ERSTE BANK A.D. NOVI SAD
BOARD OF DIRECTORS
Number: 1436/2026-562/7-3
Date: 17.03.2026.

GENERAL TERMS OF PROVIDING PAYMENT SERVICES TO CORPORATES

I. INTRODUCTORY PROVISIONS

Article 1
In the General Terms of Providing Payment Services (hereinafter: General Terms) to Corporates (hereinafter: User), Erste Bank a.d. Novi Sad (hereinafter Bank) shall, as the payment service provider, set out the mutual rights and obligations relating to payment service execution in accordance with the Law on Payment Services (Official Gazette no. 139/2014 and 44/2018) and the accompanying by-laws.

Terms
Article 2
1) payment transaction means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;
2) payment order means any instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction;
Payment order means order in hard copy issued by the consumer at the Bank business units, verbal order approved by the Bank for individual Users as the method of issuance, e-order electronically issued by user to the Bank
in the manner approved by the Bank (e-mail, fax), and order issued using the Bank application for Internet payments the so-called E-Bank and an order issued using the Bank application for M-Bank;
3) e-payment order means electronic message containing instruction which is electronically generated, sent, verified, received, processed, and stored;
4) payment account means account used for executing payment transactions, maintained by payment service provider; Payment account may be current or other payment account;
5) current account is payment account maintained with the Bank, used for executing payment transactions and for other purposes relating to services provided by banks to payment service users.
6) payment instrument means any personalised device and/or a set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to issue or initiate a payment order;
7) payment card means a payment instrument issued to the User based on request for payment card issuance opted for by the User in the course of account opening or subsequently in the course of the account maintenance.
8) payment service user means, in sense of these General Terms, a legal entity that uses or has used a payment service in the capacity of a payer and/or payee or has addressed the payment service provider in order to make use of such services;
9) payer means a natural person or legal entity that issues a payment order from its payment account or gives consent to execute a payment transaction based on the payment order issued by a payee, or, if there is no payment account, a natural or legal person that issues a payment order;
10) payee means a natural or legal person designated as the recipient of funds subject to a payment transaction;
11) business day means a day, namely part of the day in which the relevant payment service provider of the payer or of the payee involved in the execution of a payment transaction is open for business as required for the execution of a payment transaction to its payment service user;
12) credit transfer means a payment service where the payer instructs the payment service provider to initiate the execution of one or more payment transactions, including issuing of a standing order, at the charge of payment account, including standing order issuance, after which payee's payment account shall be approved in the amount of payment transaction;
13) credit instant transfer means domestic payment transaction in RSD which may be initiated by a payer at any time of day, every day in year, and the transfer is executed instantly or almost instantly through the National Bank of Serbia IPS payment system.
14) direct debit means a payment service where a payee, based on the payer's consent, initiates a payment transaction to debit the payer's payment account. The payer may give such consent to the payee, its payment service provider or payee's payment service provider.

15) standing order means an instruction given by the payer to the payment service provider which holds the payer's payment account to execute credit transfers at regular intervals or on predetermined dates;
16) value date means a reference date, that is, reference time used by a payment service provider for the calculation of interest on funds debited from or credited to a payment account;
17) reference exchange rate means the exchange rate which is used as the basis to calculate any currency exchange which is made available by the payment service provider or comes from a publicly available source;
18) reference interest rate means the interest rate which is used as the basis for calculating interest which is publicly available and is determined independently of the unilateral will of the payment service provider and the user which have entered into a payment service agreement;
19) unique identifier means a combination of letters, numbers and/or symbols specified to the payment service user by the payment service provider to be used in a payment transaction to identify unambiguously the respective payment service user and/or its payment account;
20) domestic payment transaction means a payment transaction in which the payer's payment service provider and payee's payment service provider provide the service within the territory of the Republic of Serbia;
21) international payment transaction means a payment transaction where a payment service provider provides this service in the territory of the Republic of Serbia, and another one provides such service in the territory of a third state, as well as the payment transaction where the same payment service provider provides such service to a payment service user in the territory of the Republic of Serbia, and for the same or another payment service user in the territory of a third state; transactions in dinars between residents and non-residents as well as transactions in dinars between residents shall be deemed as international payment transactions;
FX account which ensures payment process automation in international payments;
22) PIN (Personal Identification Number) means a personal identification number assigned to the User for payment instrument, used for unambiguous identification of the User and granting of consent for payment transaction execution;
23) payment system means a system for the transfer of funds between its participants with written and standardised procedures and rules for the processing, netting, and/or settlement of transfer orders, applied to all participants in the system.
24) NBS IPS system means a system the operator of which is the National Bank of Serbia which enables the payment service providers to execute single instant credit transfers (instant payments) 24 hours a day, seven days in week, 365 days in year (24/7/365) almost instantly, i.e. within only a few seconds.
25) corporate entities – legal entities, authorities, and organisations of government, government administration authorities, local government units, associations, and societies (sport, culture, charity, etc.), and other legal entities.
26) Bank acts – in sense of the provisions of the General Terms of Business means any documents and decisions which are, according to prescribed procedure, passed by the Bank authorised bodies and made available to the User through individual Distribution Channels, governing the rights, authorisations, and obligations of the User, User's Representative, and any other persons assuming the rights and obligations for the User to the Bank as well as of the Bank itself (for example: General Terms of Business of the Bank, Price Lists, decisions on fees, etc.)
27) Distribution Channels – means any methods and means through which access, agreement, and use of the Bank product or service are possible. Within the wording of the General Terms, the term "distribution channel" may mean one of the following: Bank business unit (branch, sub-branch, teller desk), Internet presentation of the Bank http://www.erstebank.rs (hereinafter: web page), E-Bank, M-Bank, ATMs, and other determined by the Bank to be a distribution channel for specific product or service.
28) Account – means any current and other payment account opened at the Bank, used for the execution of payment transactions in local and foreign currency as well as for other purposes relating to payment transaction services.
29) payment account change means a service provided by the payment service provider to the User, in accordance with the Law on Payment Services.
30) Payer's payment service provider means a bank where the account of the person who is debited in the amount of the payment transaction initiated by such person as the payer is maintained
31) Payee's payment service provider means a bank where the account of the person who is debited in the amount of the payment transaction initiated by such person as the payee is maintained.
32) remote payment transaction means a payment transaction initiated via internet or through a device that can be used for distance communication;
33) payment transaction initiation means the taking of actions which are a precondition for starting the execution of a payment transaction, including payment order issuance and authentication;

34) payment transaction initiation provider performs the service where, upon the request of payment service user, payment order shall be credited to the payer's payment account held with other payment service provider;
35) Provider of service of account information shall perform the service provided through the Internet, providing grouped information on one or multiple payment accounts a payment service user holds with other payment service provider or multiple payment service providers
36)) authentication means a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;
37)) strong customer authentication means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;
38)) personalised security credentials mean personalised data and features provided by the payment service provider to a payment service user for the purposes of authentication;
39) Issuing of payment instruments means a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions with such payment service provider;
40) Acquiring of payment transactions means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee;
41) IBAN (International Bank Account Number) means the international identification number of a payment account, used to designate a payment account in accordance with the decision establishing the unique structure for the identification and classification of accounts and the chart of accounts for the application of international rules and the IBAN standard, which is used for the unambiguous identification of a payment account;
42) 3D Secure (3DS) is a security protocol used for the protection of on-line payment using cards (debit and credit). The purpose thereof is to provide an additional authentication layer to reduce the risk of non-authorised transactions;
43) Single Euro Payments Area – SEPA (hereinafter: SEPA area) means the territorial area comprising the Member States of the European Union and other states or territories that have met the criteria for accession to the SEPA area, as well as the regulations of the European Union and the rules, practices, standards, and guidelines contained in the SEPA rules for the execution of payment transactions, within which payment transactions are carried out in a mutually harmonised manner, under equal conditions and with equal rights and obligations, in accordance with those acts. The list of the SEPA area countries is available at https://www.europeanpaymentscouncil.eu/document-library/other/epc-list-sepa-scheme-countries;
44) SEPA rules for the execution of payment transactions (payment scheme) denote a unified set of rules, practices, standards and/or operational guidelines for executing payment transactions – agreed upon by payment service providers for the purpose of executing payment transactions – which is separate from any payment infrastructure or payment system that supports the implementation of that set of rules, practices, standards and/or operational guidelines;
45) SEPA Credit Transfer means a domestic and international payment transaction executed via a credit transfer in euros within the SEPA area. Credit transfer means a payment service whereby the payer, with the payer's payment service provider, initiates the execution of one or more payment transactions to debit the payer's payment account, after which the payee's payment account is credited with the amount of that payment transaction or those payment transactions;
46) mTOKEN means a program connected to the User's mobile device through the mobile banking application, which enables authorisation and authentication.

II PAYMENT SERVICES

Article 3
The Bank shall execute the following payment services:
1) services of account opening and maintaining and closing
2) services ensuring incoming payment of cash on payment account, services necessary for such account opening, maintaining, and closing;
3) services ensuring outgoing payment of cash on payment account, as well as any services necessary for such account opening, maintaining, and closing;
4) fund transfers from/to a payment account, in one of the following ways:
(1) credit transfers,
(2) direct debit, including one-off direct debit,
(3) using a payment card or similar means;
5) execution of payment transactions where funds are covered by a credit line for a payment service user, in one of the following ways:
(1) credit transfers,
(2) direct debit, including one-off direct debit,
(3) using payment card or similar means;
6) issuing and/or acquiring payment instruments where the payment service provider enables to the payee the execution of payment transactions initiated by the payer using particular payment instrument;

A user who has activated eBanking and/or mBanking service (has access to its payment account through Internet) shall be entitled to use the payment initiation service provided by the payment initiation service provider and the service of the provision of information on account provided by the provider of the service of providing account information. If the user intends to use these services, the User shall arrange such services with the payment initiation service provider or with the account information service provider. The Bank shall not, in any manner whatsoever, be responsible for the obligations resulting from the agreement of the User and such service provider. Regarding the payment orders received through the payment initiation service provider, the Bank will act in the same manner as in the event of the orders issues directly from the User, save for objective reasons.

Article 4
Framework Payment Service Agreement

Payment Service Agreement shall be executed as framework payment service agreement.
Framework Payment Service Agreement includes agreement on account opening and maintaining/application form for E-Bank/M-Bank, direct debit form, General Terms, Price List, and the Cut-off Times of the Bank.

Framework agreement is executed in writing in Serbian or both Serbian and English.

The Bank shall ensure that the Payment Service User receives minimum one copy of the framework agreement.

Account Opening and Maintaining

Article 5

The Bank shall open payment account based on completed Account Opening Application and documentation referred to in the List of Necessary Documentation for Account Opening, as well as other documentation concluded by the Bank, in the process of documentation collection, to be necessary for the identification of the User and beneficial owner. In the event the User does not provide the data which would enable the Bank to implement the analysis of the User, in accordance with the provisions on the Law on the Prevention of Money Laundering and Terrorism Financing, the Bank will not onboard the User or it will terminate already established relation.

Distribution Channels – means any methods and means through which access, agreement, and use of the Bank product or service are possible. Documentation shall be provided in writing (original, copy, or certified copy) according to the specification from the List of Necessary Documentation received upon request together with Account Opening Application and it may be overtaken at all of the Bank sales units as well as on the Bank Internet presentation.

When opening current account, the Bank shall provide the User with the data on the number of account serving as unique identification designation of the User in payment transactions, which is to be stated when executing payment services.

Opened account shall be reported to the National Bank of Serbia in the Single Account Register.
The Bank shall reserve the right to reject Application without any obligation to explain its decision to applicant.
The Bank shall enable the User opening a payment account with a new payment service provider to change the payment account in the same currency, solely based on the authorisation by the User submitted in writing to the new service provider, provided that the User has no overdues under such account and that other conditions prescribed in the Law on Payment Services are fulfilled. The Bank shall be entitled to charge the fee for such service, in accordance with the Law.

FX accounts shall be opened and maintained by the Bank for every currency individually.

The Bank may open specific accounts to the User for particular purposes (such as account for the cover of payment to abroad, account of cover – for payment to Kosovo, account for inflows from abroad based on credits, account for inflows from abroad based on donation, account for inflows from Kosovo, etc.).

To such opened accounts, the provisions of agreement on account opening and maintaining which have been executed with the Bank, existing signature specimen, and e-bank authorisations apply.
The client will be notified on transactions on specific accounts by the Bank through statements from such accounts.

If the User needs to execute payment transactions in a currency which is not tied to the account, it is necessary to address the Bank, for the purpose of opening of the account in such currency;

Article 6
The first business relation of the Bank and User shall be exclusively established in personal contact of the Bank personnel and representative or other persons of User authorised for such operations.

The Bank may identify representative excluding his/her presence in person, through qualified e-certificate.

In proxy/power of attorney, the User shall state the data on the person who will, on behalf of and for the account of the User, be authorised person to physically bring orders, in the event when orders are issued by the User in hard copy.

The Bank shall be entitled to, upon order receipt, identify person, and reject order execution in the event that order provider is the person not stated as such by User. In this manner, the Bank shall prevent fraud and order execution not approved by the User.

For persons having authorisation to use the E-Bank and M-Bank services, the User shall provide the Bank with the data on the authorised persons, in accordance with the rules of the E-Bank and M-Bank use.

Payment Account Change

Article 6a

Payment Account Change means a service that the Bank will enable a User opening or holding an account at a new payment service provider (hereinafter: new payment account) to switch payment account in the same currency.
Payment account switch shall solely be made based on the authorisation of the User provided by the User to the new payment service provider (hereunder: Authorisation), with or without closing of the payment account opened with the previous payment service provider.
Based on the authorisation submitted to the Bank as a new payment service provider, the User may determine standing orders, consents for direct debits, incoming payment transfers, and other payment services the execution of which shall be switched to a new payment account provided that the Bank provides such services.
The User shall provide the Bank with the Authorisation in writing, whereby the Bank will immediately upon the receipt of such Authorisation, provide the User with the counterpart or copy as an evidence of receipt. Upon the receipt of the Authorisation, the new and previous payment service provider shall implement the activities set out in the Law, in accordance with the Authorisation.

