



ANNEX 6

SPECIAL TERMS AND CONDITIONS FOR THE USE OF ELECTRONIC AND MOBILE BANKING SERVICES APPLICABLE TO LEGAL ENTITIES AND ENTREPRENEURS

1. INTRODUCTORY PROVISIONS

These Special Terms and Conditions for the Use of Electronic and Mobile Banking Services for Legal Entities and Entrepreneurs of AikBank a.d. (hereinafter: the Bank) govern the mutual rights, obligations, and responsibilities of the Bank and legal entities and entrepreneurs when using electronic banking services (hereinafter: eBanking services) and mobile banking services (hereinafter: mBanking), in accordance with the Law on Payment Services (hereinafter: the Law).

The Bank provides the User with services via electronic networks as well as information on transactions available through such means, including the days and hours during which such services are accessible.

In line with technological advancements and the services offered to the User, the Bank may integrate new services within the electronic transaction network. Transactions carried out via such new services shall be executed in accordance with instructions issued by the Bank.

The Bank charges the User fees for the services rendered in accordance with the Bank's Price List. The Bank reserves the right to grant the User more favourable fees than those defined in the Price List.

By using any of the functionalities, the User confirms their acceptance of the terms of use and is responsible for acting in accordance with the user manuals.

These Special Terms and Conditions for the Use of Digital Banking Services for Legal Entities and Entrepreneurs, together with:

- the Framework Agreement on Terms of Use for Electronic and Mobile Banking Services,
- the General Terms and Conditions of AikBank a.d. Beograd (hereinafter: GTC),
- the Special Terms and Conditions for Payment Accounts and Payment Services for Legal Entities and Entrepreneurs,
- the Price List for Services of the Bank Applicable to Legal Entities and Entrepreneurs (hereinafter: the Price List),

- the Transactions Schedule for Payment Transactions for Legal Entities and Entrepreneurs, which constitutes an annex to these Special Terms and Conditions (hereinafter: the Transactions Schedule),
- the Transaction Limits for Electronic and Mobile Banking constitute the Framework Agreement (hereinafter: the Framework Agreement / Agreement).

2. Definitions of Terms

For the purposes of these Special Terms and Conditions for the Provision of Electronic and Mobile Banking Services applicable to Legal Entities and Entrepreneurs (hereinafter: the Annex), certain terms shall have the following meanings:

Digital Banking refers to the set of services and functionalities offered by the Bank, including:

- Electronic banking
- Mobile banking
- Contact Center and SMS services

Electronic Banking refers to the service provided through the Bank's electronic platform that allows the use of services related to a payment account using appropriate application software on a computer, in accordance with the Bank's current offering.

Mobile Banking refers to the service provided through the Bank's mobile application that allows the use of services related to a payment account using appropriate application software on a mobile telecommunications device, in accordance with the Bank's current offering.

Contact Center Service refers to the set of Bank services accessed via information and telecommunications technology and includes: the Interactive Voice Response (IVR) system and communication with Contact Center operators.

Interactive Voice Response (IVR) refers to a Contact Center service that enables access to information about the Bank's products and services.

SMS Service means a service through which the Bank enables the User to receive information via SMS messages on the



status and changes in their accounts and payment cards with the Bank.

User Manual means a Bank-issued document that explains how to use a specific service within Digital Banking for legal entities and entrepreneurs, available at the Bank's branches and on its website.

Payment Services User - the User refers to a legal entity or entrepreneur who has established a contractual relationship with the Bank regarding the use of Digital Banking for legal entities and entrepreneurs in accordance with these Special Terms and Conditions.

Authorized User refers to a natural person authorized by the User to access and use various functionalities within Digital Banking for legal entities and entrepreneurs.

Payment Transaction means a deposit, transfer, or withdrawal of funds initiated by the User as the payer or payee, or initiated on behalf of the payer, regardless of the underlying legal relationship between the payer and the payee.

Remote Payment Transaction is a payment transaction initiated via the internet or a device that may be used for remote communication.

Payment Order means an instruction from the User, as payer or payee, to the Bank requesting the execution of a payment transaction.

Transaction refers to a payment transaction executed using electronic or mobile banking.

Batch Payment Order means multiple payment orders grouped and submitted together to the Bank for execution using the Electronic Banking service.

Transaction Record refers to the list of Transactions on a selected account for a defined period.

Instant Credit Transfer refers to a domestic payment transaction up to RSD 300,000 (inclusive), marked as urgent, initiated via a paper payment order or other payment instrument at any time of the day, any day of the year, where the transfer of funds is executed in real or near-real time.

Payment Account refers to the account used for executing payment transactions, used to issue a payment order or initiate a payment transaction.

Initiation of a Payment Transaction refers to actions that are prerequisites for initiating the execution of a payment transaction, including the issuance of a payment order and the performance of authentication.

Payment Instrument means any personalized device and/or set of procedures agreed between the User and the Bank, used by the User to issue a payment order or initiate a payment transaction.

Payment Instrument Based on a Payment Card is any payment instrument, including a payment card, computer, mobile phone, or other technical device containing a payment application that enables the payer to initiate a payment transaction using the payment card.

Issuance of Payment Instruments is a payment service whereby the payment service provider issues a payment instrument to the payer based on an agreement for the initiation and processing of payment transactions.

Payment Brand refers to any physical or digital name, term, sign, symbol, or combination thereof used to identify the card payment scheme under which a card-based payment transaction is executed.

Co-branding of a Payment Instrument refers to the inclusion of at least one payment brand and at least one non-payment brand on the same card-based payment instrument.

