to pay a fee according to the Bank's Tariff. It will be considered unjustified to dispute the difference in the amount of the transaction and the amount posted to the Account in case of currency conversion when the difference is due to a discrepancy between the date of the transaction and the date of its posting in the Bank and the difference in the applied exchange rates for the relevant dates and currencies. The wording of the preceding sentence does not constitute an exhaustive list of cases of unjustified dispute of transactions/operations.

X. LIABILITY OF THE PARTIES

1. The Authorized Holder and the Account Holder shall be liable under the conditions of solidarity for all obligations arising from the use of the Service.

2. (Amended, in force as of 12 September 2018) The Account Holder/Authorized Holder shall bear the losses related to all unauthorized payment transactions resulting from the use of a lost, stolen or misappropriated payment instrument where the Account Holder/Authorized Holder has failed to maintain the personalized security features of the Service, but not exceeding BGN 100. This provision shall not apply if: (i) the loss, theft or misappropriation of the payment instrument could not have been established by the Account Holder/Authorized Holder prior to the payment, unless they have acted fraudulently, or (ii) the damage was caused by the act or omission of an employee, representative or branch of the Bank or subcontractor of the Bank.

3. (Transferred into a new clause, in force as of 12 September 2018) The Account Holder/Authorized Holder shall bear all losses incurred in connection with unauthorized payment transactions, regardless of their amount, if they have been caused by fraud or intentional non-performance or due to gross negligence of one or more of their obligations under the Agreement and these General Terms and Conditions.

The failure of the Account Holder and/or the Authorized Holder to immediately notify the Bank of the circumstances under Article VII.2, as well as their failure to prevent third party from knowing the Access code and/or other personalized security features of the Service, shall constitute gross negligence of the Account Holder/Authorized Holder. The failure to provide antivirus software (latest version) or use of the Service by computers to which other persons have access is a case of gross negligence of the Account Holder/Authorized Holder. The wording of this provision does not constitute an exhaustive list of all cases of gross negligence by the Account Holder and/or the Authorized Holder.

4. (New, in force as of 12 September 2018) In the cases under Article 80(4) PSPSA, clauses 2 and 3 above shall not apply, except where the Account Holder/Authorized Holder has acted for the purpose of fraud.

5. (Amended, in force as of 14 September 2019) The Authorized Holder and the Account Holder shall be liable to the Bank for all damages caused by improper use of the Service and/or storage of the Access code and/or PSTs.

6. (Amended, in force as of 14 September 2019) The Bank shall not be liable for any damages caused during the use of the Service if before receiving the notification under the previous provision it has executed in good faith an order to perform an operation placed by a person who, on the basis of unambiguous circumstances, was authorized to do so. In such cases, the liability of the Authorized Holder/Account Holder may only be limited in the presence of a mandatory provision in the applicable legislation at that time, stipulating this limitation, and to the amounts specified therein. In all cases where the transaction is executed on the basis of a positive electronic identification (by entering the Mobile banking code, the Access code, the Biometric data registered in the operating system of the mobile device and the use of PSTs), it shall be assumed that the person who executed it was unequivocally authorized to carry the execution. The wording of the preceding sentence does not constitute an exhaustive list of unambiguous circumstances within the meaning of this provision.

7. (Amended, in force as of 12 September 2018) The Bank shall not be liable where due to objective circumstances beyond its control, such as force majeure or other extraordinary circumstances, the Authorized Holder/Account Holder is not able to use the Service, including but not limited to failure of the information system, interruption of communication lines, power failure, etc.

8. (Amended, in force as of 8 May 2021) The Bank shall not be liable where the Authorized Holder fails to receive an SMS or another electronic message sent in accordance with these General Terms and Conditions due to the lack/termination of contractual relations of the Authorized Holder with a mobile operator and/or other technical reasons (lack of scope, roaming, coverage, switched off telephone, etc.) or if the Authorized Holder has changed his/her mobile phone number / mobile operator without notifying the Bank, as well as in case of

loss or theft of a mobile phone or other circumstances with a similar effect.

9. (New, in force as of 16 July 2018; amended, in force as of 12 September 2018) The Bank shall not be liable for executed orders and actions under a power of attorney, unless it has been notified in writing in accordance with the procedure established by it that the power of attorney has been revoked, and before the receipt of the notification it has executed in good faith an order of a person who, on the basis of unambiguous circumstances, appears authorized to carry out the order / action.