If the Bank is the previous payment service provider, following the implementation of all necessary activities prescribed in the Law, the Bank will close the account the switch of which is requested provided that the User has provided the consent in the Authorisation for the account closing at the Bank and that the User has no outstanding liabilities on such account. Unless the conditions for closing of the account referred to in this paragraph are met, the Bank will, without delay, notify the User thereof.
Information on the obligations and responsibilities of the previous and new payment service provider, in accordance with the Law, deadlines for the implementation of actions, and the fees charged regarding payment account switch, any data the User must present to the Bank, possibility of extra judicial settlement of disputable relation, in accordance with the Law governing the protection of financial service users, shall be available free of charge, in hard copy or other permanent data carrier, at all Bank branches as well as on the Bank's web site, and, upon the request by the User, will be provided to the User free of charge.
Provisions of this item governing the account switch will also apply to the User's payment account switch with the Bank, i.e. to the payment account switch when the Bank is, at the same time, the previous and new payment service provider.

Data of the User Significant for Safe Payment Service Execution

Article 7

Data of the User significant for safe payment service execution shall include:
- data on legal representative
- data on persons authorised for the disposal of funds on the user's accounts
- data on the persons authorised for issuing electronic payment orders (E-Bank and M-Bank)
- address as well as other contact data of the User
- appointment of proxy holder, procurator, or other person for temporary or restricted representation
- other data registered with the Agency for Business Registers (ABR)
- any change of the above-mentioned data.

Any data relating to private individuals shall be reported by the User by presenting valid identification document and copy of such personal document for the Bank records (for legal representative, procurator, authorised person, and other proxy holder). Application shall also include signature specimen of the private individuals authorised for the disposal of funds from the accounts.
The applicant of the Account Opening Application shall permit the Bank to verify and further process the personal data referred to in the Application, in accordance with the Law on Personal Data Protection and the Bank General Terms of Business.

Article 8
The User shall register any persons and restrictions of such persons for the disposal of funds on accounts.

In the event the Bank enables the User to issue orders in writing or electronically, the persons of the User holding such authorisations must also be reported.

The User shall, without delay, report to the Bank any changes in authorisations or limitations of the disposal of funds, authorised persons authorised for using the E-Bank/M-Bank and execution of agreements, or other limitations in terms of legal transactions during the agreement effectiveness, otherwise, the Bank shall not be liable for any damage sustained by the User if such obligation is not performed.

Article 9
The User shall report the address of its head office, and if such address differs from the address for mail receipt, the User shall report the address for the mail receipt which must include mailing address and electronic i.e. e-mail address, as well as contact telephones and contact persons.

The Bank will define the methods and deadlines of the delivery of regular notifications, such as account balance statements, order execution notification, etc. and it shall be deemed that it has fulfilled its obligation of notification when notifications are delivered to the reported electronic address of the User.

If the User has failed to report the electronic address, the Bank may use the electronic address of the User registered at the BRA for sending of notices.

Any notices/documents may also be submitted to the User through Account Statement (in addition to or in the statement).

General notices relating to the contractual relation of the User and the Bank shall be also delivered by the Bank to the User to its reported electronic addresses.

Unless the User has the electronic address for mail receipt, statements may be overtaken at the Bank's teller desks.

Article 10
Reporting of any changes shall be made by the User to the Bank on form: Data Change Application. For the purpose of the efficiency of change reporting, the Bank shall also temporarily accept electronically delivered report of data change and it shall only consider it as warning for the non-execution of orders or other requests of the User until reporting is personally made in the prescribed form and by filing documentation evidencing reported change. Data Change Application may be downloaded by the User from the web pages and at the points of sale of the Bank.

The User shall fill in and provide the Bank with the respective application, in the event of the change in: any data registered with the Agency for Business Registers, court, and other relevant authorities, any data relating to ownership structure change, any data relating to the change in personal data of the persons authorised for signing and disposal of funds on account, any changes in authorisations of such persons, as well as any changes relating to authorisations provided to special persons by representative.

Timely reporting of change registered in register means reporting of change immediately after such change has been made, without any delay, but no later than 3 days from the occurrence of such change and/or registration at the ABR or within 3 days upon the receipt of the resolution on the change if such change is registered with court or other relevant authority.

Article 11
The Bank shall not be liable and shall not bear any damage of the User arising from the User's failure to report, in an accurate and timely manner, any data relating to private individuals having any authorisations with the User, which may impact the execution of payment services and, in general, any funds of the User held with the Bank.

It shall be deemed that the Bank has performed the obligation of the delivery of any notifications to the User based on the registered or reported mailing address or e-mail address, and it will not be liable for any damage arisen on the side of the User due to the failure of reporting address change.

The Bank shall be entitled to refuse services to the User and block the User's account in the event it is aware of the changes defined in Art. from 6 to 10 which have not been reported to the Bank by the User.

The User shall be liable for any failures or damage which may arise due to the non-compliance with the obligation of the submission of data on arisen changes, as well as due to the failure to be in compliance with the obligation of providing any other data required by the Bank.

The User shall immediately and obligatorily notify the Bank on any unauthorised use of payment services (unauthorised order issuance, internal forgeries, signature misuse, etc.) and on any other security breach it becomes aware of.

The User shall be liable to the Bank for the damage which would arise due to unauthorised and incorrect use of service by the User.

The Bank shall be entitled to stop executing payment services to the User as well as block the User's account in the event it is aware of an unauthorised use of services or breach of any other security form.

III PAYMENT SERVICE PROVISION

Payment Order Issuance Method

Article 12

The Bank shall receive payment orders through its distribution channels, in accordance with the provisions of account opening and maintaining agreement and the provisions of special agreements on the services (Office banking/Novoklik/Erste eBiz, Erste mBiz, payment cards) provided by the Bank relating to such accounts.

Order may be received at the Bank:
- by personal submission at a branch of the Bank, in writing, - electronically via /Novoklik/Officebanking/Erste eBiz, and Erste mBiz application, or by scanning and presenting QR code;
- by e-mail to particular Users
or
- indirectly through a payee (direct debit, submission of bill of exchange for collection, payment card use), and through payment initiation service provider

The Bank shall enable the User to submit payment order and processing of payment order by direct submission of the order for the purpose of execution at teller desk, whereas in the event of the submission of cashless payment orders, submission shall also be possible at specific marked location within points of sale.

The Bank shall, based on operation experience, enable individual Users to electronically submit orders (by e-mail) to specifically provided e-mail addresses of the Bank. In the event of applying such method of order submission, the Bank shall be entitled not to execute order in the event of even slightest suspicion of the accuracy and authenticity of an order as well as to revoke such option at any time.
Submitting orders by e-mail shall not be possible after 30 June 2026.

The User may conclude the E-Bank and M-Bank services with the Bank, which are the Bank applications enabling the User to examine its account balance and initiate payment transactions.
Electronic payment order issued within /Officebanking/Novoklik/Erste eBiz, and Erste mBiz application shall have the force of signed order.

At the Bank points of sale, as well as on the Bank's Internet address, there is the Manual on Domestic and International Payments, the User must comply with.

Order Receipt Time

Article 13
The time for payment order receipt shall be the moment when the Bank directly receives an order from the User unless otherwise is agreed, or indirectly through payee or through payment initiation service provider.
The date when the Bank indirectly receives payment order or when it is received from payee shall be deemed the date of the initiation of payment transaction execution and verification of the conditions of execution.

If payment service User and the Bank determine that payment order execution is to begin on a certain date or on the date at the end of certain period or on the date when the User makes the funds available to its payment service provider – it shall be deemed that payment order is received on such determined date. Unless such date is business day of payment service provider, it shall be deemed that order is received on the next business day of such provider.

For payment transactions initiated with card after the User has given its consent for payment transaction execution and the Bank has implemented authentication procedure, the time of receipt shall be the time when the Bank receives order for debiting the User's account from the payee's payment service provider.

If payment order receipt time is not business day of the Bank and/or if the Bank has received order after particular deadline for payment order receipt in accordance with the Cut-off Times, it shall be deemed that such order is received on the next business day, save in the event of instant payment when the rules for order execution shall apply based on the Cut-off Times for such payment type.

The User’s payment account cannot be debited before the payment order receipt.

Article 14
Orders processed in the manner provided for in Article 13 shall include:
- all internal orders (when order issuer and recipient hold accounts at the Bank),
- external orders (when order recipient holds account at other Bank) up to the amount of RSD 300,000.00.

- external orders designated as urgent (when order recipient holds account at other Bank) up to the amount of RSD 300,000.00.

Orders shall be provided in prescribed form, including obligatory documentation, if such documentation is set out in the regulations as obligatory in addition to the order, compiled by the sequence of time of execution determined by the User.

The User and the Bank may arrange a different appearance of the payment order form.

The User may submit order at any business unit of the Bank where payment services are executed or issue the order through the E-Bank/M-Bank application.

In the event of change of a person in signature specimen, payment services may be executed only upon the submission of new signature specimen to the Bank.

The User shall be liable for the accuracy of all data in Order and it shall bear the risk of inputting incorrect data and fraud. Any damage arising from the non-compliance with this provision shall be borne by the User.

The Bank shall not be liable in the event when Order is rejected in payment system or
when it is not possible to execute it in a correct and timely manner due to the User's error.

Any orders in the amount exceeding the amount set out in the Law on the Prevention of Money Laundering and Terrorism Finance or orders for the execution of which documentation is prescribed must be provided together with the documentation confirming payment grounds. In the event of submission of order at the Bank teller desk, original documentation shall be presented to the Bank for examination, and the Bank shall keep documentation copy. In the event of order issuance through the E-Bank/M-Bank, documentation shall be submitted via the application (if the application supports such functionality) or by e-mail, whereby the bank shall be entitled to request to be provided with the original for examination.

Orders in which the User requires payments for which obligatory submission of documentation is prescribed as the evidence and/or grounds relating to transaction shall solely be executed by the Bank if prescribed documentation is presented and if such documentation corresponds to the payment nature referred to in the order.

Article 15
Orders must be filled in a legible, clear, and unambiguous manner. Any data required in order form must be filled in, stating execution date, and including obligatory signatures of persons authorised for signing order.

Signatures on Order must be identical to signatures in signature specimen. If the User wants to use the stamp in the operation with the Bank, it must be separated from signature in respective Order, i.e. stamp imprint must not be put over signature.

Any orders issued through the E-Bank/M-Bank must be authenticated using the user identification elements by the person they have been issued to,

Payment code must be input in accordance with payment code list in such manner that code corresponds payment nature.

Payment in accordance with model 97 shall be input only if such model has been predetermined by payee.

The User shall ensure to accurately sum up collective orders. Payee's account must be completed in a legible and accurate manner.

The User shall be responsible for the accuracy and completeness of data in the Order even in cases if it requires the Bank to fill in the order in accordance with the User's instructions.

Consent for Payment Transaction

Article 16

Payment transaction shall be deemed authorised if the payer has given its consent to the execution of payment transaction or if the payer has given the consent for the execution of a series of payment transactions such payment transaction is a part of.
Method of giving consent to payment transaction execution shall depend on payment instrument and order receipt channel.
The User shall give the consent for the execution of payment transaction initiated:
- at the Bank branches - by signing payment order,
- through the E-Bank and M-Bank using one-off code, biometric data (fingerprint or facial recognition), mtoken, smart card, or other security designation, and final transaction verification in the manner defined in the application for such service,
- by scanning the QR code on monthly bills or scanning the QR code at point of sale of merchant
- by payment card, Reading the chip by inputting the card in the reader and inputting the PIN code on the ATM or in the POS terminal, , by contactless reading of the chip at ATM and PIN input, by contactless reading of the chip, including and excluding PIN input, at the merchant's point of sale, in accordance with the restrictions for contactless payments by the Card organisation; using the card within digital wallet in the manner described in Part 6A.3 hereof; reading of magnetic tape or inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code) for particular POS terminals, including and excluding slip signing; in the event of the payment transactions where physical presence of the card is not necessary (Internet transactions, orders by e-mail or telephone) by inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code). To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account, via push notification and entering PIN or biometric data for George mobile application users
- using digitalised payment card, tap relevant device on POS terminal, and/or by selecting Digital Wallet payment option on the internet point of sale and by inputting personalised security elements determined or agreed by the user with the Service Provider,
- if the User has agreed and signed Application From/Agreement for the execution of single and/or a series of payment transactions with the Bank or payee (standing order and direct debit)
- with a qualified electronic signature in the cloud – ConsentID – when signing a transfer order for the collection of an electronic promissory note in the Central Registry of Electronic Promissory Notes, managed by the National Bank of Serbia.

Order Execution
Article 17
The Bank will execute payment order if the following conditions are met:
- if order is accurate and/or contains minimum data necessary for the execution thereof,
- if there is cover on account for the payment of total amount referred to in the order and fee/commission for executed transactions, or if the User executing incoming payment to its current account provides the Bank with cash in the amount necessary for order execution,
- if consent is granted for payment order as per agreement
- if, in addition to the payment order, the prescribed documentation is submitted.
The Bank shall determine the fulfilment of the conditions for an order execution at the time of receiving the order.

If execution date is determined in an order in advance, the Bank shall verify the conditions for payment order execution at particular date of execution.

Article 18
Payment order may be incoming, outgoing, and transfer payment order. The Bank shall execute orders if all of the conditions defined in Article 12 to 17, in accordance with receipt time, are met, if cover is provided for the execution thereof on the User's account, and unless there are any legal obstacles for order execution.

Payment Transaction Execution Deadline

Article 19
Payment orders shall be executed in accordance with the time of receipt and execution date, in accordance with the Cut-off Times.

Order execution time shall be set in accordance with RTGS cut-off times and the National Bank of Serbia Clearing System.

For domestic payment transaction executed in RSD, the Bank shall, as the payer's payment service provider, ensure the approval of the transaction amount on the account of the payee's payment service provider on the same business day on which the Bank has received the payment order from the payer – User.

For payment transactions which are not covered in the above paragraph, the terms for payment transaction execution set out in the law or in relevant by-laws shall apply.

In the event of domestic payment transaction up to RSD 300,000 initiated as an instant credit transfer, the Bank shall ensure that the transaction amount is instantly or almost instantly credited on the account of the payee's payment service provider, following the receipt of such an order.

The provisions of the regulations governing foreign exchange transactions shall apply to the execution of international payment transactions, and the provisions of these General Terms and/or Framework Agreement and Law on Payment Services shall apply to any issue not set out herein.

Debit Value Date and Credit Value Date

Article 20
The Bank shall, as the payer’s payment service provider, ensure that the value date of debiting the payment account of the User – payer in connection with the payment transaction execution is the same as or later than the date when such payment account is debited in the amount of payment transaction.