Payment Application refers to the software or appropriate equivalent installed on a computer, mobile phone, or any other device that enables the initiation of a card-based payment transaction and the issuance of a payment order by the payer.

Acceptance of Payment Transactions refers to a payment service whereby, based on a contract between the payment service provider and the payee, the processing and transfer of funds to the payee is executed.

Account Servicing Payment Service Provider refers to the payment service provider who opens and maintains the payment account for the payer, i.e., the Bank.

Payment Initiation Service Provider is a payment service provider who, at the request of the payment service user, issues a payment order charged to the payer's payment account held with another payment service provider.

Account Information Service Provider is a payment service provider who provides a service via the internet that enables aggregated information to be presented about one or more payment accounts held by the payment service user with another or multiple payment service providers.

Payment Services User - the User refers to an entrepreneur or legal entity that uses or has used a payment service as a payer and/or payee or has approached the Bank for the use of such services.

Payer means a natural or legal person who issues a payment order charged to their payment account or gives consent for the execution of a payment transaction based on a payment order issued by the payee, or if there is no payment account – a natural or legal person who issues the payment order.

Payee means a natural or legal person designated as the recipient of the funds subject to a payment transaction.

Funds means cash, account balances, and electronic money.



Cash means banknotes and coins.

Business Day refers to a day, or part of a day, on which the Bank operates in a way that enables the execution of a payment transaction for its User as a payment services user.

Value Date is the reference date or time used by the Bank in interest calculations on funds debited or credited to the payment account.

Reference Exchange Rate is the rate used for currency conversion, made available by the Bank or derived from a publicly accessible source.

Reference Interest Rate is the rate used for interest calculation, publicly available and determined independently of the unilateral will of either the User or the Bank that concluded the contract.

Unique Identifier means a combination of letters, numbers, and/or symbols assigned by the Bank to the User and used in the payment transaction to unambiguously identify that User and/or their payment account.

Means of Remote Communication refers to any means that the User and the Bank may use to conclude an agreement when they are not physically present at the same location.

Durable Medium means any medium that enables the User to store information addressed to them, access it, and reproduce it unchanged for a period appropriate to the purpose of storing the data.

Domestic Payment Transaction refers to a payment transaction where both the payer's and the payee's payment service providers provide services within the territory of the Republic of Serbia.

International Payment Transaction refers to a payment transaction where one payment service provider provides the service within the Republic of Serbia and the other within a third country, or where the same provider renders the service for one payment services user in Serbia and for the same or another user in a third country.

Account Holder refers to the legal entity or entrepreneur that holds accounts with the Bank and conducts business via those accounts using electronic banking services.

Electronic Message means a set of data generated, sent, received, or stored electronically, optically, or through similar media.

Sender of an Electronic Message is the person who has sent the message themselves or on whose behalf the message was sent, excluding any intermediary used to transmit or receive the message on behalf of the authorized person.

Recipient of an Electronic Message is the person who received the message themselves or on whose behalf the

message was received, excluding any intermediary involved in transmitting or receiving the message on behalf of the authorized person.

Push Notification means a message delivered to an application installed on a specific device.

In-app Message means a message delivered within the electronic or mobile banking application, accessible to the User upon login to said application.

Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile network.

Authorized eBanking User is a natural person authorized by the User's legal representative through Access Documents to perform certain actions/transactions via the eBanking and/or mBanking services.

Authentication refers to a procedure that allows the payment service provider to verify the identity of the payment services user or the validity of the use of a specific payment instrument, including the use of the user's personalized security elements, and may be carried out in various ways depending on the technological solutions provided by the Bank (e.g., mPIN, biometrics, QR code).

Strong Customer Authentication means authentication using two or more elements categorized as: knowledge (something only the User knows), possession (something only the User possesses), and inherence (something the User is), which are independent of each other so that compromising one does not compromise the others, and is designed to protect the confidentiality of authentication data.

Authorization represents confirmation by the User of the intended and initiated action (e.g., confirming a payment, accepting an offer, signing contractual documentation), in accordance with the technological solutions provided by the Bank (e.g., SMS OTP code, mPIN, biometrics).

Personalized Security Elements are personalized data and features assigned by the payment service provider to the User for authentication purposes.

Sensitive Payment Data includes any data, including personalized security elements, that can be used to execute fraudulent actions. In the context of payment initiation and account information services, the account holder's name and account number are not considered sensitive payment data.

Means of Identification and Authorization Available to the User, depending on the selected application solution made available by the Bank:

- **eBanking user account** is the profile of an eBanking authorized user created in the eBanking application, which enables the user to utilize the agreed eBanking services based on the data and authorizations defined

in the Access Documentation. The user accesses their account by logging in with unique access parameters, which form part of the eBanking package in accordance with the selected application solution provided by the Bank and defined in the user manual for the selected solution.