XI. FEES AND COMMISSIONS

1. (Amended, in force as of 12 September 2018) When ordering and using the Service, the Account Holder shall have to pay the Bank fees and commissions according to the effective Tariff of the Bank. The Bank shall be entitled to unilaterally change the amount of due fees and commissions, as well as to introduce new fees and commissions, for which it shall notify the Account Holder and the Authorized Holder in compliance with Article XIII.5 of these General Terms and Conditions. When the changes in the due fees and commissions are more favourable for the Account Holder/Authorized Holder, they shall be applied without prior notice.

2. The Bank shall be entitled to collect ex officio the fees and commissions due by the Account Holder and the Authorized Holder from all accounts of the Account Holder and/or the Authorized Holder opened with it, for which the Account Holder and the Authorized Holder give their explicit, irrevocable, and unconditional consent by signing the Agreement (including the annexes/addenda thereto).

XII. TERMINATION OF THE CONTRACTUAL RELATIONS

1. The Agreement for the provision and use of the Internet Banking service shall be concluded by the Parties for an indefinite period.

2. The Account Holder may unilaterally terminate the Agreement without giving a specific reason with one month's written notice to the Bank.

3. The Bank shall be entitled to unilaterally terminate the Agreement with the Authorized Holder and/or the Account Holder without giving a specific reason with two months' written notice. The notice under this Article shall be provided to the Account Holder/Authorized Holder in hard copy or other durable medium (including by email) to the correspondence address(es) specified in the Agreement.

4. The Bank shall be entitled to unilaterally terminate the Agreement with the Authorized Holder and/or the Account Holder without notice in the event that the Authorized Holder and/or the Account Holder fail(s) to implement their obligations under these General Terms and Conditions or under the Agreement.

5. The Agreement shall be considered terminated in case of receipt of a written notification for incapacitation of the Account Holder or any Authorized Holder, whereby in the

latter case the termination shall be considered valid for the respective Authorized Holder only.

6. (Modified, in force as of 8 May 2021) If within 6 (six) months from the date of the conclusion of the Agreement, the Authorized Holder does not use the Activation Code for initial signing up for the Service, then the access of the latter to the Service shall be automatically blocked, and the subsequent unblocking of the access to the Service shall be effected by submitting a form to any financial center of the Bank, signed by the Account Holder and the Authorized Holder.

7. (Modified of 23 January 2021) If the Authorized Holder is also at the same time a proxy of the Account Holder with the right to dispose of the amounts available in the Accounts of the latter, in case the Account Holder/the legal representatives of the Account Holder notify the Bank in writing by appearing in person in a financial center of the Bank, by sending a notice by mail with acknowledgement of receipt, by registered mail, by notarized invitation for withdrawal of the power of attorney and termination of the powers of the Authorized Holder to access and/or dispose of the amounts available in the Account, upon expiration of the term of the power of attorney, as well as upon the termination of its validity on other grounds pursuant to the law or the provisions of the power of attorney, the Service Agreement shall be considered terminated in respect of the Authorized Holder unilaterally and without notice by the Bank and the access of the Authorized Holder to the Service shall be terminated. In such cases, the Agreement shall remain in force with respect to the Account Holder and the other Authorized Holders, if any.

8. (Modified as of 23 January 2021) The Bank shall be entitled to unilaterally terminate without notice the Agreement with the Authorized Holder and to terminate the access of the latter to the Service, in case it becomes aware that the rights of the Authorized Holder to dispose of the amounts available in the Account have been terminated on any grounds, including if it finds or is notified in writing by the legal representatives of the Account Holder by appearing in person in an office of the Bank, by sending a notice by mail with acknowledgement of receipt, by registered mail, by notarized invitation for withdrawal of the power of attorney or deletion of the registration of the Authorized Holder as a legal representative/Procurator of the Account Holder with the Commercial Register and the Register of Non-Profit Legal Entities (CRRNPLE). In such cases, the Agreement shall remain in force with respect to the Account Holder and the other Authorized Holders, if any.

8.a (New, in force as of 23 January 2021) The Service Agreement shall remain in force for an Authorized Holder authorized in compliance with the requirements for the powers of attorney under Section III of these General Terms and Conditions, provided that after the date of the power of attorney, the persons who have signed it lose their authority to represent the Account Holder. Such power of attorney may be withdrawn by written notice to the Bank sent by the Account Holder/legal representatives of the Account Holder by appearing in

person in a financial center of the Bank, by sending by mail with acknowledgement of receipt, by registered mail, by notarized invitation.

9. (Previous Article XII.7, amended, in force as of 14 September 2019) The Authorized Holder and the Account Holder shall remain liable to the Bank until the repayment of all obligations related to the use of the Service, including after the termination of the Agreement, regardless of the grounds for termination.