The Bank shall, as the payee's payment service provider, ensure that the value date of crediting the payment account of the User as the payee, in connection with payment transaction execution, is no later than the business date when the payment transaction funds are credited on the Bank account.

Execution of Payment Transaction to the Payee

Article 21
The Bank shall, as the payee's payment service provider, without undue delay, credit the payment account of the User:

1) if the amount of the payment transaction for the User – payee has been credited to the payee's payment service provider’s account or if the Bank has otherwise received such amount;
2) if the Bank has, as the payee's payment service provider, received all information necessary for crediting the payment account of the User – payee or making funds available to the User – payee.

After the payee’s payment account has been credited, the Bank shall, as the payee's payment service provider, immediately make that amount available to the User – payee.

Provisions of para 1 and 2 of this Article shall apply when payee’s payment service provider is, at the same time, the payer’s payment service provider.

If funds have been credited to the account of the Bank as the payee’s payment service provider on the day which is not a business day, it shall be deemed that the Bank has received such funds for the User on the next business day.

Article 22
If, at the time of order execution, there are no funds on the User's account or there are insufficient funds for order execution, the Bank shall try to execute such order until the end of business day, on the date when it is indicated that the order should be executed.

In cases when the User issues several orders for which there are no sufficient funds for the execution of the order which has been, based on the sequence during the day received earlier, the Bank will execute the payment order for which there is cover on the account. Any orders for the execution of which no cover is

provided during the day designated for the execution thereof will be automatically deleted from the records of execution upon the expiry of such business day and will be deemed rejected.

Order Rejection

Article 23
The Bank shall reject the execution of any order which is not provided and completed in accordance with the General Terms, for which the execution terms have not been met.

In the event of instant transfer order, the Bank shall be entitled to reject such order if it receives a notification from the IPS system operator on the rejection of the execution of such order due to the failure to fulfil the conditions for the execution of such transfer, set out in the rules of such system. The Bank will not execute instant payment order in the event the payee's payment service provider is not a participant in the IPS system.

The Bank shall be entitled to reject the order which meets all conditions for execution if such execution would be contrary to the regulations governing the prevention of money laundering and terrorism finance and regulations in the area of sanctions, or internal acts of the Bank rendered based on such regulations.

If payment order is rejected by the Bank, it shall be deemed that payment order has not been received.

Payment Order Recall

Article 24
The Payer may recall payment order – by providing the Bank with request for recall in writing or electronically depending on the method of the issuance of payment orders, at the time and in the manner which ensure the initiation of such recall prior to the execution of the instructions contained in such order provided that the Bank has not executed such payment order.
When the Payer has specifically arranged the beginning of order execution with the Bank, the order may be recalled no later than the closing time for order execution on the business day preceding the day set out as the beginning of order execution and/or until the time of forwarding the order for clearing.
If transaction is initiated by the payee using direct debit, the payer may recall such order no later than at the end of the business day preceding the date set out for debiting payer's account.
Where a payment transaction is initiated by a payment initiation service provider or by the payee or by the payer through the payee, the payer shall not revoke the payment order after giving consent to the payment initiation service provider to initiate payment transaction or after giving consent to execute the payment transaction to the payee.
For payment transactions initiated by payment card, the payer may not recall payment order upon transaction authorisation and/or upon inputting PIN and approving transaction.
If the user recalls an order upon the expiry of the deadlines referred to in paragraph 1–3 of this Article, the Bank may take reasonable actions to prevent the order execution while being in compliance with the applicable regulations and professional rules.
Recall of order upon the expiry of the deadlines referred to in paragraph 1–3 of this Article may be charged by the Bank, in accordance with the Price List.
Upon the expiry of recall deadline, payment service user may recall payment order only based on the agreement with the Bank or other payment service provider participating in payment transaction execution. If payment transaction is initiated by payee or payer through payee, payment order recall may not, upon the expiry of the deadlines referred to in paragraphs 1–3 of this Article, be executed without the payee's consent.

Notification of the User on Payment Transactions

Article 25
The Bank shall, upon the User's request, issue confirmation of order receipt as well as the confirmation of the order execution.
This request must be sent by the User to the Bank upon the order presentation. For the issuance of this confirmation, the fee provided for in the Price List shall be charged by the Bank, and the confirmation shall be issued immediately upon the order execution, but no later than next day.

The User shall be provided with report by the Bank on any changes on the account by e-mail, upon any change on the account, but no later than two days upon executed change. The User who does not have an electronic address may overtake the report on changes on the account at the Bank’s teller desk.

Statement on changes on the account shall visibly present all of executed orders.

Liability for Non-approved Payment Transaction

Article 26

The Bank shall be liable for the execution of a payment transaction for which there is no consent granted by the payer, in accordance with the General Terms.

In the case of an unauthorised payment transaction, the Bank shall refund to the payer the amount of the unauthorised payment transaction immediately, and in any event no later than the following business day after noting or being notified of the payment transaction, except where the Bank suspects fraud or misuse by the User, in which case the Bank shall, within ten days from learning of an unauthorised payment transaction, take one of the following actions:

1) provide an explanation to the User regarding the grounds for rejecting the refund and report fraud and/or misuse to the competent authority; or

2) refund the amount of that transaction to the payer where, after further verification, it concludes that the payer did not commit fraud or misuse.

The Bank shall restore the payer's payment account to the state in which it would have been had the unauthorised payment transaction not taken place, so that the credit value date for the payer's payment account shall be no later than the date the amount of the payment transaction had been debited.

The Bank shall also refund to the payer all charges levied for the executed unauthorised payment transaction and refund and/or pay any related interest the payer would be entitled to if the unauthorised payment transaction had not taken place.

Where the payment transaction is initiated through a payment initiation service provider, the obligations defined in this Article shall apply if the Bank maintains the payer-s account.

Payer's Liability for Unauthorised Transaction

Article 26a

Notwithstanding Article 26, the User shall bear losses resulting from the execution of non-approved payment transactions if such transactions have been executed due to use of lost or stolen payment order, payment instrument, or payment instrument which has been misused, because the User has not protected personalised security elements for transaction confirmation (PIN, user identification elements when e-banking/m-banking is used) or acted contrary to the provisions of these General Terms relating to the protective measures and safe use of payment instrument. The User shall bear any losses resulting from the execution of non-approved payment transactions if such transactions have been executed due to fraud by client.

If the Bank does not provide appropriate means of the notification on lost, stolen or misappropriated payment instrument, the User shall not bear losses resulting from the use of that payment instrument, except where it has acted fraudulently.

The User will not bear any losses resulting from unauthorised payment transactions executed after it notified the Bank on lost, stolen or misappropriated payment instrument, except where these losses occurred due to the User acting fraudulently.

Rights and Obligations of the Bank in Case of Incorrectly Executed payment transactions

Article 27
The Bank shall, as the payment service provider, have the following rights and obligations in particular cases of incorrectly executed domestic payment transactions:

1) if the payer's payment service provider transfers to the payee's payment service provider the amount of the payment transaction that is higher than the amount indicated in the payment order or executes, by mistake, the same payment order several times – the payee's payment service provider shall, based on the evidence submitted by the payer's payment service provider that has made the error, make refund without undue delay;

2) if the payee's payment service provider has been transferred the amount lower than the amount indicated in the payment order, the payer's payment service provider may, within the term referred to in Article 42 of this Law, transfer to the payee's payment service provider the difference, even without request by the payment service user for correct execution of the payment transaction;

3) if funds are transferred to a payee other than the one indicated in the payment order, the payer's payment service provider may, within the term referred to in Article 42 of this Law, correctly execute the payment transaction even without the request of the payment service user for correct execution of the payment transaction, and the payee's payment service provider whom the funds are wrongly transferred shall in any case, based on evidence submitted by the payer's payment service provider that has made the error, make refund (as recovery) to the payer's payment service provider without undue delay.

In the cases referred to in item 1) and 3) of the above paragraph, the Bank shall be entitled to debit the account of the User i.e. payee by higher paid i.e. groundlessly received amount.

In the cases referred to in item 1 and 3) of the above paragraph, the Bank shall be entitled to debit the account of the User i.e. payee by higher paid amount i.e. groundlessly received amount.

The refund referred to in this Article shall take precedence over any other payment transaction from the payment account from which the recovery is to be made.

Rights and obligations of payment service providers in cases of fraudulent or misused transactions

Article 27a

If it receives from the payer's payment service provider a refund request along with data, information and documentation based on which it is determined that the payment transaction is probably fraudulent or misused, the payee's payment service provider shall not credit these funds to the payee's account, and/or shall prevent the use of those funds to the payee within the next three business days from the day of receipt of those data, information and documentation.

If in the case referred to in paragraph 1, the payee's payment service provider, subsequently, but before the expiry of the deadline referred to in that paragraph, receives data, information and documentation from the payer's payment service provider, including the corresponding application to the competent government authority, which all together beyond any reasonable doubt points to the conclusion of fraud or unauthorised use, the payee's payment service provider shall:

1) without delay, make a refund to the payer, if the payee could not prove or make probable the origin of those funds or refused to provide appropriate evidence within 15 business days from the day when its payment service provider informed it of the data, information, documentation and application referred to in this paragraph;
2) enable the payee to use funds after 30 business days from the day of the expiry of the deadline referred to in paragraph 1 of this Article, if the payee has proven and/or made probable the origin of those funds within the deadline referred to in item 1) of this paragraph, and the competent government authority failed to adopt and submit an act on the prohibition of the use of those funds.

The payee's payment service provider shall be accountable to the payer for the loss arising from the payment transaction referred to in paragraph 1 of this Article, if it enabled the payee, contrary to paragraphs 1 and 2 of this sub-item, to use funds, and it is determined in relevant procedure that the payee committed or participated in fraud or unauthorised use.

Liability for Using Unique Identifier

Article 28

If payment order is executed in accordance with the payee's unique identifier referred to in such order, it shall be deemed that this order has been correctly executed relating to the payee determination irrespective of other data the payment service provider has been provided with.

If unique identifier filled in by the User in the order is incorrect, the Bank shall not be liable for non-executed or incorrectly executed payment transaction.

In the case referred to in paragraph 2 hereof, at the request of a payment service user, the payment service provider shall immediately take all reasonable measures in order that the payment service user receives the refund of a payment transaction amount, and the payee's payment service provider shall cooperate to this aim with the payer's payment service provider and provide all the necessary information to the provider so that the payment transaction amount is refunded. If in the case referred to in this paragraph the money cannot be refunded to the payer, the payer's payment service provider shall, upon the payer's written request, immediately submit all the available information which the payer needs to exercise the right to refund (e.g. information about the payee's payment service provider and/or the payee), including the information which the payee's payment service provider is required to provide to the payer's payment service provider under this paragraph.

In the event of non-executed payment transaction due to incorrect unique identifier referred to in paragraph 2 of this Article, the Bank shall ensure to, immediately upon becoming aware thereof, refund the amount of non-executed payment transaction to the payment service user.

Liability of an intermediary for unauthorised, non-executed, defective or late payment transactions

Article 28a

The payment service provider shall be liable to the payment service user for an unauthorised, non-executed or incorrectly executed payment transaction, or delay in payment transaction execution in dinars even if the liability is attributable to an intermediary participating in the execution of that payment transaction among payment service providers.

Obligation to trace funds in case of unauthorised, non-executed or defective payment transactions

In case of an unauthorised, non-executed or incorrectly executed payment transaction, the payment service provider shall, regardless of the liability for correct execution of a payment transaction, upon request of its payment service user, take immediate and adequate steps to trace the funds and notify the user about the outcome of measures taken without undue delay.

Exclusion of Liability for the Actions of Intermediary Bank

Article 29
For international payment transactions, the Bank shall not be liable if the intermediary bank participating in the payment chain charges its fee, thereby decreasing the amount paid to the payee (if the bank has not, in the course of initiating transaction, been aware thereof or if it has informed the client thereof), even when OUR costs are arranged.

For international transactions, the Bank shall not be liable to payment service user for a non-executed or incorrectly executed payment transaction even if the liability is attributable to an intermediary participating in the execution of that payment transaction among payment service providers.

For international payment transactions, the Bank shall not be liable if a foreign bank of the payee credits the payee's account in the local currency, not in the currency in which the User has executed transaction, or if the foreign bank executes payment transfer in another currency, not in the one in which the payment transaction has been initiated.

Liability Exclusion due to Force Majeure or Law

Article 30
The Bank shall not be liable for incorrectly, non-timely executed and/or for non-executed payment transaction in the event of force majeure which has prevented the fulfilment of obligations or if payment transaction execution is prohibited under other regulation.

Force majeure means, without limitations, any events hampering or preventing the execution of payment services, such as war, disturbances, terrorist acts, strikes, electric power outages, breakdown of telecommunication connections or other communication channels, actions and regulations by any public or other authorised body, termination or incorrect operation of payment system, which could not be impacted by the Bank, which are the objective hindrance for the provision of such services.

The liability of the Bank when, due to the application of the regulations governing the prevention of money laundering and terrorism finance and/or due to the change in sanction related regulations, the Bank rejects payment transaction execution or prolongs the terms referred to in the Cut-off Times, shall be excluded

Confirmation on the availability of funds

Article 30a.

Upon the request of a payment service provider issuing card-based payment instruments, an account servicing payment service provider shall immediately confirm whether an amount necessary for the execution of a card-based payment transaction is available on the payment account of the payer, provided that all of the following conditions are met:

1) the payment account of the payer is accessible on-line at the time of the request;

2) the payer has given explicit consent to the account servicing payment service provider to respond to requests from a specific payment service provider to confirm that the amount corresponding to a certain card-based payment transaction is available on the payer's payment account;

3) the consent referred to in item 2) of this paragraph has been given before the first request for confirmation is made.

The payment service provider issuing card-based payment instruments may request the confirmation referred to in paragraph 1 of this Article where all of the following conditions are met:

1) the payer has given explicit consent to the payment service provider to request such confirmation;

2) the payer has initiated the card-based payment transaction for the amount referred to in paragraph 1 of this Article using a card-based payment instrument;

3) the payment service provider issuing card-based payment instruments authenticates itself towards the account servicing payment service provider before each confirmation request, and securely communicates and exchanges messages and data with the account servicing payment service provider in accordance with the regulation referred to in Article 75d of Law on Payment Services.