- **mBanking user account** is the profile of an mBanking authorized user created in the mBanking application, which enables the user to utilize the agreed mBanking services based on the data and authorizations defined in the Access Documentation. The user accesses their account by logging in with unique access parameters, which form part of the mBanking package in accordance with the selected application solution provided by the Bank and defined in the user manual for the selected solution.
- **mToken, Certificate, or Smart Card** refers to a security device or application on a mobile or other electronic device used for logging into the eBanking service and/or mBanking service and for transaction authorization.
- **mToken** is an application or service within the existing application for smart devices that generates OTP passwords; OTP passwords may be displayed numerically or as a QR code.
- **Smart Card** is a security device with an integrated chip on which the electronic certificate and cryptographic keys required for the use of the eBanking system are stored.
- **Smart Card Reader** is a device that enables reading data, i.e., the use of an electronic certificate from the smart card.
- **Equipment** is a collective term for smart cards and smart card readers.
- **Security envelope with passwords or PIN mailer** is a secure letter delivered to the User, containing passwords and/or codes for accessing eBanking services.
- **PIN** is a numeric combination assigned to the User by the Bank or set by the User as a secret code required to log into the mobile banking application or to authorize payment orders and requests for the use of additional services or features within the application.
- **LIB - Activation Code** refers to a one-time password received by the Authorized User from the Bank used for activating the user account for eBanking and/or mBanking services. It can be used only once, is time-limited, and becomes invalid afterward, preventing reuse for reactivation.
- **One-Time Password (OTP)** refers to a one-time code with a time limitation, consisting of numbers and/or letters or a combination thereof (alphanumeric characters), assigned by the Bank during the activation process of eBanking and/or mBanking services and/or for transaction authorization.
- **QR Code** is a standardized two-dimensional mark, a barcode, that contains information readable by a QR code scanner.
- **Authorization using a QR Code** is a feature within the mToken service that allows the user to log into the eBanking application or authorize a payment order or another request by scanning a QR code.
- **Biometrics** refers to the use of facial or fingerprint scanning, depending on the method supported and activated on the user's device, for logging into the application or authorizing orders or other requests within the application.
 - When biometrics are used in the mobile banking application, the device's own functionality is used. Biometric data is not exchanged with the Bank, nor does the Bank have access to the user's biometric data.
- **Security question** is a predefined question that can be used within the application for additional identity verification.
- **Security answer** is the answer to the security question, defined by the User and usable in the application for additional identity verification.
- **Qualified electronic certificate** is an electronic certificate issued by a qualified certification authority.
- **Digitalized payment card** refers to a payment card issued by the Bank that has been digitalized within electronic banking and/or mobile banking and/or other applications that provide such functionality. A digitalized payment card can be used at points of sale equipped with contactless POS terminals for processing card transactions. The Bank determines the types and categories of payment cards that can be digitalized based on their characteristics.
- **Request for activation of electronic/mobile banking** refers to a document submitted by a User who does not already have a contracted digital banking service for legal entities and entrepreneurs, requesting access to electronic and mobile banking services.
- **Request for data changes** refers to a form or a set of actions initiated to update the data of the User or the Authorized Users. The User is obligated to complete

and submit such a request to the Bank.

In accordance with further technological developments of its solutions, the Bank may enable the User to use additional or modified means of identification, authorization, or signing, as defined in the user manual for the selected application solution.

3. Conditions for the Provision of Payment Services **Basic conditions under which the Bank provides payment services**

The Bank provides payment services in accordance with the provisions of the Law governing domestic payment transactions executed in dinars, as well as international payment transactions regardless of the currency used.

The mutual rights and obligations of the Bank and the User regarding the provision of payment and other services related to the payment account are governed by the Agreement, the Special Terms and Conditions for Payment Accounts and Payment Services for Legal Entities and Entrepreneurs, and the General Terms and Conditions.

3.1. Electronic Banking

Definition of electronic banking services

Electronic banking services include the performance of transactions via electronic means and refer to all electronic products and services of the Bank used by the User in accordance with the user manual relating to the application solution made available by the Bank.

Transactions include payment transactions and other business transactions, including the ability to submit requests for certain services of the Bank.

Electronic banking also entails regulating the mutual rights, obligations, and responsibilities between the Bank and the User in the use of electronic banking services, i.e. it represents the electronic exchange of information, as well as the management of funds and account operations of the User with the Bank through electronic banking, in accordance with the access documentation for users of eBanking services.

The Bank offers the possibility of opening an eBanking account by signing an eServices Agreement.

By activating this service and depending on the selected application solution, the Bank offers the following electronic banking services:

- Account balance and transaction overview
- Transfer of funds and payment transactions in domestic payment operations
- Transfer of funds and payment transactions in international payment operations

- Allocation of foreign inflows

When completing the request form, the User selects one of four authorization levels:

- View only
- View and payment
- View and order initiation (without the right to authorize orders)
- View and order authorization (without the right to initiate orders)

With further development of electronic services, the Bank may introduce additional services, which the User will be informed about via the application itself, as well as through other agreed communication channels: SMS, email, Viber, or push notifications (if technically possible), etc.

3.2. Mobile Banking

Definition of mobile banking services

Through mobile banking, the Bank provides the mBanking application, which enables the execution of transactions via a mobile device, without the need to visit the Bank.

Mobile banking also entails regulating the mutual rights, obligations, and responsibilities between the Bank and the User in the use of mobile banking services, i.e. it represents the electronic exchange of information, as well as the management of funds and account operations of the User with the Bank through mobile banking, in accordance with the access documentation for users of mBanking services.

By activating this service and depending on the selected application solution, the Bank offers the following mobile banking services:

- Account balance and transaction overview
- Transfer of funds and payment transactions in domestic payment operations
- Transfer of funds and payment transactions in international payment operations

When completing the request form, the User selects one of the following four authorization levels:

- View only
- View and payment
- View and order initiation (without the right to authorize orders)
- View and order authorization (without the right to initiate orders)

With further development of mobile services, the Bank may introduce additional services, which the User will be informed

about via the application itself, as well as through other agreed communication channels: SMS, email, Viber messages, etc.

3. Conditions for Using Payment Services via Electronic Channels

3.1.1. Conditions Under Which the Bank Provides Electronic and Mobile Banking Services

By concluding the Agreement, the User acquires the right to use one of the electronic services from the Bank's current offering for the purpose of utilizing individual or all of the Bank's services, specifically:

- E-banking
- M-banking

The User is obligated to independently and at their own expense provide the minimum technical requirements for using the above services, as defined in the User Manual.