10. (New, effective as of 14 November 2019) Upon the termination of all agreements for Accounts and all banking products used by the Account Holder with the Bank, the Agreement and the access to the Service shall be automatically terminated.

XIII. SUPPLEMENTARY PROVISIONS

1. (New, in force as of 16 May 2018) The Bank processes personal data in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("General Data Protection Regulation"). For detailed information on the purposes and legal basis for the processing of personal data; the categories of recipients of personal data; the period of retention of personal data; the rights of data subjects in connection with the processing of their personal data by the Bank, as well as information on the methods in which they may be exercised; contact details of the Data Protection Officer and any other information required to be provided to data subjects under the General Data Protection Regulation, see the Privacy Notice available on the Bank's website (www.postbank.bg), as well as on paper in each office of the Bank.

2. These General Terms and Conditions, including the information on the minimum technical requirements, shall be provided to the Account Holder/Authorized Holder in hard copy or on other durable media (including by sending by e-mail or publishing them on the Bank's website (www.postbank.bg) in the form of understandable text and in accessible form in Bulgarian). During the validity of the Agreement, the Account Holder/Authorized Holder shall be entitled to receive upon request the terms and conditions of the Agreement, as well as these General Terms and Conditions, including the minimum technical requirements, in hard copy or on other durable media.

3. All notices and statements in connection with the Agreement must be made by the Parties in writing and in Bulgarian and shall be deemed to have been received if sent by fax, by delivery in person or by mail with acknowledgement of receipt, or by registered mail, or by e-mail, reached to the addresses of the Parties (respectively to the e-mail addresses) specified in the Agreement and in the General Terms and Conditions, as well as if provided to the Account Holder/Authorized Holder by the use of the Service or by publishing them on the Bank's website referred to above, unless otherwise stated in these General Terms and Conditions. The following e-mail address shall be valid for sending notifications and statements by e-mail to and from the Bank: info@e-postbank.bg.

4. (Amended, in force as of 14 September 2019) The Parties agree that in connection with the notices to the Account Holder/Authorized Holder provided through the respective Internet service provider, including under Article XIII.7, the Bank shall not be liable for non-receipt or untimely receipt of the notices when the non-receipt or the untimely receipt, respectively, is due to reasons beyond the control of the Bank (for example: problems in the transmission communication environment of the respective Internet service providers, force majeure, etc.), as well as in the cases of termination of the contractual relations between the Bank and the respective Internet service provider, regardless of the reason for such termination.

5. (Amended, in force as of 12 September 2018) The Bank shall reserve the right to unilaterally change these General Terms and Conditions, including the Tariff and the Interest Rate Bulletin, including, but not limited to, the cases where this is required by changes in applicable law, changes in the Bank's practices in offering the Service or changes in the specifics/functionality of the Service itself, making such changes available to its clients by publishing them on the Bank's website - www.postbank.bg before their entry into force. From the time of their entry into force, they shall be binding on the clients. In the cases where the Account Holder is a user within the meaning of the PSPSA, the Bank shall make available to the Authorized Holder and the Account Holder the changes according to the procedure provided for in this Section not later than two months before the date on which the changes take effect. If the Authorized Holder/Account Holder does not accept the proposed changes, they shall be entitled to object to them by terminating the Agreement within the two-month period under the previous sentence, without being liable for any costs and expenses in relation with the termination. If the Authorized Holder/Account Holder fail to terminate the Agreement according to the procedure under the preceding Article, they shall be considered to have accepted the proposed changes and the changes shall become binding on them as soon as they become effective. In cases where the Account Holder is not a user within the meaning of the PSPSA, the changes in these General Terms and Conditions shall enter into force for them as soon as they are accepted by the Bank, unless they should become effective at a later date pursuant to the decision on their acceptance or in compliance with the applicable legislation.

6. In the event of changes in the legislation governing the relations regulated in these General Terms and Conditions, the relevant provisions of the General Terms and Conditions shall be amended accordingly as soon as the changes become effective, unless the change concerns provisional legal norms.

7. (Amended, in force as of 14 September 2019) The Authorized Holder and the Account Holder shall be bound to notify the Bank of any changes in the initial data provided by them upon signing the Agreement, including any changes in the relevant address (including e-mail) and mobile phone numbers specified in the Agreement

within 7 days from the occurrence of the respective changes, whereby the declaration of different data from the data specified in the Agreement in a subsequent document signed by the Account Holder/Authorized Holder and submitted to the Bank shall be considered a notification on the occurrence of changes in the data provided upon signing the Agreement. Otherwise, all notices, activation codes of PSTs, invitations, SMS and other messages under these General Terms and Conditions and the Agreement shall be considered received if they are sent to the Authorized Holder and/or the Account Holder at the relevant address (including e-mail) or the mobile phone number specified in the Agreement.