The confirmation referred to in paragraph 1 of this Article shall consist only in a simple 'yes' or 'no' answer and not in a statement of the account balance. That answer shall not be stored or used for purposes other than for the execution of the payment transaction.

The confirmation referred to in paragraph 1 of this Article shall not allow for the account servicing payment service provider to block funds on the payer's payment account.

At the payer's request, the account servicing payment service provider shall inform the payer about the payment service provider which submitted the request referred to in paragraph 1 of this Article and the answer provided.

Rules on access to payment account in the case of payment initiation services

Article 30b.

Where the payer's payment account is accessible on-line, the payer has the right to make use of a payment initiation service provider to obtain payment initiation services.

When providing the payment initiation service, the provider of this service shall:

1) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

2) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

3) ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

4) every time a payment is initiated, securely confirm its identity towards the account servicing payment service provider of the payer, in accordance with the regulation referred to in Article 75d of Law on Payment Services, and communicate and exchange data and messages with that account servicing payment service provider, the payer and the payee in a secure way;

5) not store sensitive payment data of the payment service user;

6) not request any data other than those necessary to provide the payment initiation service;

7) not use, store or access any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;

8) not modify the amount of the payee or any other feature of the payment transaction.

When the payer gives its explicit consent for a payment transaction to be executed, in order to ensure the payer's right to use the payment initiation service the account servicing payment service provider shall perform the following actions:

1) communicate and exchange data and messages securely with the payment initiation service provider, in accordance with the regulation referred to in Article 75d of Law on Payment Services;

2) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all available information regarding the execution of the payment transaction to the payment initiation service provider;

3) treat payment orders transmitted through a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing and speed, priority or charges vis-à-vis payment orders transmitted directly by the payer.

The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Rules on access to and use of payment account information in the case of account information services

Article 30c.

Where a payment account is accessible on-line, the payment service user has the right to make use of account information services.

When providing the account information service, the provider of this service shall:

1) provide services only where based on the payment service user's explicit consent;

2) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the account information service provider through safe and efficient channels;

3) for each communication session, confirm its identity towards the account servicing payment service provider of the payment service user, in accordance with the regulation referred to in Article 75d of this Law, and securely communicate and exchange data and messages with that account servicing payment service provider and the payment service user;

4) access only the payment accounts designated for the use of this service by the payment service user and information on associated payment transactions;

5) not request sensitive payment data linked to the payment accounts;

6) not use, store or access any data for purposes other than for performing the account information service explicitly requested by the payment service user.

When the payment service user gives its explicit consent for an account information service to be provided, in order to ensure the user's right to use the service the account servicing payment service provider shall perform the following actions:

1) communicate and exchange data and messages securely with the account information service provider, in accordance with the regulation referred to in Article 75d of Law on Payment Services;

2) treat data requests received from an account information service provider without any discrimination for other than objective reasons.

The provision of account information services shall not be dependent on the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

Limits of the access to payment accounts by payment service providers

An account servicing payment service provider may deny an account information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account by that payment service provider, including the unauthorised or fraudulent initiation of a payment transaction.

In the case referred to in paragraph 1 of this Article, the account servicing payment service provider shall inform the payment service user that access to the payment account is denied and the reasons therefor in the form agreed in the framework contract. If it is unable to inform the user thereof before access is denied, the account servicing payment service provider shall do so immediately after access to the payment account is denied.

By way of derogation from paragraph 2 of this Article, the account servicing payment service provider shall not inform the payer in accordance with that paragraph if providing such information is prohibited by regulations or would compromise objectively justified security reasons.

The account servicing payment service provider shall again allow access to the payment account once the reasons for denying access no longer exist.

Where the account servicing payment service provider denies access to a payment account in accordance with paragraph 1 of this Article, it shall immediately notify the National Bank of Serbia thereof, and include the relevant details of the case and the reasons for denying access.

Based on the notification referred to in paragraph 5 of this Article, the National Bank of Serbia shall take appropriate measures in accordance with this Law.

Payment transactions where the transaction amount is not known in advance

Article 30d.

If a payment transaction is initiated by or through the payee in the context of a card based payment transaction and the exact amount is not known at the moment when the payer gives consent to execute the payment transaction, the payer’s payment service provider may block funds on the payer’s payment account only if the payer has given consent to the exact amount of the funds to be blocked.

The Bank shall release the funds blocked on the User’s payment account without undue delay after receipt of the information about the exact amount of the payment transaction and at the latest immediately after receipt of the payment order.

Execution of payment transactions based on bills of exchange

Article 30e.

A payment transaction on the basis of a bill of exchange is the payment transaction where the payee initiates a payment transaction for debiting the payer’s payment account on the basis of a bill of exchange and payment order requiring the transfer of funds from the payer’s to the payee’s account.

The bill of exchange referred to in paragraph 1 of this Article, including the electronic bill of exchange, shall be issued in accordance with the law governing bills of exchange and shall represent an irrevocable consent of the issuer given to its payment service provider to execute the payment transaction initiated by the bill of exchange holder in accordance with that paragraph.

If the bill of exchange referred to in paragraph 1 of this Article is recorded in the register of bills of exchange and mandates maintained by the National Bank of Serbia pursuant to regulations on enforced collection from funds in accounts, pursuant to these regulations the payee may initiate a payment transaction to debit the payer’s current account with any payment service provider servicing this account.

Provisions of para 1–3 of this Article shall not exclude or impair the rights that a bill of exchange issuer, bill of exchange holder or other persons holding bills of exchange have under the law governing bills of exchange. In the case of an electronic bill of exchange, these rights can be exercised using the official statement of the electronic bill of exchange, instead of the original electronic bill of exchange.

The National Bank of Serbia maintains the central register of electronic bills of exchange, which is integral to the register referred to in paragraph 3 of this Article, and issues the statement referred to in paragraph 5 of that Article, which has the properties of an authentic and public instrument.

The National Bank of Serbia regulates in detail the electronic bill of exchange, the central register of electronic bills of exchange and the official statement of the electronic bill of exchange referred to in this Article, the recording of the electronic bill of exchange, its deletion and use within this register, access to the register and banks' obligations in relation to such access and use of electronic bills of exchange, and other matters relevant for the operation of this register.

Customer Operations with Electronic Promissory Notes

An electronic promissory note represents a dematerialized own promissory note in accordance with the law governing promissory notes, with the clause "without protest." It is maintained, stored, and used as a set of data in electronic form within the Central Registry of Electronic Promissory Notes (hereinafter: Central Registry).

The Central Registry is an integral part of the Promissory Note Register and represents a specialized software solution managed by the National Bank of Serbia. It regulates the process of enforced collection from the User's account. The Terms of Use of the Central Registry (hereinafter: Terms of Use) define how electronic promissory notes are issued, how actions related to promissory notes are carried out, registered, and recorded in the Register, how they are delivered to creditors, and used in other ways. This system enables centralized electronic recording and storage of data regarding electronic promissory notes and their usage.

Access to the Central Registry is available to clients of the Bank who use the NovoKlik and E-Biz mBiz (Halcom) electronic banking applications.

The National Bank of Serbia adopts the Terms of Use and publishes them on its official website, as well as within the Central Registry.

Users agree to the application of the Terms of Use upon accessing and using the Central Registry.

Individuals listed in the User's Authorized Persons List (KDP) on the effective date of these General Terms are considered authorized to perform all actions related to electronic promissory notes. This includes the right to register, issue, and sign promissory notes, as well as to carry out promissory and other related actions within the Central Registry. The User may initiate changes to the scope of authorizations by signing the Bank's prescribed form.

When opening an account, a new User decides whether they wish to use electronic promissory notes and, on the Bank's prescribed form, defines the scope of authority for the individuals who will carry out actions related to electronic promissory notes.

Throughout the contractual relationship, the User may change the authorized persons or their scope of authority for handling electronic promissory notes by signing the Bank's prescribed form.

When actions related to electronic promissory notes are performed by the User, the Bank's role is to verify the scope of authority and the identity of the individuals performing those actions, and to confirm to the Central Registry that they are authorized, so that the actions can be executed in the Central Registry.

Execution of international payment transactions and payment transactions in currencies of third countries

Article 30f
Provisions of regulations governing foreign exchange operations shall apply to the execution of international payment transactions and payment transactions in the currencies of third countries.
The Bank will not execute international payment transactions for securities buying if funds are paid to a foreign broker or to the escrow account of the User managed by the foreign broker.

Provisions of these General Terms shall apply to all aspects relating to the execution of payment transactions referred to in paragraph 1 of this Article which are not specified in regulations governing foreign exchange operations.
By way of derogation from paragraph 1 of this Article, the National Bank of Serbia may prescribe operational, technical and other requirements to apply to the payment transactions executed in euros within the Single Euro Payments Area (SEPA).

SEPA Credit Transfer (SCT)

Article 30g
The SEPA Credit Transfer (SCT) represents a standardised method for executing payment transactions in euros within the Single Euro Payments Area (SEPA), ensuring efficient, secure, and reliable transfer of funds between users' payment accounts in the SEPA member states, in accordance with unified technical and business rules Key characteristics of the SEPA credit transfer include the following:

• Transactions are executed solely in the euro (EUR) currency;
• Payer must provide a correct IBAN (International Bank Account Number) of the payee;
• Payee must have an account at the financial institution which is a member of the SEPA system;
• Payments are made for the full original amount;
• Transactions are executed based on the "SHA" cost model
• The deadline for executing the order is no later than the next Bank business day from the date of receipt of a complete and properly filled-out payment order (D+1)

When issuing a payment order for the SCT execution, the Bank must obtain the following data from the User:

1) name and surname, or name of payer;
2) number of payer's account in the IBAN format;
3) data on credit transfer amount;
4) number of payee's account in the IBAN format;
5) name and surname, or business name of payee;
6) other information regarding payment transaction.

When executing a credit transfer, the Bank, as the payee's payment service provider must provide or make available to the payee the following data:

1) name and surname, or business name of payer;
2) data on payment transaction amount;
3) payment transaction description.

Time of SEPA SCT order receipt and execution is set out in the Bank's Cut-off Time.

The Bank will process each order for a SEPA SCT in the following case:

- when all of the prescribed obligatory elements of the order are completed,
- when the order is submitted at a time when the Bank can process the SCT order with regard to the execution date, i.e., no later than one interbank business day before the execution date,
- when the payment order is denominated in EUR,
- when the SHA option is selected as the credit transfer cost option,

The SHA cost option when executing an SCT means that the User bears the fee for executing the transaction in accordance with the Bank's Price List, without paying the costs of foreign correspondent banks.
The Bank is obliged, when it receives an SCT from a participant in the SEPA area in favour of a payee who is its User, to ensure that if the amount of the payment transaction for the payee has been credited to its account and if it has received all information necessary to credit the payee's payment account, it credits the funds to the payee's payment account without delay.

User's Complaints

Article 31

The User shall take care of the statements received from the Bank, review such statements, and file complaint relating to any mismatch or contest of debts and/or claims in the statement the User is provided with.

The period within which the User may file complaint for transactions shall expire on the fifth day requested by the User in the order as the transaction execution date, i.e. from the date of account debit.

The period referred to in the above paragraph does not appliy to the transactions referred to in Article 27a hereof.

Complaints shall be submitted by the User to the Bank in writing at the Bank point of sake, electronically to address info@erstebank.rs, via mBank and eBank applications, or by telephone to no. 0800 201201 (whereby the complaint is submitted in writing as soon as possible), stating the number of the order, order execution date, and accurate and clear description of the data which are the subject of the complaint.

The Bank shall start the procedure of complaint solving immediately upon the receipt and notify the User on the complaint procedure completion.

Upon the expiry of the complaint term, the Bank will not take such complaint into consideration, and the User shall be liable for any material consequences of disputed transactions.

Fees and Commissions for Payment Transaction Services

Article 32
Within its payment services, the Bank shall charge:
- current account maintenance fee
- fee for E-Bank/M-Bank - fee for issuance of confirmation on order receipt and execution
- fee for the submission of report on changes under account
- fee for certifying statement on changes under account
- payment transaction fee/commission
- other fees and commissions defined in the Bank Price Lists.

Any fees and commissions shall be defined in Placement Price List, Payment Service Price List, and Price List of Products and Services to Corporate Clients of Small Enterprises and Entrepreneurs Department.

Fees shall be defined in the absolute amount and they shall be variable i.e. the fees may be changed by the Bank in accordance with the movement of costs and other parameters impacting the level of fees in accordance with the Bank acts.

Commissions shall be defined in percentage amount where the base for percentage application shall be the value of transaction defined by the User in an order the Bank is provided with. Commissions shall, in addition to percentage amount, always include defined minimum value in absolute amount designating the value of minimum calculated commission charged i.e. which must apply if lower value is obtained by applying percentage to value in order.
Also, commissions shall include defined maximum value in absolute amount designating value of maximum calculated commission charged i.e. which must apply if higher value is obtained by applying percentage to value in order.

Article 33
Fees shall be charged through business account of the User by debiting the User's account, and they shall be clearly visible in the Statement on Changes on the Account, on a monthly basis.

Dinar account maintenance fee shall be charged if the User has had minimum one transaction on his account (inflow, outflow, account debiting for fees and liabilities under other products of the Bank), save for the clients which have been approved specific tariffs, when the fee is charged irrespective of the number of transactions.

Commissions shall be paid upon the execution of every order, on the date indicated by the User as the date of the execution of payment referred to in the order, or in other intervals the User has agreed upon with the Bank, by debiting the User's account, which shall be clearly visible in Statement on Changes on the Account.
Unless the User has settled due fees/commissions or there are no available funds on the account for the collection thereof, as well as if the User has breached the limit on the account, the User’s account will be, from

the date when the fees/commissions have fallen due or the limit has been breached, maintained in negative balance in the amount of outstanding claims of the Bank, until the date of fee/commission settlement and/or covering the amount of the breached limit.

To the amount of the negative balance, the Bank shall calculate and collect the default fee, at the rate set out in the Law on Default Interest. The Bank shall, upon the User's request, provide the User with the statement on all charged fees for the services connected to the payment account, minimum on an annual basis. (hereinafter: report on charged fees). Report on charged fees will be delivered by the Bank to the user in accordance with the terms set out in relevant by-law of the National Bank of Serbia.

Collection of fees and commission shall, in the event the User lacks funds on account upon order execution, be made upon the first funds inflow to the User's account or at the end of the month when fee calculation and collection shall be made.
Fees for FX payments and cover for FX transactions shall be collected by debiting the User's account.
Unless there are sufficient funds for the collection of fees and FX cover referred to in the above paragraph, account will not be maintained in the negative balance.