User manuals for each individual service are available to the User on the official website of the Bank, explaining how to use each service (hereinafter: User Manuals), including installation procedures. By signing the Agreement and/or another appropriate document (hereinafter: Agreement), the User defines the type and level of Services they will use.

The User (a legal entity or entrepreneur) shall inform the Bank of the access type and authorizations for the authorized user or rights holder. The User confirms that every action or omission of the authorized user or rights holder is valid and binding for the User and accepts responsibility for any consequences arising from their actions.

The User may access individual or all services after concluding the Agreement with the Bank, i.e., after the service is activated by the Bank. The User will be notified of new functionalities via the application in use or through other agreed communication channels.

The services will be available to the User from the moment of activation, 24 hours a day, seven days a week, to the extent and in the manner defined in the Agreement and User Manual published on the Bank's website.

The Bank bears no responsibility in cases where the User is unable to use the Service due to telecommunications issues or other circumstances beyond the Bank's control. Services are accessible through the following channels:

1. Internet
2. SMS messages
3. Email
4. Mobile device

For each service, the Bank will provide the User with access to information and the ability to conduct transactions, in

accordance with the following:

The Bank shall provide the Client – the payer – before and after executing each individual payment transaction, with the following information:

1. Before executing an individual payment transaction initiated by the Client – payer – under the framework agreement, the Bank must provide the payer, upon request, with precise information on the execution time of the payment transaction and the fees to be charged. If the fees are charged as a lump sum – then a breakdown of each fee comprising the total must be provided.
2. When executing a payment transaction under the framework agreement, the Bank must, immediately after debiting the payer's account or upon receipt of the payment order if the payer does not use a payment account, deliver the following information on paper or another durable medium:
 - A reference identifier or other information enabling the payer to identify the individual transaction and related details of the payee;
 - The transaction amount in the currency in which the payer's account is debited or the currency indicated in the payment order;
 - Any fee charged to the payer for executing the transaction. If fees are charged as a lump sum – a breakdown of each component of the fee must be provided;
 - Any interest paid by the payer, if applicable;
 - If currency conversion was performed – the exchange rate used and the transaction amount after the conversion;
 - The value date of the debit or the date of receipt of the payment order.
3. The framework agreement may stipulate that the Bank will periodically provide the information referred to in point 2 above, at least once per month, using a method agreed with the payer that enables storage and unaltered reproduction of the information.
4. The Bank is obliged, upon request, to provide consumers (natural persons using services for personal or non-commercial purposes) with a free monthly paper statement containing the information referred to in point 2 above.

The User is deemed to have consented, by registering their phone number, mobile number and/or email address with the Bank, that the Bank may identify them via WAP protocol, SMS and/or email messages and other available methods and thus



provide access to data about accounts, credit and debit cards, and other products and services used at the Bank, in the manner and scope defined in the User Manual. The User must treat all passwords used to access services as confidential.

Payment orders submitted via any of the services will be executed in accordance with applicable regulations and this Annex.

Telephone calls related to service use may be recorded and used as proof of instructions and executed transactions. Such voice recordings may be used solely for the resolution of User complaints and legal disputes.

To increase the security of electronic transactions, the Bank may provide the User with a security device or security letter, to be used for one or more services. The User must use the device or letter in accordance with the User Manual and protect it from damage and unauthorized use.

The Bank and the User agree that the validity or evidentiary value of electronic documents and electronic messages cannot be challenged solely because they are in electronic form, and that an electronic signature that can be verified through an electronic certificate, and/or ePin, mTOKEN, OTP via SMS message, qualified certificate, produces legal effects equivalent to a handwritten signature, in accordance with applicable laws.

The Bank and the User further agree that an electronic signature:

1. Is uniquely linked to the signatory of the electronic message;
2. Provides sufficient information to identify the signatory of the message;
3. Is generated using tools under the sole control of the signatory;
4. Is linked to the electronic message such that any subsequent change can be detected.

The Bank and the User further agree that an electronic message is considered to have been sent by the sender if:

- The sender personally sent the message; or
- The message was sent by a person authorized to act on behalf of the sender regarding that message.

An electronic message is considered to have been received by the recipient if:

- The recipient personally received the message; or
- The message was received by a person authorized to act on behalf of the recipient regarding that message.

3.1.2. Unique Identifier

Upon concluding the Agreement, the Bank issues the User a unique identifier (account or card number), which the User is obliged to specify for the proper issuance or execution of a payment order and which serves to identify the account and payment card holder (e.g., account or card number).

By accurately specifying the unique identifier (account number) of the payee in the payment order, it is considered that the payment order has been correctly executed in relation to the payee.

The Bank is not liable for any non-executed or incorrectly executed payment transaction if the User submits a payment order with an incorrect unique identifier (account number) of the payee.

In such cases, upon the User's request, the Bank is obliged to immediately take all reasonable measures and provide the User with all necessary information to exercise the right to a refund of funds (e.g., about the payee's payment service provider and/or the payee), including information that the payee's payment service provider is required to provide the Bank in accordance with this provision.

In case of a non-executed payment transaction due to an incorrect unique identifier (account number), the Bank is obliged to immediately refund the amount of the non-executed transaction to the User upon learning of it.

The User may not use the services for unlawful purposes, including purchasing goods or services prohibited by law. Any unlawful use, as well as the purchase of goods and/or services prohibited by law (e.g., pornography, prostitution, drug trafficking, and other illegal activities), is punishable and results in termination of the right to use the service.