8. The Service may also be used in respect of credit card(s) issued by the Bank without a bank account opened with the Bank. In this case, the Service may only be used for making utility payments and local tax payments under clause III.6.1.2(g) of these General Terms and Conditions, whereby the rules under these General Terms and Conditions for the Account Holder and the Authorized Holder, respectively, shall apply to the rights and obligations of the credit card holder when using the Service. The card holder shall be entitled to request access through the Service only to credit card(s) issued by the Bank for which he/she is personally a card holder and shall be required to use only the credit card in person through the Service. In the event that the credit card holder allows the use of the credit card by another person through the Service, he/she shall be liable to the Bank and to all third parties for all illegally performed transactions through the Service, as well as for all other direct and indirect damages. The provisions of the General Terms and Conditions of Eurobank Bulgaria AD for Issuance and Use of Visa and American Express Credit Cards and the appendices thereto shall also apply to the issues not settled in these General Terms and Conditions regarding credit card transactions made by using the Service.

9. For all issues not settled in these General Terms and Conditions and in the Agreement, the provisions of the legislation in the Republic of Bulgaria in force shall apply.

10. (Amended, in force as of 12 September 2018) In case the Account Holder **is not** a user within the meaning of the PSPSA, pursuant to Article 46(5) and Article 67(4) of the Payment Services and Payment Systems Act, the provisions of Chapter IV of the PSPSA and Article 68(1), Article 78, the restriction in the scope and amount of losses that may be incurred by the Account Holder/Authorized Holder related to unauthorized payment transactions pursuant to Article 80 PPSA, Article 82(2) and (3), Article 91, Article 92 and Article 93(1) PPSA shall not apply to the Account(s) and the Service, and the Bank shall not be liable to the Account Holder and/or the Authorized Holder pursuant to the foregoing provisions in this Article, and the Account Holder and/or the Authorized Holder may not file claims against the Bank on the basis thereof and/or the provisions of these General Terms and Conditions that implement them.

In case the Account Holder is a user within the meaning of the PSPSA, the Bank shall submit a report on the fees in compliance with Article 106 PSPSA, with a minimum content consistent with Article 107 PSPSA, which is to be received upon request, free of charge, once a year, in hard copy, in n any financial center of the Bank, and without revoking this right, the report may be received through inquiries in the Service, if there is such functionality.

11. (Amended, in force as of 8 March 2021) In case of a written objection or complaint received by the Bank concerning the relations between the Bank and the Authorized Holder/Account Holder, regulated by these General Terms and Conditions and the Agreement, the Bank shall consider the case and notify the Authorized Holder/Account holder in Bulgarian, in writing, in hard copy or by e-mail, for its decision within 15 working days of the receipt of the objection or complaint. Exceptionally, when the Bank is unable to rule within the period specified in the preceding sentence for reasons beyond its control, the Bank undertakes to send to the Authorized Holder/Account Holder a reply in which it shall clearly state the reasons for the delay and the deadline in which the Authorized Holder/Account Holder will receive the decision of the Bank. Nevertheless, the Bank shall notify the Authorized Holder/Account Holder of its decision on the objection or complaint within 35 business days after the receipt of the objection or complaint. If the Bank fails to notify the Authorized Holder/Account Holder within the above deadline or the Bank's decision is not acceptable to them, they may refer the dispute for consideration by the Conciliation Committee for Payment Disputes at the Commission for Consumer Protection. The address of the Commission for Consumer Protection is: 1 Vrabcha Street, fl. 3, 4 and 5, 1000 Sofia. Additional information on the Conciliation Committee for Payment Disputes at the Commission for Consumer Protection and the conditions for its referral is available on the Bank's website - www.postbank.bg, Client Relations Section, in its financial centers, as well as on the website of the Conciliation Committee for Payment Disputes at the Commission for Consumer Protection - <https://abanksb.bg/pkps/>.

12. The disputes between the Parties shall be resolved by mutual agreement, and in case such is not achieved, the dispute is to be resolved by the competent Bulgarian court in compliance with the procedure under the Civil Procedure Code, and for clients who are not consumers within the meaning of the PSPSA, the dispute shall be resolved by the competent Bulgarian court in Sofia.

These General Terms and Conditions of Eurobank Bulgaria AD for Electronic Banking Services "Internet Banking" for Individual and Corporate Clients are published on the Website at www.postbank.bg, as last amended and supplemented in force as of 30 August 2021.