The Bank shall reserve the right to change level and method of fee and commission calculation.
All of the Bank's acts defining the level and method of fee and commission calculation shall be available in all of the Bank's points of sale and in the Bank's web site. Any change in these Bank acts shall be announced 15 days prior to the application thereof.

Article 34
The User may contract the use of other payment services relating to account with the Bank, such as:
- e-banking services: //Officebanking/Novoklik/Erste eBiz
- m-banking services: Erste mBiz
- debit/credit card
- other services prescribed in the Bank acts.

Main characteristics and terms of using the above-mentioned payment services shall be defined herein, in special agreement, or application forms, and general terms for using such service.

Payment Card

Article 35
Upon opening of the account to the User, the Bank shall, upon the User’s request, issue the payment card to the User which shall be the payment instrument based on which the User shall dispose of the funds on the account and/or initiate payment transactions.

The Bank shall, in accordance with Article 9 paragraph 1 of the Law on Multilateral Interchange Fees and Special Operating Rules for Card-based Payment Transactions (“Official Gazette of the RS”, no. 44/2018), first issue to the User who wants a business debit payment card the payment card where processing, netting, and reconciliation of transfer orders, issued based on its use in domestic payment transactions, are executed within the payment transaction system of the Republic of Serbia.

Upon the issuance of the payment card where processing, netting, and settlement of transfer order within domestic payments are executed within the payment transaction system of the Republic of Serbia, the Bank will, upon the User’s request, also issue the business debit card of another payment brand (Visa, MasterCard, etc.) to such User.

Application for the issuance of the cards referred to in the above paragraph may be submitted at the same time when the application for card issuance referred to in paragraph 2 of this Article is submitted.

The Bank shall, upon the expiry of the validity of previously issued debit card of other payment brand, upon the request by the User, issue the business debit card of other payment brand to such User, and, in the event of re-issuance, such User will also be issued the payment card where processing, netting, and settlement of transfer orders issued based on its use in domestic payments are executed within the payment transaction system in the Republic of Serbia (save if the User has already been issued such payment card).

Following current account opening, the User shall be issued the debit card in the manner described in this Article, and the User may, upon its request, also be issued credit card if the conditions for the issuance thereof are met.

Credit card is the payment instrument through which an approved loan shall be used up to the level of the available balance under such loan.

FX debit card shall be issued upon the User's request and maintained in the currency to which FX current account is tied.
The Bank shall also issue an additional credit Card upon the User's request to the persons listed in Credit Card Issuance Application. The provisions of these General Terms shall apply to the holder of the additional card.

The Card shall be made out to the User and it shall not be transferable. The Card shall be the ownership of the Bank upon whose request it must be returned.
Holder of account the Card is tied to (hereinafter Account Holder) shall solely be liable for proper Card use.

The Bank shall be entitled to, during the Card validity and/or automated Card re-issuance, change a type of payment Card, of same or other payment Card brand in which case, the Bank will, excluding any additional costs, make the change of the Card used by the User and ensure the functionalities that correspond to the functionalities of the card which is replaced.

The Bank shall retain the right not to issue the payment card in the event of the Card inactivity during a longer time period.

Card Issuance and Card Data Protection
The User shall be provided with the Card and PIN (personal identification number). The Bank shall guarantee the Card User the secrecy of the PIN issuance until the Card is handed to the User. Obligation of the User shall be to sign Card immediately upon the receipt thereof, as well as to protect any data therein and to keep PIN in secrecy separately from the Card. The non-signed card shall be invalid, and any financial consequences in the event of the misuse of the non-signed Card shall be borne by the User.

The User must not keep the card and PIN together, otherwise, in the event of theft, loss, or misuse of the card, it shall be deemed that the User has acted in gross negligence, therefore, the User shall bear material liability for any transactions arisen due to the breach of this obligation, in accordance with Article 26 hereof.

The User must not disclose PIN to other persons (including, without limitation, family members, merchant, bank officer). Otherwise, the User shall bear material liability for all transactions arisen due to the breach of this obligation. The User must not leave Card as pledge or collateral, or provide card to be used or be in possession of other persons, otherwise, the User shall bear complete material liability for any transactions executed due to the non-compliance with this obligation.

In the event the User suspects that anyone is aware of the PIN, the User shall change the PIN at the Bank ATM or request card blocking, making of new card and new PIN in writing. Otherwise, the entire risk of PIN fraud shall exclusively be at the charge of the Account Holder the Card is tied to.

Personalised card elements must not be made available to other person by the User (e.g. by forwarding the picture of the card, etc.). In such case, it shall be deemed that the User has acted in gross negligence, and the User shall bear all material consequences resulting from such use of the card.

The User acknowledges that it is aware that the Bank will not, for security reasons, request the User to confirm data on the Card electronically or by telephone, otherwise the User shall fully bear the risks and consequences of identity theft and unauthorised use of data from the card due to the provision of data on the Card as mentioned above.

Card Use
Consent for payment transaction execution shall be provided by the Card User prior to the payment transaction execution in one of the following manners:
Reading the chip by inputting the card in the reader and inputting the PIN code on the ATM or in the POS terminal, by contactless reading of the chip at ATM and PIN input, by contactless reading of the chip, including and excluding PIN input, at the merchant's point of sale, in accordance with the restrictions for contactless

payments by the Card organisation; using the card within digital wallet in the manner described in Part 6A.3 hereof; reading of magnetic tape or inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code) for particular POS terminals, including and excluding slip signing; in the event of the payment transactions where physical presence of the card is not necessary (Internet transactions, orders by e-mail or telephone) by inputting the security elements required by the Payee (card number, validity date, CVV2/CVC2 code). To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account, or via push notification or entry of PIN or biometric data for the George mobile application users.

To verify the User's authenticity, the Payee may request an additional authentication of the User by inputting the One Time Password on the Internet points of sale providing payment using 3D service. Inputting an OTP password obtained through SMS, the User confirms the consent to debit the payment on the User's account.

User authentication for transactions executed at on-line points of sale that enable payment using the 3DS service, for users of the George mobile application, is performed via a push notification within the George mobile application (with the entry of a PIN code or biometric data), whereby the user's consent for executing the payment debiting the user's account is confirmed.

From 30 June 2026, User authentication for transactions executed at on-line points of sale that enable payment using the 3DS service will **solely** be made via a push notification within the George mobile application (with the entry of a PIN code or biometric data), whereby the user's consent for executing the payment debiting the user's account is confirmed. To be able to make payment using a card on the aforementioned on-line points of sale, the Card User must have an activated George mobile application, in accordance with item 12.1.3 and 12.4 of the General Terms of Providing Payment Services to Private Individuals and Registered Farms.

The Card User may also grant consent for payment transaction execution through payee and payment initiation service provider.

Data on the card registered for payment on a web site MAY be replaced with new card data following the re-issued card if such process is initiated by the Internet merchant with the card company

The Card may be used at all points of sale and ATMs in Serbia/abroad where the logo of the card company is displayed for withdrawing cash on ATMs and at teller desks of banks and post office (if relevant terminal is installed) and for the payment of goods and services at POS terminals and by the Internet.

Credit card user may not, using the E-Bank/M-Bank transfer funds to current account, transfer funds from credit card to be debited to other accounts, and withdraw cash on the Bank teller desks.

The Bank shall not be liable if any merchant does not want to accept the Card though VISA/MAESTRO/ MASTER CARD/DINACARD logo is displayed or if, due to an incorrect terminal use and/or technical problems, it is not possible to execute transaction upon the User's request.

The User shall, upon the request of goods and service seller (hereinafter: Acquirer) provide the Card whose right of use has expired.

The User shall, when paying for goods and services, also sign and overtake appropriate slip at acquiring point. Acquirer shall issue slip/account copy to the User.

The User shall not use the Card for illegal purposes, including purchase of goods and service the sales of which is prohibited in the territory of the country the Account Holder is in at the time of transaction. The User shall assume full liability in the event of an illegal purchase using the Card subject hereof.

The User must not conclude fictive cashless transactions with Acquirer with the aim of obtaining cash.

The Card whose validity period has expired must not be used, otherwise the User shall be fully liable for any transactions executed due to the non-conformance with this obligation.

The Bank shall, for security reasons, set out cash amount limit and the amount of goods and service payment which may be used at ATMs and POS terminals on a daily basis. The limits for the card use by the persons authorised by the User shall be set out by the User in the Card Issuance Application. The User shall be entitled to change the amount of daily limit by submitting the application for limit change, whereby it is not necessary to draw up the Annex to the Framework Agreement.

In the course of the contactless transaction execution, there is a possibility that a POS terminal does not request either the PIN input or the User's signature. Card organisations, based on their rules, determine the maximum limit up to which it is not necessary to input the PIN for contactless transactions. Occasionally, for security reasons, the User may be requested to execute a contactless transaction in the same manner as when paying for goods and services at a POS terminal for chip card acceptance, by entering the PIN code.

If currency exchange is made when the card is used, the exchange rate for the currency exchange shall be determined in accordance with these General Terms.

The Card validity period shall be embossed on card. The Card shall be valid until the last day in stated month. If the User is in compliance with the provisions of the Framework Agreement, after the validity period expiry, the User shall be automatically re-issued the Card (in accordance with these General Terms and the law), at the fee provided for in the Price List. The Card User shall be entitled to, within 30 days prior to the Card validity, state unless he wants to be re-issued the card.

At the time of the initiation of any payment transaction with the Card or digital card, the User must have funds on the card account in the amount of the transaction amount, and for transactions abroad in currency other than RSD which shall be additionally increased by 3% for the transactions abroad. Based on the initiated payment transactions using the card, the Bank will make the provision of the funds on the account to which the card is tied. Funds provision will last for 15 days from the transaction execution date. Following the defined term, provision will be automatically cancelled in the system, whereby provision cancellation shall not release the User of the obligation to provide sufficient funds for the settlement of the executed transaction. Upon the receipt of the order for debit by the payee's service provider, the Bank will book i.e. debit the card account even following the cancellation of the respective provision, in which case the User shall provide sufficient funds on the card account for the transaction settlement. If the User finds that the debit has been booked, but the provisioned funds have not been released, the User must immediately contact the Bank to make any necessary checks.
The User is aware that the amount of the provision may differ from the debit amount. In the course of the execution of payment transactions using payment card, users should also take into consideration that the date of account debit can differ from the payment transaction occurrence date for this payment transaction type.

In the event of rejection of on-line transactions executed with Debit Card (Card not present transactions), the Bank notifies the User on the rejected transactions via SMS notifications.
Notifications will be sent via SMS solely to the telephone number reported in the bank system.

Currency Exchange Rate
When exchanging local currency into foreign currency, foreign currency into local currency, and foreign currency into other foreign currency, the Bank shall apply the exchange rate from the Bank Exchange Rate List, applicable at the time of exchange unless otherwise is agreed by parties on a case-by-case basis.
In the event payment card is tied to the RSD Account, for the costs incurred using the card abroad, the Bank will convert the amount of transaction in FX into RSD as follows: MasterCard International or Visa International will translate original amount in EUR at Referential Exchange Rate, and from such amount, RSD value will be calculated at the selling exchange rate for FX of the Bank for EUR, applicable on date of debiting.
In the event the card is tied to the FX account, for transactions executed in RSD, the Bank will convert RSD in the currency of the FX Account, at the Bank buying exchange rate applicable on date of debiting.
In the event the card is tied to the FX account, for transactions executed in RSD, if original transaction currency is one of the currencies from the Bank's exchange rate list and identical to the currency of the FX account, the account shall be debited in the amount of the original currency.
In the event the original transaction currency is not included in the Bank exchange rate list and differs from the FX account currency, MasterCard International and Visa International shall convert the original amount in EUR in accordance with Referential exchange rate, and the Bank shall, from such amount, calculate RSD counter value at the Bank selling exchange rate applicable on date of debiting, and from such amount at selling exchange rate, the Bank shall calculate the counter value in the value of the FX account and debit the FX account by such amount.

MasterCard and Visa exchange rates shall be publicly available on Internet pages www.visaeurope.com and www.mastercard.com and, they shall be variable during day, and the Bank exchange rate lists shall be available on the Bank Internet page and at all branches.

Complaints Based on Card Transactions

The User shall keep slip/bill copy for the purposes of complaint. The User may file complaint within 5 days from the date of debiting. Complaint may be sent by submitting the prescribed form at the closest point of sale of the Bank, by e-mail at info@erstebank.rs or by telephone to no. 0800 201201 (where the complaint is submitted in writing as soon as possible) by the authorised person of the User, stating the data on the transaction subject to the complaint.

The Bank shall start the procedure of complaint solving immediately upon the receipt and notify the User on the complaint procedure completion.

Upon the expiry of the complaint term, the Bank will not take such complaint into consideration, and the User shall be liable for any material consequences of disputed transactions.

For the complaints relating to the quality of goods and services paid with the Card, the User shall solely address the Acquirer.

Lost/Stolen/Misused Card

The User/Authorised User shall, without delay, report the Card loss or theft to the Bank and request blocking of any further use thereof from the Bank, and the Bank shall ensure the execution of the aforementioned activities at any time. The Card theft/loss/misuse shall be reported by the User at the closest Bank sub-branch, by calling number 021/67 72 116 available 24/7, or by sending e-mail from the User's address reported to the Bank, to e-mail address sigurnost.kartice@erstebank.rs.. The User/Authorised User shall, when reporting the stolen/lost/misused card, state the number of the Card or personal identification number of the Authorised User in order for the Bank to prevent its further use. The User/Authorised User shall, within 2 next business days, confirm the report of the lost/stolen/misused Card in writing.

The Card found after reporting loss must not be used and it must be returned to the Bank in order to be destroyed.

In the event of any unauthorised use of the Card and/or data from the Card, the User/Authorised User shall, immediately, upon becoming aware thereof, report to the Bank any transaction executed based on an unauthorised use of the Card and/or data from such Card.

Date of Statement receipt shall be deemed the date when the User becomes aware of the occurrence of the circumstances referred to in the above paragraph.

The User/Authorised User shall, without delay, report to the Bank a damage and technical deficiency of the Card in the manner provided for in para 1 of this Article.

Protective and other Measures

The User shall use payment card in accordance with these General Terms.