By assigning unique secret elements—such as PINs for identification, one-time OTP passwords, user certificates, access passwords, security questions and answers, and other identification and authorization tools made available by the Bank depending on the selected application solution—the User is enabled to access the services. The User assumes responsibility for keeping the aforementioned secret security elements confidential, for distributing them to persons deemed appropriate by the User, and for covering any costs incurred through their use.

If the User has not secured a Smart Card reader, they may request one from the Bank, which will charge a fee for issuing the Smart Card reader in accordance with the applicable Price List.

3.1.3. Form and Manner of Giving and Withdrawing Consent for Issuing a Payment Order or Executing Payment Transactions

The User may dispose of funds in all accounts opened under an Agreement on the opening and maintenance of payment



accounts concluded with the Bank, for which the use of specific services is provided.

The Bank will execute the User's electronic payment order requesting the execution of a transfer of funds if the following conditions are met:

1. The order is submitted via electronic services in accordance with the Agreement, the General Terms and Conditions, and this Annex;
2. The User has secured sufficient funds for the execution of the order, including any fees charged in accordance with the Bank's Price List;
3. The User has given consent for the execution of the payment order (meeting the conditions above in accordance with the steps defined in the User Manual); The User may give consent through the payee or a payment initiation service provider;
4. There are no legal obstacles to execution (under other applicable regulations).

When specific documents or data are required for executing the payment order under special regulations, the Bank will execute the payment order if those documents or data are submitted or presented in the prescribed format.

Consent may be withdrawn by submitting a statement of withdrawal of consent for the execution of a payment transaction or a series of payment transactions (via the communication channel selected in the Request or within the application itself), or by contacting the Bank's Contact Center, provided the Bank has not already received the payment order.

The Bank may reject a payment order if the conditions under this Article are not met, or when required by regulations, or when there is reasonable doubt regarding the authenticity of the payment order or any of its elements.

A bank holding the User's account may not reject a payment order if all the conditions stipulated in the payment services agreement are met, except in the cases mentioned above.

The Bank will inform the User of the rejection of a payment order in dinars (via the application itself, orally, by telephone, or by another agreed method), including reasons for the rejection, where possible, and instructions for correcting the deficiency that caused the rejection, within the same business day the payment order was submitted—unless such notification is prohibited by law.

Exceptionally, the deadline for informing the User of the rejection of a payment order in a foreign currency is determined by law or another regulation.

In cases where an electronic payment transaction was not executed—and especially where relevant regulations do not prohibit it or where technically possible—the Bank may allow

the User to submit a request to cancel a payment transaction for which they had previously provided consent, via the electronic or mobile banking application, in accordance with the User Manual made available by the Bank.

However, a cancellation request cannot be submitted for instant credit transfers.

If technically possible (e.g., if the transaction has not yet been executed or for other technical reasons), the Bank will cancel the electronic payment transaction upon receiving such a request.

The User is obliged to monitor the status of the submitted cancellation request via the selected electronic or mobile banking application.

3.1.4. Time of Receipt of Payment Order and Deadlines for Execution of Payment Services or Individual Transactions

The time of receipt of a payment order and the deadlines for the execution of payment transactions are further regulated by the Transactions Schedule.

The User's payment account may not be debited before the payment order is received.

3.1.5. Rights, Obligations, and Responsibilities of the User

The User undertakes to:

1. Acquire, maintain, and use appropriate computer and communication equipment, a mobile device, or other necessary equipment at their own expense for the use of specific or all Bank services, in accordance with the technical requirements defined in the User Manual;
2. Protect the computer equipment and software used to access Bank services and use them solely in the manner intended for each individual Bank service;
3. Safeguard the equipment, usernames, passwords, codes, PINs, and other identifiers, protecting them from theft, loss, damage, or misuse, and will not write them down or disclose them to third parties;
4. Return the equipment provided by the Bank in good condition upon the Bank's request;
5. Carry out all operations via the Bank's services in accordance with the Agreement, this Annex, the General Terms and Conditions, and other applicable regulations;
6. Immediately notify the Bank of the loss, theft, misuse, or unauthorized use of the Equipment and/or mobile device or suspected unauthorized use of the Bank's services, and immediately submit a request to the Bank to disable (block) the use thereof;

7. Inform the Bank of any changes to information necessary for uninterrupted and secure service use, such as phone numbers, mobile numbers, or email addresses used to access certain services;
8. Notify the Bank in writing of any changes to the legal entity's registration details, legal representative authorizations, legal status, or other modifications, providing appropriate supporting documents from the Serbian Business Registers Agency (APR);
9. Monitor the outcome of financial transactions performed via E-banking and M-banking services by checking the status of submitted payment orders. The User bears full responsibility for verifying and signing completed payment orders, given that electronically signed transactions are executed automatically;
10. Use electronic and mobile banking services in all relations established based on concluded agreements (e.g., account opening with the Bank), for which electronic and mobile banking services are provided. The Bank shall enable the User to use specific E-banking and M-banking services also in relation to newly concluded agreements, provided that technical and/or functional requirements are met.

3.1.6. Limit

The Bank may prescribe limits for transactions performed via electronic and mobile banking, which will be published on the Bank's website and in the Bank's branches, in the document titled "Limits for the Use of Payment Instruments," as well as within the electronic banking and mobile banking applications.

The User may define or amend usage limits at any time by submitting a request, provided that technical conditions allow it.

The Bank reserves the right to change the amount of the limit, of which the User will be notified in advance.

3.1.7. Rights and Obligations of the Bank

The Bank undertakes to provide the User with all necessary elements for accessing and using the Bank's services during the Bank's business hours for specific payment services, except in cases of force majeure, technical difficulties, or other unforeseen events.

The Bank is liable to the User for direct damage caused intentionally or through negligence by the Bank.