The User shall, immediately upon the card receipt, take any reasonable and appropriate measures to protect personalised security elements of such an instrument (PIN, card number, etc.).

If Internet payment is made possible with the payment card, unless the site on which payment is made supports 3-D Secure protection mechanism, the User is, based on such payment, exposed to higher risk of possible misuse of the data from the Debit Card.

If the User deals with i-commerce, the User must not communicate the card data to the customer (save for the account number). If data misuse and/or unauthorised transactions occur in such case, it shall be deemed that the User has acted in gross negligence and shall bear material consequences of such executed transactions.

If the User receives an SMS to authorise a payment transaction by inputting the code/OTP password, but the User has not initiated such transaction, the User must not verify such transaction, otherwise his account will be debited in the amount of such verified transaction.

If the card is used in the course of purchase/sales on the Internet, the User must not, if the User is referred to other web site, or if the User receives the message to input the personalised elements of the card on another web site (i.e. the web site of Postal Service of Serbia), act in such manner, because in the majority of cases, though it initially seems that those are the official web sites, those are false web sites used for the misuse of the data from the card.

The User shall, on a regular basis, follow any notices on the Bank Internet address relating to warnings in connection with the possibilities of payment card misuse (phishing etc.) and act accordingly.
The User shall ensure, for the purpose of prevention of fraud, to be informed on the security rules of using payment instruments on the web site of the Association of Serbian Banks www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata.

Payment Instrument Blocking
The Bank shall block further use of a payment instrument – payment card, completely or partially (for certain transaction types based on certain parameters), if there are reasonable grounds relating to payment instrument security, if there is suspicion of unauthorised use of payment instrument or the use thereof for the purpose of fraud, or if there is an increased risk that the User will not be able to meet its payment obligation when the use of such instrument is related to the approval of loan and/or overdraft to the User (blocked account card is tied to, etc.).
The Bank shall notify the User on its intention and reasons of payment instrument blocking. Unless it is able to notify the User thereof prior to payment instrument blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking or payment instrument blocking shall be delivered by the Bank to the User in the manner set out in the Framework Agreement unless the provision of such notification is prohibited under regulations or if there are reasonable security reasons not to do so.
The Bank will ensure re-use or replacement of the payment instrument with a new one – when reasons for blocking thereof cease.

Liability for Damage
For any damage arising from non-approved payment transactions by using payment card, the User shall be liable in accordance with Article 26a hereof.

DIGITALISED CARD AND DIGITAL WALLET

Article 35a

Definitions

Digital Wallet Service Provider – local or foreign legal entity providing digital wallet service, with which the Bank has set up business cooperation to enable its users to add and use the payment cards issued by the Bank in the form of Digital Card (Apple Pay, GooglePay, etc.).

Digital Wallet – software solution by the Digital Wallet Service Provider used for mobile payments, enabling adding of payment card(s) to the application for the purpose of digitalisation and use at points of sale, at ATMs, as well as on web pages and applications of merchants supporting this payment method. Digital Wallet is an application with which a client can make payment on POS terminals having the option of contactless reading, both in Serbia and abroad, through the devices having NFC (Near Field Communication) wireless communication, as well as in the applications and web pages of the merchants accepting this payment type for specific digital wallet Service Providers.

Digitalised Card – personalised security element in the Digital Wallet that is generated in the process of the digitalisation of valid Bank payment card, which can be used as a payment instrument for initiating and executing payment transactions at points of sale, on web pages and applications of the merchants supporting this payment method. The Bank enables the digitalisation of VISA and Mastercard debit and credit payment cards issued by Erste Bank to private individuals and legal entities, entrepreneurs, and registered agricultural holdings

The Bank shall be entitled to, during the Card validity and/or automated Card re-issuance, change a type of payment Card, of same or other payment Card brand in which case, the Bank will, excluding any additional costs, make the change of the Card used by the User and ensure the functionalities that correspond to the functionalities of the card which is replaced.

Use of Digital Wallet Functionality

To use the digital wallet functionality, a User is required to:
- Have a device with the NFC technology, supporting the digital wallet service and/or a device

compatible with relevant application (hereinafter: adequate device),
- download and install the Digital Wallet application on an adequate device unless such application exists on such device,
- connect the downloaded Digital Wallet application with his/her account on the adequate device,
- set the device closing using one of the methods enabled on the device (pattern, fingerprint, PIN code, face scanner, etc.).

In order to avoid doubt, solely digital wallet Service Provider shall determine the type and characteristics of the device on which it is possible to install the application and arrange the Digital Wallet service provision. Use of the digital wallet functionality is requested by a client selecting an option for adding card and accepting these Terms and Rules in the digital wallet application.
The Bank has enabled its clients the digitalisation of the VISA debit and/or VISA credit card and Mastercard debit and/or Mastercard credit card (hereinafter: Card) issued by the Bank to its Clients.

Payment Card Digitalisation Process

In order for the User to add the existing Card issued by the Bank into previously downloaded and activated Digital Wallet application, the User is required to:

- hold an activated valid Card,
- have a mobile telephone number of the mobile operator registered in the Republic of Serbia, recorded in the Bank's system,
- when adding the card in the Digital Wallet, insert the data necessary for the Card digitalisation into relevant fields (card number, valid thru date, and three-digit CVV code).

During the card digitalisation process, the Digital Wallet application may overtake certain data from the User's account (name, surname, state, address of residence, zip code, apartment number, and telephone number), which the User confirms or changes, as necessary. The Bank shall not have access to the aforementioned data.
Following the payment card registration, the User shall receive one-off verification code (SMS OTP) sent to the mobile telephone number registered at the Bank. With a view to successfully completing the process, the Client shall input the received code into the field provided for the input in particular box. User shall not bear the digitalisation expenses.

Digitalised Card Use

Using a digitalised card, the User may perform secure payment at stores, in applications, and web sites supporting and accepting this payment method.

Consent for the execution of a payment transaction initiated by using Digitalised Card in Digital Wallet shall be granted by the User by tapping relevant devices on POS terminal or by selecting the payment option using the Digital Wallet on the web point of sale and inputting personalised security elements determined by the user or arranged with the Service Provider.

For any transactions executed with the Digitalised Card, the Bank will debit the User's account it is tied to. Card registered in the Digital Wallet.

For payment transactions executed with the Digitalised Card, if they are provided for in the Bank Tariff List, collection of fees shall be made in the same manner as if a transaction is initiated with the User's physical Card.

Since the User has an option to add more than one payment cards in his/her Digital Wallet,
historically first card added by the Client into the Digital Wallet shall become a default card for making payments. If the User wants to make payment using another digitalised card, it is necessary to select it before payment transaction initiation. In the Digital Wallet application, the Client can subsequently adjust and change the default card.

If, for any reason whatsoever, the agreement based on which the User has been issued the Card based on which the Digitalised Card is generated is terminated or the Bank, for any reason whatsoever, denies the right of Card use (blocks the card), the Digitalised Card use shall be terminated at the same time.

Deletion of the Digitalised Card from the Digitalised Wallet shall not impact the possibility of the use of the

Card based on which a Digitalised Card has been deleted and if the User subsequently wants to use his/her card as a Digitalised Card, it can be re-registered in the Digital Wallet.
Deletion of the Digitalised Card from the Digital Wallet shall not release the User of his/her obligation to settle all liabilities arising from the use of such Digitalised Card prior to deletion.

Obligations of the User

To prevent any cases of unauthorised use of the Digital Wallet and digitalised card as well as any fraud, the User shall:

- protect the relevant device on which the Digital Wallet application is stored against any unauthorised access and/or use, keep it with due care with a view to preventing loss or theft and setting locking of the relevant device using one of the methods enabled on the device (pattern, fingerprint, PIN code, facial scan, etc.).
- the User shall not reveal or make available to third parties any data on the card and account the digital wallet is tied to, in particular the OTP code received in SMS, security elements from the payment card – card number, CVV on the back of the card. Revealing the data, the User acts in gross negligence and is exposed to the risk of the Card/Digitalised Card misuse, which could result in unauthorised transactions up to the amount of the funds available on the account the Card/Digitalised Card is tied to, and the Bank shall not be liable to the User for any arisen damage.
- immediately upon becoming aware thereof, the User shall notify the Bank on any event the consequence of which is loss, theft, unauthorised access, or use of a relevant device on which the Digital Wallet application is stored, misuse of the Card/Digitalised Card/Digital Wallet, by contacting the Bank's Call Center on number **021/6772116** or via e-mail address **sigurnost.kartice@erstebank.rs**;
- the User shall not permit any third party to use the Digital Wallet for executing transactions.
- the User shall not register his/her Digitalised Card on the mobile telephone or other relevant device of a third party;
- the User shall comply with other protective measures stated herein, which relate to the Card.

Obligations by the Bank

Starting from the fact that the Bank issues the Cards to the User that the User may digitalise in his/her Digital Wallet, the Bank shall, pursuant to the provisions of the Law on Payment Service, ensure the following:

- personalised security elements of the Card are made available solely to the User whom the Bank has issued such Card;
- the User may, at any time, notify the Bank on loss, theft, or misuse of the device on which the digitalised card is stored or request re-enabling of the Digitalised Card when conditions for blocking thereof are terminated, by contacting the Bank's Call Center at number **021/6772116** or to e-mail address **sigurnost.kartice@erstebank.rs**;
- prevent any further Digitalised Card use after the User has notified the Bank on loss, theft, or misuse of the device on which the Digital Wallet application is stored, or on the Digitalised Card misuse.

Termination or Restriction of the Rights of Digitalised Card Use

The Bank shall, at any time, be entitled to prevent adding of the Card in the Digital Wallet and/or permanent or temporary Digitalised Card use if any of the following conditions is met:

- in the event of suspicion that an unauthorised person tries to add the card in the Digital Wallet;
- if, in the process of adding a Card into the Digital Wallet, the Bank obtains an information that the Mobile Device to which the Card is added has been lost or stolen;
- if the Bank prevents adding of such Card type into the Digital Wallet or the Bank does not further permit adding of the card into the Digital Wallet of the service provider;
- if there is a suspicion of an unauthorised use of the Card and/or Digitalised Card, and/or Card use with the intention of fraud;
- in the event of blocking or expiry of the Card based on which the Digitalised Card has been created;
- upon the User's request.

Card blocking and/or prevention of use by the bank shall also apply to the Digitalised Card, created based on the Card. Digitalised card blocking must not result in blocking of the Card based on which the Digitalised Card is created. If the digital wallet Service Provider, for any reason whatsoever, prevents the User to add and use

the Bank's Digitalised Card, the User may also contact the Service Provider. The Bank is not able or obligated to impact the Service Provider in terms of the availability of the Digital Wallet service for the User.

General Provisions

The Bank shall not be liable for the Digital Wallet application functionality:

- when lack of the Digital Wallet application functionality arises on the side of the digital wallet application Service Provider, the bank could not impact, whereby such lack of functionality does not relate to the part of the Bank's application for the provision of payment services when a Client does not meet the prerequisites for the use of the Digital Wallet application, in particular those listed in Section Use of Digital Wallet Functionality herein;
- in the event of defects or deficiencies of the User's equipment, network, or other in other events that prevent the Digital Wallet use

in accordance with and to the extent set out in the provisions of the Law on Payment Services, the Bank shall be liable for the Digital Wallet application if any circumstances, interruptions, or errors in the digital wallet result in any unauthorised, non-executed, or incorrectly executed payment transaction or cause a damage to the User. In the event of any loss, misuse, or theft of the data necessary to use the Digital Wallet or in any other case of unauthorised use of the Digital Wallet, the Bank shall retain the right not to replace the Card.
In the event of suspicion about the misuse of the Card data, possibility of the misuse by the User, or execution of unauthorised transactions received from the card association, the Bank shall be entitled to unilaterally disable further possibility of the digitalised card use.

Closing Provisions

If the User has any issue regarding the functionality use, the User can contact the Bank's Call Center via the following telephone number: **0800201201.**
The Bank shall not process the User's personal data in the process of card digitalisation and does not obtain any such data.
Inputting the personal data and initiating the Card digitalisation in the Digital Wallet application, the User shall provide the aforementioned personal data to the digital wallet Service Provider, in accordance with the rules and notice on personal data processing defined by the digital wallet Service Provider for the purpose of the card digitalisation.
Provisions herein relating to the liability for damage, protective and other measures, and payment card blocking shall accordingly apply to the Digitalised Card/Digital Wallet, as well.
Applicable agreement provisions referred to in the framework agreements executed with the payment service users and/or provisions of the General Terms relating to the Card use issued by the Bank, as well as the provisions referred to in the General Terms relating to unauthorised, non-executed, or incorrectly executed payment transactions arising from the digital wallet use, in the event referred to in Article 27a hereof, shall apply to any rights, obligations, conditions, and responsibilities of the Digital Wallet use not defined herein.

E-Bank and M-Bank

Article 36
The User may execute the agreement on E-Bank and M-Bank services with the Bank, which are the Bank's applications enabling the User to access the account balance and turnover on accounts, execute banking services agreements, and initiate payment transactions.

NovoKlik, Office Banking, and Erste eBiz (hereinafter: E-Bank Services) shall be the E-Bank services provided by Erste Bank a.d. Novi Sad (hereinafter: Bank).

Erste mBiz (hereinafter: M-Bank) means the mobile banking service of Erste Bank a.d. Novi Sad (hereinafter: Bank).

The use of Erste eBiz service is conditioned with the use of Erste mBiz service and it may not be independently agreed or used.

E-Bank and M-Bank shall enable the user to execute and review payment transactions and review account balance.

These General Terms shall define in detail the options of each of the E-Bank and M-Bank services and stipulate the rights and obligations of using thereof. Smart card is a security device with installed chip, on which e-certificate and cryptographic keys necessary for e-banking service are stored. Smart card shall be used for electronic identification within card validity.

- Smart card reader means a device for reading data from smart card.
- Personal number (PIN) means a combination of characters assigned to the User by the Bank which, together with smart card, ensures the use of e-banking.
- The User identification means a set of elements necessary for E-bank service identification and use
- Username is the parameter comprising a number of characters, received by the User when Erste eBiz service is registered, used for the authentication to such service
- Registration and activation code – combination of numbers and letters, assigned to the User by the Bank.
- mToken is a solution within the Bank's mobile application generating one-time authentication or authorisation codes and enables log-in and account verification in the eBiz application.

E-Bank and M-Bank Service Use Agreement

E-Bank and M-Bank User may become any legal entity holding the current account at the Bank (hereinafter: the User), which provides the Bank with correctly filled-in and signed Application Form or flags a dedicated field in the Account Opening Application ,and accompanying documentation for the approval of the E-Bank and M-Bank service use, which shall be an integral part of Agreement on Current Account Opening and Maintaining, providing for the possibility of using such services.
The Applicant shall, by filling in certain fields of the Application Form, determine the level of authorisation of the persons accessing the E-Bank and M-Bank services. All persons listed in the Application Form shall confirm the accuracy of stated data with their signature. The authorised person shall, with his signature and stamp, guarantee for the provision of authorisation to authorised users and, at the same time, grant authorisation to the users with the right of verification to arrange additional functionalities through the E-Bank and M-Bank services. Any authorised person shall have certain authorisation type for the E-Bank and M-Bank use assigned by the User's Legal Representative in the Application Form.
Use of the user identification submitted by the Bank shall be deemed as the consent for the use of the E-Bank/M-Bank.
Legal representative may revoke granted authorisations and he shall notify the Bank on any change in the level of the authorisation by the persons having access to the E-Bank and M-Bank services by providing the bank with relevant notice.

E-Bank and M-Bank Services
The User may, at own choice, opt for using the following:

E-Bank services:
- NovoKlik
- Erste eBiz
- Office Banking

Erste eBiz M-Bank Services:
- Erste mBiz

E-Bank and M-Bank Service Scope

- Novoklik means Desktop user application enabling the User to view account balance; view account turnover; view account statement; execute payment using RSD (including instant – urgent ones) and FX payment orders on current date and on a future date; receive and send personal and general messages.
- **Office Banking** means Desktop user application enabling the User to view account balance, view account turnover; view account statements; execute payment using RSD payment orders on current date and liabilities payment on a future date (including instant – urgent payment orders).

- **Erste eBiz** service means a Web user application enabling the User to perform the following: access account balance; view of account turnover; view statements; execute payment orders for RSD (including instant – urgent orders) and FX payment transactions on current date and on a future date; activate Erste mBiz m-banking service. The Bank shall enable the User to use all of the functionalities offered in the Erste eBiz application, and the User shall, at own discretion, determine which of the functionalities he wants to use.
- **Erste mBiz** service means a mobile application enabling the User to perform the following: access account balance; view of account turnover; view statements; execute payment orders for RSD (including instant – urgent orders) and FX payment transactions on current date and on a future date. mBiz service enables log-in to the eBiz application and order signing in the eBiz application by generating mtoken codes as the second authentication factor. The Bank shall enable the User to use all of the functionalities offered in the Erste mBiz service, and the User shall, at own discretion, determine which of the functionalities he wants to use.

The Bank shall reserve the right to change the volume and content of the E-Bank and M-Bank services on which the User shall be notified through the content of its web pages.

E-Bank and M-Bank Service Use

NovoKlik – Upon the approval of the application form by the Bank, the Bank shall provide the User with the smart card reader, smart card, and personal identification number (PIN), instructions for downloading installation package and User Manual through link.
For the approval of using the NovoKlik service, the User shall, in addition to the Application Form, also sign the following documents:
In the event the User does not have an issued e-certificate for individual user, the User shall also provide the Bank with the following documents:
- General order for the issuance of qualified personal digital certificates for legal entity
- Application for receiving digital certificate of legal entity (for each individual user for which smart card issuance is requested).
In the event the User has already got an issued Halcom e-certificate, the following is to be provided:
Certificate in writing on the sameness of digital certificate for authorised individual user.
If the User has already got the above-mentioned, the Bank will enable the User the use of the existing smart card upon the approval of the submitted documentation by the Bank.
The User may begin using the service upon the installation of the programme in accordance with received instructions. The User may be provided with the necessary user support by an authorised person of the Bank.
Smart card shall be issued for the validity period of the e-certificate determined by issuer, and upon the expiry of such period, the e-certificate validity must be renewed. Card renewal means the issuance of new smart card.
Receipt and sending of E-invoices to NovoKlik service will be ensured upon the approval of application form by the Bank.

Office Banking – Upon the approval of application form by the Bank, the Bank shall provide the User with the smart card reader, smart card, and personal identification number (PIN), instructions for downloading installation package, and User Manual through link.
If the User has already obtained the above-mentioned, the Bank will enable the User to use the existing smart card after the submitted documentation is approved by the Bank.
The User may begin using the service upon the installation of the programme in accordance with received instructions. The User may be provided with the necessary user support by an authorised person of the Bank.
Smart card shall be issued for the validity period of the e-certificate determined by issuer, and upon the expiry of such period, the e-certificate validity must be renewed. Card renewal shall not require the issuance of new smart card.

Erste eBiz – After the Bank approves the eBiz application form, the Bank sends the User a username by e-mail, and the User generates an mToken code in the mBiz application, thereby activating the account. The User can access the eBiz application using the username and the mToken code generated in the Erste mBiz application. The Erste eBiz application may also be accessed by the User via Halcom e-certificate and password received established in the course of the activation, following the PIN entry. Instruction on the Erste eBiz functionality use shall be available on the web page for the service activation.

Following Erste mBiz application, the User may opt for log-in using offered biometric data as well as to grant consent for payment transactions in the same manner.

Erste mBiz – After the consolidated application form is approved by the Bank for Erste eBiz and Erste mBiz service the Bank shall provide the User, by e-mail, with the registration code and activation code in the SMS to the registered mobile telephone number (hereinafter: user identification). The User shall start using the Erste mBiz service following the receipt of the user authentication and, when the Erste mBiz service is accessed for the first time, the User shall create mToken and generate a four-digit PIN used when logging on to the application. The instruction on the Erste mBiz functionality use shall be available on the web page for the service activation.

All of the forms of using the E-Bank and M-Bank services which are electronically executed applying the prescribed user identification shall be identical to signing.
The User shall fill in all orders and any necessary specifications in an orderly and accurate manner and authenticate them in the manner provided for in the user identification and specific application, taking care of the available amount of funds on accounts at the Bank, otherwise the User shall bear the risk of non-execution, incorrect execution, and/or rejection of payment order execution.
The User may execute international payment transactions (for the E-Bank and M-Bank services supporting international payments), including the obligatory input of number and date of document based on which the international payment is executed (agreement, invoice, proforma invoice, etc.). The User is not obligated to provide the Bank with the original order. Documentation which, if prescribed, evidences the grounds and obligation of payment to abroad shall be submitted by the User to the Bank through the application (in the event of the application which supports that) or by e-mail, whereby the Bank shall be entitled to be provided with the original for examination.
The Bank shall guarantee to the E-Bank and M-Bank service User to freely dispose of funds on all demand accounts, opened based on the agreement entered into with the Bank, up to the amount of funds on account, also including overdraft on such accounts.
Payment order execution deadline shall be defined in the Bank Cut-off Times.
The Bank shall not assume liability for the non-availability of the E-Bank and M-Bank service resulting from technical issues of computer equipment, breakdown, or disorders within telecommunication channels, power system outage, or as a consequence of force majeure, and it shall not assume liability for any damage resulting from any loss or destruction of any data and equipment of the User due to the installation and use of the E-Bank and M-Bank service.

Protection of Payment Instrument Data and Reporting of User Identification Loss, Theft, and Misuse
The User shall keep secrecy of the user identification and smart card and accept full liability for any obligations resulting from the attributes of the user identification and/or smart card. The User shall, immediately upon the receipt of the user identification, take any reasonable and appropriate measures for the purpose of protecting the personalised security elements of the user identification.
The User shall immediately and inevitably notify the Bank on any theft, loss, and non-authorised use of his user identification, SMART card, or other security device and on any other form of breaching security the User becomes aware of, and initiate blocking of the E-Bank and M-Bank service use, in one of the following manners: initiating the e-bank service use blocking in the manner provided for in the application, in person at the Bank branch, or by calling contact center at 021/423-364 or 0800-201-201 on business days 8 a.m. – 5 p.m. and on Saturday 8 a.m. – 1 p.m. or by sending e-mail requesting blocking the service of the e-bank to the e-mail address: blokadaplatnoginstrumenta@erstebank.rs

Protective and other Measures
The User executing payment transactions through E-Bank shall be in compliance with the following security requirements:
- The User shall, on the devices from which E-bank services will be used, ensure licensed, properly configured operating system and software, as well as anti-virus programme, including set updating on a regular basis, and use of personal firewall programme is recommended, as well;
- access E-Bank application, use current Web browser version and set automated updating of the programme;
- the User shall not use the option that Web browser remembers user name and password or other security element used for the E-bank application. It is recommended that the User changes password on a regular basis (e.g. on a monthly basis), and the User must not communicate the password to others. - When creating a password, frequent words, or personal data known to others should not be used (e.g. names of children,

date of birth, telephone number, account number, etc.) should not be used. The User must not keep the password on his mobile devices;
- the User must not respond to messages (SMS or through social networks), requests in pop-up windows, and e-mails, or those otherwise received through the Internet, which require the disclosure of sensitive and confidential personal information, or data of financial nature.
– report to the Bank any loss or theft of mobile device, as well as change in the holder of the telephone number. Otherwise, the Bank shall not be liable for any cases of fraud.
- The User must not leave the E-Bank application turned on, and he shall be liable for the damage arising from the misuse by any persons from his environment.
- if the User notices any unusual operation or appearance of the E-Bank application, he shall immediately notify the Bank thereof.

The User who executes payment transactions through M-Bank shall be in compliance with the following security requirements.
- on the devices from which M-Bank services will be used, security measures installed by the producer (such as jail break or root) must not be disabled;

Recommendations for safe M-Bank use:
- the User should activate the security functionalities offered by mobile device (for example, device screen locking after certain period of inactivity, biometric screen unlocking, etc.).
- use the programme for the protection against malware and viruses,
- the User should act carefully in the event of bluetooth connection with other devices and disable the Bluetooth connection when it is not necessary. In the course of connection of other device with mobile telephone, it is recommended to use a safe method of connection requiring PIN generation for determining the source device initiating connection. It is necessary to ignore any attempts of connection which are unknown to the User.
- the User should be cautious when mobile device is connected to be charged on the devices of other people (such as desktop or notebook computers of others or ports for charging mobile devices in public places). By connecting mobile device to charging port, data and application on the device could be accessed under certain conditions, whereby the User is not aware thereof.

The User must not respond to any messages in which the sender addresses the User on behalf of the Bank or asks the User to provide any of his personal data, user identification, account number, etc. The User is obligated to immediately report any such case to the Bank.

If the User notices any unusual operation or appearance of the E-Bank application, the User shall immediately notify the Bank thereof.

The User shall report to the Bank any loss or theft of mobile device, as well as change in the holder of the telephone number if it is used for executing payment transactions through the M-bank application. Otherwise, the Bank shall not be liable for any cases of damage and fraud.

The User shall follow the Bank web site on a regular basis, in particular, notices by the Bank in connection with the E-Bank and M-Bank services and adequately respond, in accordance with such notices.

The User shall ensure, for the purpose of prevention of fraud, to be informed on the security rules of using payment instruments on the web site of the Association of Serbian Banks www.ubs-asb.com/korisnici-finansijskih-usluga/bezbednost-bankarskih-klijenata.

Payment Instrument Blocking
The Bank may reject or delay transaction execution and/or block any further use of payment instrument (E-Bank and M-Bank) if there are reasonable grounds relating to payment instrument security, in the event of suspicion of unauthorised use of payment instrument or the use thereof for the purpose of fraud, or if there is an increased risk that the User will not be able to meet the payment obligation when the use of such instrument is related to the approval of loan and/or overdraft to the User.

The Bank shall notify the User on its intention of payment instrument blocking and reasons of such blocking. Unless it is able to notify the User thereof prior to payment instrument blocking, the Bank shall do so immediately upon blocking. Notification on the intention of blocking or payment instrument blocking shall be delivered by the Bank to the User in the manner set out in the Framework Agreement unless the provision of such notification is prohibited under regulations or if there are reasonable security reasons not to do so.

The Bank will ensure re-use or replacement of the payment instrument with a new one – when reasons for blocking thereof cease.

The Bank will automatically block the service use to user if incorrect user data are input three times during logging. In such case, the User may unblock service access in person in the Bank premises or by calling the User Support.

If the Bank, using special application, determines that the operating system used by the User for initiating payment transactions through the Officebanking/Novoklik/Erste eBiz and Erste mBiz is virus infected enabling the unauthorised person to access the security elements of the payment instrument and unauthorised use thereof, due to which payment instrument security is affected, the Bank will prevent any further use of the Officebanking/Novoklik/Erste eBiz and Erste mBiz, and request the User to take actions to eliminate such virus.

The Bank shall not be liable for any damage arisen from the execution of unauthorised transactions if they have been executed for the reasons referred to in the above paragraph.

The Bank will ensure the re-use of the Netbanking/Officebanking/Novoklik/Erste eBiz and Erste mBiz service after the User takes actions upon its request, and after it is determined that there is no further threat to the security of the payment instrument use.

Special Security Actions Implemented by the Bank

For the purpose of protecting the security of Payment Service Users, the Bank conducts monitoring of payment transactions and, based on indicators and expert assessment, determines whether there are any security or safety threats, risks of unauthorised use of payment instruments, risks of executing unauthorised payment transactions, the presence of malware on devices through which the User performs payment transactions via electronic banking, suspicion of fraud and abuse, and any other indications that may suggest that the User's funds are affected or that the User has already suffered harm.

If the Bank assesses that, for the purpose of protecting the User's funds, it is necessary to take actions to eliminate the identified risks and security threats, the Bank has the right to:

– block the User's account in order to prevent the outflow of funds resulting from the compromise of a card, eBank or mBank applications, or prevent misuse or fraud by third parties involving the User's account funds,

- block payment instruments (cards, eBank, and mBank),

– refuse the execution of payment transactions it considers risky, or postpone the execution until it is verified with the User whether the transaction is unauthorised, or require additional authentication for such transactions,

- take other actions deemed as necessary with a view to protecting the User.

The Bank shall inform the User on its intention to implement, or of any already implemented, security actions, as well as of the reasons for taking such actions. If the Bank is not able to inform the User before taking the actions, the Bank is obliged to do so immediately after the measures have been taken unless providing such notification is prohibited by regulations or there are justified security reasons for not doing so. .
Where possible in the specific case, the Bank provides certain instructions to the User in order to eliminate the identified risks, and the User is obliged to provide additional information about the transaction and the circumstances relevant for assessing and mitigating the risks at the Bank's request.
After the reasons for taking the actions cease to exist, the Bank enables the User to dispose of the funds in the account and use the payment instruments, and informs the User thereof.