The Bank is not liable for damages caused by force majeure, war, unrest, terrorist acts, natural or ecological disasters, epidemics, strikes, power outages, disruptions in telecommunication and other networks, transmission errors in telecommunication systems, decisions and actions of authorities, or any similar causes not attributable to the Bank, which prevent access to services.

The Bank is not liable for the loss or destruction of data on the User's equipment used to access services.

The Bank is not responsible for consequences arising from unauthorized or improper use of the equipment by the User, nor for telecommunication or transmission services provided by third parties, or for any disruptions or malfunctions of services beyond the Bank's control.

The Bank may temporarily suspend the agreed services in case of necessary system upgrades, repairs, or maintenance of its infrastructure, in which case the Bank will notify the User at least two (2) business days in advance, except in urgent cases or when security reasons prevent such notice.

The Bank reserves the right to modify, upgrade, and adapt its current system and security protocols.

The Bank does not guarantee nor assume responsibility for hardware and software not part of the eBanking/mBanking system.

4. Information and Data on Fees and Currency Exchange Rates

4.1.1. Type and Amount of Fees Charged by the Bank to the User

The type and amount of fees for services provided by the Bank to Users—including those related to the manner and frequency of delivering or making available information in accordance with the Law—are defined in the Framework Agreement with the User, in accordance with the applicable Bank Price List.

By agreeing to individual or all services, the User consents to and authorizes the Bank to charge the account for the agreed service fee immediately upon activation, in accordance with the current Price List.

If there are insufficient funds in the account to cover the service fee, the User will not be able to use the service until there are sufficient funds to cover the activation fee for the agreed service.

The User agrees and irrevocably authorizes the Bank, without further consent or approval, to collect all due and unpaid fees related to the use of specific or all agreed services in accordance with the Price List by debiting all accounts the User holds with the Bank, unless legal restrictions prevent execution.

In case of insufficient funds in the currency of the Bank's claim, the User agrees that the Bank may convert funds from other currencies available in the User's accounts and use them to settle the Bank's receivables.

The Bank reserves the right to modify fee amounts or introduce new fees, of which it will notify the User.

Changes in interest rates and currency exchange rates may be applied immediately and without prior notice to the User if

based on changes to the agreed reference interest rate or reference exchange rate. The Bank will notify the User in writing of changes to the interest rate without delay, either on paper or on another durable medium.

For services enabling the execution of payment transactions by means of payment orders for transfers from the payer's account to the payee's payment account, the Bank charges a fee for each such individual payment transaction in accordance with the Price List.

4.1.2. Currency Exchange Rate – Payment Transaction Currency

A payment transaction shall be executed in the currency agreed upon between the payment service user and their payment service provider, in accordance with regulations governing foreign exchange operations.

The Bank shall execute a payment order in the currency indicated on the payment order.

Execution of a payment order may require the purchase and/or sale of domestic or foreign currencies (currency conversion); for such transactions, the Bank shall use the buying/selling exchange rate from the Bank's daily **Exchange Rate List** for foreign currencies.

For conversion from the domestic currency to a foreign currency (purchase of foreign currency), the Bank shall apply the **selling rate** for foreign currencies, while for conversion from a foreign currency to the domestic currency (sale of foreign currency), the **buying rate** shall be applied.

The Bank's **Exchange Rate List** is available at the Bank's branches and on its website, with the possibility that the Bank may apply a more favourable exchange rate mutually agreed upon with the User (verbally or via email).

Currency conversion cannot be executed without the User's consent.

5. Information on the Methods and Means of Communication Between the User and the Bank

All communication between the Bank and the User related to the rights and obligations under the Agreement shall be conducted in the Serbian language.

This does not exclude the use of other languages at the User's request, subject to the Bank's capabilities and in accordance with good banking practices.

Means of communication between the User and the Bank, depending on the type of communication, may include:

- **Verbal communication** – by visiting a branch or calling the Bank's Contact Center
- **Written communication** – notifications, letters, and other correspondence

- **Electronic communication** – via the Bank's website, chat, email, digital banking applications (electronic and mobile banking), and features within those applications depending on technical capabilities (e.g., in-app messages, push notifications); use of apps and social media such as Viber, WhatsApp, Facebook, etc.; sending SMS messages or using applications that enable individual communication with the User, as well as other app-based solutions made available by the Bank according to technical possibilities.

Information and notifications shall be delivered via the agreed communication channel. All relevant data related to the execution of payment transactions, as well as contact addresses for communication with the Bank, can be found on the Bank's website.

The User has the right to receive one copy of the Agreement in written form or on another **durable medium**, as well as the right to request, during the contractual relationship, a copy of the agreement or pre-contractual information in the form of a draft agreement, in a manner that allows the User to become acquainted with the conditions related to the provision of payment services and compare offers from different payment service providers and assess whether these conditions and services meet their needs.

At the User's request, the Bank is obliged, prior to executing an individual payment transaction initiated under the Agreement, to provide accurate information about the execution time of that payment transaction and the fees to be charged. If the Bank charges these fees as a lump sum, it must also disclose the type and amount of each individual fee included in the total fee.

6. Information on Protective and Other Measures Related to the Execution of Payment Transactions

6.1.1. Procedure in Case of Loss, Theft, or Misuse of the Payment Instrument

The User is obliged to use the payment instrument in accordance with the prescribed or agreed conditions governing the issuance and use of that instrument, including the details outlined in the user manual.

The User is especially obliged, immediately upon receiving the payment instrument, to take all reasonable and appropriate measures to protect the personalized security elements of that instrument (e.g. a security envelope).