Liability for Damage
For any damage arising from non-approved payment transactions by using E-Bank/M-Bank, the User shall be liable in accordance with Article 26a hereof.

Notification and Complaints

The User shall be reported on payment transactions executed through the E-Bank and M-Bank services by the Statement provided electronically. The User agrees to receive additional notifications, of informative or other nature, through various Bank distribution channels.
The User may file complaint regarding a transaction executed through the E-Bank and M-Bank, shall be no later than 5 days from the date of debiting. Complaint may be sent by message within the E-Bank and M-Bank services, by e-mail at info@erstebank.rs or by telephone to no. 0800 201201 (whereby the complaint is to be submitted in writing as soon as possible) by the authorised person of the User, stating the number of the order, order execution date, and accurate and clear description of the data regarding which the complaint is filed.

The deadline referred to in the above paragraph is not applied to the transactions referred to in Article 27a hereof

The Bank shall start the procedure of complaint solving immediately upon the receipt and notify the User on the complaint procedure completion.

Upon the expiry of the deadline for complaint filing, the Bank will not take such complaint into consideration, and the User shall be liable for any material consequences of disputed transactions.

Fees
Fees for the E-Bank and M-Bank services use shall be collected through the User's account or by other collection form in accordance with the Price List.
The E-Bank and M-Bank services use will be immediately charged, or an invoice will be issued by the Bank. The User accepts that the Bank may, for the purpose of fee charging, debit the User's accounts without obtaining specific signature and excluding obligation of providing the User with prior notification.

Service Termination
The User shall be entitled to cancel the E-Bank and M-Bank service use, by filing request in writing within 30-day notice period which shall start to run from the date of request receipt. Prior to the expiry of such notice period, the User shall return any assigned user identifications and settle any outstanding liabilities to the Bank. The Bank shall reserve the right to reject the User's Request for the E-Bank and M-Bank service use and may, at any time, withdraw any rights for using the E-Bank and M-Bank services if the User has failed to execute transactions through the Bank longer than 6 months, settle liabilities on a regular basis and at maturity, be in compliance with the General Terms, applicable regulations and instructions of the Bank, and if there are reasons of security protection due to the suspicion of the user identification fraud.

Payment Transaction Security Instruments

Article 37
When opening the account and issuing payment instruments, the Bank may bind the User to provide it with a number of bills of exchange in accordance with its internal acts and individual request by the Bank for the purpose of the collection of fees and commissions relating to payment transaction services if enforcement becomes necessary.

In the event the Bank has used the bills of exchange referred to in the above paragraph, the User shall be required to provide new bills of exchange. Orders of the User that fails to meet the Bank's request will not be executed by the Bank.

In the event the Users have any overdues based on fees and commissions from payment transactions, orders will not be executed by the Bank and the User's account will be blocked until the settlement of due liabilities towards the Bank.

Service Cancellation, Unilateral Agreement Termination, Account Closing, and Denial of Payment Service

Article 38
If the User wants to stop using payment services with the Bank and/or unilaterally terminate account agreement, the User shall file Account Closing Application to the Bank in the form prescribed by the Bank. In the request, it is necessary to fill in data on account with other bank to which any funds on the User's account will be transferred by the Bank, as well as date of the termination of account agreement which may not be shorter than 15 days from the date of filing the Application.

Prior to filing the application for account closing, the User shall settle any liabilities based on account maintenance, as well as any overdue fees and commissions and/or the User shall, prior to closing, ensure sufficient funds from which the collection of overdue fees and commissions will be made by the Bank.
If the User has met the obligations referred to in the above paragraph, the Bank shall act upon the User's request and close the account in the Bank system as well in the National Bank of Serbia account register. Otherwise, the Bank shall not act upon the User's request.

Article 39
The Bank shall be entitled to unilateral termination of current account agreement and/or to cease to provide payment services to the User in the following cases:
- if the Bank concludes that the User applies unauthorised actions affecting the operation of both the User and the Bank (e.g. misuse of signature, stamp, unauthorised order completion and submission, etc.)
- if the User fails to report accurate data and data changes in accordance with regulations and in accordance with Art. 6 to 10 hereof, even after the request in writing by the Bank, within 15 days from request submission
- if the user fails to provide documentation evidencing reported data and data change in accordance with regulations or upon the request by the Bank, even upon the request in writing by the Bank within 15 days from request submission – if it is concluded by the Bank that the User uses the Bank services for any activities deemed to be money laundering and terrorism finance, in accordance with the Law on the Prevention of Money Laundering
- if the User fails to fulfil the obligations provided for in the Framework Agreement
- in other cases prescribed in the Law on Payment Services and Law on Foreign Exchange Operations (provisions of account closing referred to in decisions on account opening, maintaining, and closing), regulations in the area of sanctions, and other regulations
- in other cases of the User's conduct and actions which are a significant reputation risk to the Bank.
- in any cases which are prescribed in the Bank General Terms of Business.

In the cases referred to in the above paragraph, the Bank will provide the User with the notice on the account closing or denying payment transaction services stating the reason of closing and/or denying payment transaction services.

The User shall, upon the receipt of such notice, provide the Bank with the account held at other bank to which any funds on the User's account with the Bank will be transferred by the Bank.

In the event the User fails to provide the account held at other bank, any funds of the User's account with the Bank will be forwarded to special Bank account until the time of the User's request for transfer or outgoing payment, and the User's account will be closed.

The User's accounts will be closed by the Bank on 15th day upon the submission of notification to the User referred to in paragraph 2 of this Article. Account closing shall also be immediately recorded in the National Bank of Serbia account register.

Article 40
The Bank will temporarily deny payment service provision to the User:
- if the Bank suspects that the User applies any unauthorised actions affecting the operation of both the User and the Bank (e.g. misuse of payment instrument, signature, stamp, unauthorised order completion and submission, etc.)
- if the User fails to report accurate data and data changes in accordance with regulations and in accordance with Art. 6 to 10 hereof until the time of Users reporting respective change
- if the User fails to provide the documentation evidencing reported data and data change in accordance with regulations or upon the request in writing until the time the User provides documentation
- if it is suspected by the Bank that the User uses the Bank services for the actions considered to be money laundering and terrorism finance in accordance with the Law on the Prevention of Money Laundering and Terrorism Finance
- if the Bank receives order by a regulatory authority (Ministry of Finance, Ministry of Internal Affairs, and other regulatory bodies and authorities) for the temporary denial of payment transaction services to the User.

The User shall be notified by the Bank on temporary denial of payment services in writing except in the event of the service denial referred to in indent 5 of the above paragraph, and evidence and/or documentation will be required for the User to confirm meeting of conditions for the termination of payment service denial.

The Bank will suspend payment service denial only upon the provision by the User of requested evidence referred to in the above paragraph.

Payment Account Debiting without Payment Order

Article 41
The Bank will debit the User's account – without payment order, in the following cases:
1) in the process of enforcement and/or forced collection taken against the user, in accordance with the law;
2) for the purpose of collecting due fees for the Bank services, due claims based on the loan approved by the Bank to the User, or other due claims of the Bank to the User if such collection method is agreed;
3) in the event of filing bill of exchange for collection issued by the User if there are sufficient funds for the collection using the bill of exchange;
4) in the event of the correction of the error by the Bank arising from the execution of payment transactions, incorrect booking of account debiting or crediting
5) in the event referred to in Article 27 and 27a hereof
6) In other cases provided for herein
7) in other cases prescribed in the law.

Payment Service User Protection

Article 42
If the payment service provider or electronic money issuer fails to comply with the provisions of this Law, other regulations or general terms of business governing payment services or electronic money, good business practices relating to these services or obligations arising from payment service contracts and/or contracts concerning electronic money – the payment service user and/or electronic money holder are entitled to the protection of their rights and interests.
The procedure of protecting the rights and interests of payment service users and electronic money holders shall be subject to provisions of the law governing the protection of financial service consumers which relate to exercising the protection of rights and interests of financial service consumers.
Provisions of the law governing the protection of financial service consumers shall apply *mutatis mutandis* to unfair contract terms and unfair business practice in the field of providing payment services and issuance of electronic money, including the procedure of their prohibition.

Right to Complaint
The User shall be entitled to file complaint to the Bank if he considers that the Bank is not in compliance with the provisions of the Law on Payment Services, general terms of business, or good business practice relating to payment services or obligations from the agreement executed with user.

The User shall be entitled to complaint of 15 days upon becoming aware of a disputable event, but, in any case, within three years from the date when his right or legal interest has been breached.

The Bank shall provide provider of such claim with a clear and understandable response to claim no later than within 15 days from the day of complaint receipt, and in such response, point out his right to file claim to the National Bank of Serbia.

The Bank shall, in its business premises in which services are rendered to users, by mail, e-mail, eBanking, and mBanking, and on its web-site provide for the possibility of filing complaint and/or enable the user to be informed on the manner of filing complaint and on the method of handling complaint.

The Right to Filing Claim to the National Bank of Serbia

If he is not satisfied with response to his complaint, or response has not been provided within the prescribed term, the complaint provider may, prior to initiating legal proceedings, file claim in writing to the National Bank of Serbia.

Complaint provider may file claim within six months from the date of response receipt or the expiry of the term for providing response.

The National Bank of Serbia shall notify claim provider on finding under such claim within three months from the date of claim receipt, and in more complex cases, such deadline may be prolonged by maximum three

months, on which the National Bank of Serbia shall notify claim provider in writing prior to the expiry of original deadline.

Extra Judicial Settlement of Disputable Relation

If a complaint provider is dissatisfied with response to his complaint or he has not been provided with such complaint within the prescribed term, disputable relation between complaint provider and financial service provider may be solved in extra judicial proceedings – mediation procedure.

After initiating mediation procedure, the user may not file claim thereafter unless this mediation has been completed in suspension or waiver, and if claim has already been filed – the National Bank of Serbia will stop proceedings thereunder and/or suspend the proceedings if mediation is completed in agreement.

Mediation procedure shall be initiated at the proposal of a party in dispute accepted by the other party. This proposal must also include deadline for the acceptance thereof, which may not be shorter than five days from the date of submitting such proposal.

The mediation procedure shall be confidential and urgent.

Parties in dispute may make decision to implement the mediation procedure before the National Bank of Serbia or other authority or person authorised for mediation.

Mediation procedure before the National Bank of Serbia shall be free of charge for the parties in such procedure.

Mediation procedure may be finalised with agreement between parties, suspension, or waiver.

Closing Provisions

Article 43
The Bank shall, within the appropriate term prior to the execution of the framework payment account agreement, at the same time when other information is provided as set out in the Law on Payment Services, provide the User with the Overview of Services and Fees, free of charge – in hard copy or other permanent data carrier, in the manner ensuring the evidence on the executed delivery. The Bank will make the Overview of Services and Fees available at its teller desk facilities and publish it on the Bank's web site.

Executing Agreement on Opening and Maintaining of Account/Payment Card Issuance/E-Bank and M-Bank Use, the User shall accept the provisions of the Bank General Terms and the Price List under which payment services shall be charged. The General Terms shall deem to be an integral part of agreed payment services.

The Bank General Terms, Price Lists, and Cut-off Times shall be published on the bank Internet address.
The User shall ensure to be informed on the content of the General Terms prior to signing the agreement and to be informed on any amendment of the General Terms.

The Bank shall present any changes relating to payment services, irrespective if they are contained in the Bank General Terms or other acts, in the Bank's points of sale and in the Bank's web site 15 days prior to the beginning of the application thereof.

The Bank shall notify the User on any changes in the General Terms / Framework Agreement no later than 15 days prior to the effectiveness of the proposed changes.

Unless the User, within 15 days prior to published amendments coming into force, cancels payment services, it shall be deemed that the User shall accept such amendments.

The User shall be entitled to be informed on any conditions of payment service execution at any time through personal enquiry at the Bank's points of sale, by telephone call to the Bank Call Center on number 0800201 201 or 060 7979 000, as well as by sending a question in writing to the Bank to the address ebank.kontakt@erstebank.rs

Article 44
The User accepts to receive additional notifications, of informative or other nature, through various Bank Distribution Channels.

The Client agrees and herewith authorises the Bank to use, process, and retain any data presented to the Bank when executing, as well as the data obtained by the Bank in the implementation of this Agreement, which are, in sense of the Personal Data Protection Law, deemed personal data, and in sense of the Bank Law deemed as secrecy, for the purpose implementing this Agreement, improvement of business cooperation with clients, development of its services and products, as well as for the purpose of implementing researches and analyses required by the Bank.
The Client agrees and herewith authorises the Bank to forward the data referred to in the above paragraph and outsource processing thereof to Erste Group members, Forum for Preventing Fraud in Credit Transactions, or a third legal entity, with the aim of achieving high quality and efficient data processing, reporting at Erste Group level, as well as for other business requirements of the Bank provided that the Bank has, in the contractual relation with the above-mentioned legal entities which are transferred data and outsourced processing, ensured the same or higher level of the protection of confidentiality, secrecy, and integrity applied to its clients, as well as that it has ensured that such data are adequately protected against any frauds, destructions, losses, unauthorised changes, or accesses and that persons engaged in processing are bound to keep data secrecy.

Article 45
The General Terms, including agreement or application form for individual payment services, Cut-off Times, Price List, and general terms of use for individual payment services shall be an integral part of the framework agreement on payment service provision.

Signing the Agreement/Application Form, the User shall acknowledge that it is aware of the provisions of the General Terms and accept the application thereof.

the Bank General Terms of Business, legislation, and other acts of the Bank governing operation with Users shall apply to any issue which is not set out in these General Terms.

The provisions of Chapter II of the Law on Payment Services excluding Articles 14 and 15, Article 16. paragraphs 3 and 4, and Article 32 of this law, as well as the provisions of Art. 51, 53, 54, 58, 60, and 63 of this Law, shall not apply to this Agreement.

Article 46
These General Terms shall apply to the users who have established the business relation with the Bank, the subject whereof shall include payment services before these General Terms have come into force, as well as to the users establishing business relation with the Bank after these General Terms come into force.

The General Terms shall come into force on **20 May 2026**, except for the provisions on the SEPA credit transfer which will come into force on 04 May 2026.