The User must immediately notify the Bank or a designated representative of the Bank after becoming aware of the loss, theft, or misuse of the payment instrument or the unauthorized use of equipment and/or mobile device or any suspicion of unauthorized use of the Bank's services. The User must treat the mobile device used together with the mobile/electronic banking application, which constitutes a payment instrument, with due care to prevent loss, theft, and misuse. The User must

notify the Bank without delay after discovering the loss, theft, or any misuse of the mobile or other device or any related data.

In such cases, the User must immediately contact the Bank's Contact Center or notify the Bank through another agreed or available communication channel and request the blocking of the services. If the report is made via telephone, it is electronically registered, and the Bank is obliged to block further use of the services.

Any material damage resulting from the loss, theft, or misuse of the payment instrument or unauthorized use of the equipment and/or mobile device or suspected unauthorized use of the Bank's services, until the moment of reporting the loss, theft, or misuse, shall be borne by the User. If the User finds the payment instrument after having reported its loss, theft, or misuse, they must not use it but must return it to the Bank without delay.

If the Bank does not allow reporting of loss, theft, or unauthorized transaction at any time—or misuse of the payment instrument, or data from it, or unauthorized use of equipment and/or mobile device, or suspicion thereof—the User will not bear the consequences of unauthorized use, unless the misuse was committed by the User.

6.1.2. Blocking and Suspension of Services

At the User's request, the Bank may block the use of services, either partially or in full.

The Bank also reserves the right to block the use of services, in whole or in part, without the User's consent in the following cases:

- if it suspects that the User or a third party is abusing the services;
- if the User fails to comply with contractual provisions;
- if the User fails to use the service within the time period defined in Article 6.1.3.

The suspension of services may also be requested by the User, either in writing at any of the Bank's branches or in another manner provided for in the user manual for each individual service.

The Bank may disable the use of the payment instrument if there are justified reasons related to the security of the payment instrument, suspicion of unauthorized use or fraud, or if there is an increased risk that the User will be unable to fulfil their payment obligations, especially when the use of the payment instrument is linked to a credit arrangement or an authorized account overdraft.

The Bank is required to notify the User of its intention and reasons for blocking the payment instrument—before the blocking, or no later than immediately after the blocking—via telephone, in writing, through the app, or via another agreed

communication channel.

The Bank will re-enable the use of the payment instrument or replace it with a new one once the reasons for its blocking cease to exist.

6.1.3. Suspension of Service – Deactivation of the User Account Due to Inactivity for More than 3 Months

In accordance with the above Article, the Bank has the right to deactivate or permanently delete a user account that has been inactive for more than 3 months (i.e. the User has not logged into the application for at least 3 months) without the User's consent. This measure aims to avoid potential costs arising from the activation or opening of user accounts, which may affect the price of the service the Bank provides to the User.

The User has the right to reactivate the account or continue using electronic and mobile banking services in accordance with the user manuals made available by the Bank.

6.1.4. Payment Transactions Where the Transaction Amount is Not Known in Advance

If a payment transaction initiated using a payment card is initiated by or through the payee, and the exact amount of the transaction is not known at the moment the User gives consent for the execution of the payment transaction, the payer's payment service provider may not reserve funds in the payer's payment account unless the payer has given consent for a specific amount of funds that may be reserved.

The Bank is obliged to release the reservation of funds in the User's payment account without delay after receiving the information about the exact amount of the payment transaction, and no later than immediately after receiving the payment order.

6.1.5. Liability of the Bank and the User for Initiating Payment Transactions or for Unexecuted, Improperly Executed, or Unauthorized Payment Transactions

In the case of an unauthorized, unexecuted, or improperly executed payment transaction, without prejudice to the obligations of the Bank and the User as outlined in Articles 3.1.2., 6.1.6, and 6.1.7 of these Special Conditions, the Bank is obliged, regardless of its responsibility for the correct execution of the payment transaction, to immediately take appropriate measures upon the User's request to trace the flow of funds from the payment transaction and provide the User with information about the outcome without delay.

The Bank may not charge the payer a fee for the actions described in paragraph 1 of this Article.

The User of payment services has the right, in accordance with the Law, to request compensation from the Bank or the payment initiation service provider, if the transaction was initiated through the latter, for any damage resulting from the



execution of an unauthorized payment transaction or the failure to execute or the improper execution or delay in the execution of a payment transaction for which the Bank is responsible.

If the User claims that they did not authorize a payment transaction or that the payment transaction was not executed or was improperly executed, and if the Bank claims otherwise, it is obliged to prove that the payment transaction was authenticated, properly recorded, and booked, and that its execution was not affected by any technical failure or other deficiency in the services it provides.

If the payment transaction was initiated via a payment initiation service provider, that provider is obliged to prove that the transaction was authenticated and properly recorded in the part of the service it provides, and that its execution was not affected by any technical failure or other deficiency in the service it was responsible for.

A payment transaction is considered authenticated, in terms of this Article, if the Bank has applied appropriate procedures to verify and confirm the use of the specific payment instrument, including its personalized security elements.

If the payer claims not to have authorized the payment transaction executed using the payment instrument or initiated via a payment initiation service provider, the records kept by the payment service provider regarding the use of the payment instrument or the initiation of the transaction are not by themselves sufficient evidence that the transaction was authorized by the payer, nor that the payer acted fraudulently or with intent or gross negligence.

In such cases, the Bank and the payment initiation service provider must provide evidence to reasonably support that the User acted fraudulently or failed to meet their obligations related to the payment instrument and its personalized security elements either intentionally or with gross negligence.

6.1.6. Liability of the User for Unauthorized Payment Transactions

The User shall bear the losses resulting from the execution of unauthorized payment transactions up to the amount of 3,000 dinars if those transactions were carried out due to the use of:

1. a lost or stolen payment instrument, or
2. a payment instrument that has been misused.

Notwithstanding the first paragraph of this Article, the User shall bear all losses resulting from unauthorized payment transactions if such transactions were carried out as a result of the User's fraudulent actions or failure to meet the obligations set forth in Article 6.1.1 of these Special Conditions due to intent or gross negligence.

The User shall not bear losses under this Article in the following cases:

1. if the User could not have detected the loss, theft, or misuse of the payment instrument before the unauthorized payment transaction occurred, except in cases covered by paragraph 2 of this Article;
2. if the unauthorized transaction was the result of an action or omission of an employee, agent, or branch of the payment service provider, or another entity to whom the payment service provider has outsourced activities, except in cases covered by paragraph 2 of this Article;
3. if the Bank did not enable the User to report the loss, theft, or misuse of the payment instrument at any time and free of charge, except where the loss was caused by fraudulent actions of the User;
4. if the Bank did not require strong customer authentication, except where the loss was caused by fraudulent actions of the User.

If the Bank requires strong customer authentication and the payee or the payee's payment service provider fails to apply such authentication, the payee or their provider shall compensate the Bank for the damage suffered as a result.

The User shall not bear losses resulting from unauthorized payment transactions executed after the User notified the Bank of the loss, theft, or misuse of the payment instrument, except where such losses were caused by the User's fraudulent actions.

By way of exception to paragraph 1 of this Article, the National Bank of Serbia may prescribe that the User shall bear losses arising from the execution of unauthorized payment transactions up to an amount lower than 3,000 dinars, particularly considering the nature of the personalized security features of the payment instrument and the circumstances under which the payment instrument was lost, stolen, or misused.

6.1.7. Bank's Liability for Unauthorized Payment Transactions

The Bank is liable for the execution of a payment transaction for which the User has not given consent (hereinafter: unauthorized payment transaction).

In the event of the execution of an unauthorized payment transaction, the Bank shall, immediately upon becoming aware of it, and no later than the next business day after it discovered or was notified of the transaction, reimburse the amount of that transaction to the User—unless the Bank suspects fraud or abuse by the User, in which case the Bank must, within ten (10) days of becoming aware of the unauthorized transaction, take one of the following actions:

1. Provide the User with an explanation for the refusal of reimbursement and report the fraud or abuse to the competent authority; or



2. Reimburse the amount of the transaction to the User if, after additional verification, the Bank concludes that the User did not commit fraud or abuse.

The Bank is obliged to restore the User's payment account to the state in which it would have been had the unauthorized payment transaction not occurred, ensuring that the value date for the crediting of the User's account is no later than the date on which the account was debited for the unauthorized payment transaction.

The Bank is also obliged to refund all fees it charged the User and pay all interest to which the User would have been entitled had the unauthorized transaction not been executed.

If the payment transaction was initiated through a payment initiation service provider, the provisions of this Article shall apply to the Bank as the account servicing payment service provider.

6.1.8. Liability for Unexecuted or Improperly Executed Payment Transactions or Delay in Execution of Payment Transactions Initiated by the User (Payer)

If the payment transaction was initiated directly by the User, the Bank shall be liable to the User for its proper execution up to the payment service provider of the payee.

If the Bank is responsible for the unexecuted or improperly executed payment transaction, it is obliged, immediately upon becoming aware of it, to reimburse the amount of the unexecuted or improperly executed payment transaction to the User or restore the User's payment account to the state it would have been in had the improper transaction not occurred, unless the User requests correct execution of the payment transaction.

In the case described in paragraph 2 of this Article, the Bank must ensure that the value date for the crediting of the User's payment account relating to the improperly executed payment transaction is no later than the date on which the User's account was debited for the transaction.

If the Bank provides the User—and if necessary, the payee's payment service provider—with evidence that the account of the payee's provider was credited with the transaction amount, the payee's payment service provider shall be liable to the payee for the unexecuted or improperly executed payment transaction.

The payee's payment service provider is required to ensure that the value date for the crediting of the payee's account is no later than the business day on which the funds from the transaction would have been credited had the transaction been correctly executed.

If the payment transaction was executed after the deadline prescribed by law, the payee's payment service provider is required—upon the Bank's request acting on behalf of the User—to ensure that the value date for the crediting is no later

than the business day on which the funds would have been credited had the transaction been executed properly in accordance with the law and these Special Conditions.

If the Bank is liable for the unexecuted or improperly executed payment transaction or a delay in execution, it is obliged to refund the User all fees it charged and pay any interest to which the User is entitled in relation to the unexecuted or improperly executed transaction.

If the payment transaction was initiated by the User through a payment initiation service provider, the User's payment service provider for the purposes of paragraphs 1 to 4 and paragraph 6 of this Article shall be considered the Bank.

In the case of such a payment transaction, the payment initiation service provider must prove that the Bank received the payment order in accordance with Article 3.1.4 of these Special Conditions and that, in the part of the service it provided, the payment transaction was authenticated and properly recorded, and that no technical failure or other deficiency affected its execution. The provider must supply such evidence without delay upon the Bank's request.

6.1.9. Liability for Unexecuted or Improperly Executed Payment Transactions or Delay in Execution of a Payment Transaction Initiated by the Payee or by the User (Payer) via the Payee

If the payment transaction was initiated by the payee or by the User through the payee, the payee's payment service provider shall be liable to the payee for correctly delivering the payment order to the Bank as the User's payment service provider.

If the payment service provider of the payee failed to deliver, or improperly delivered, the payment order in the case referred to in paragraph 1 of this Article, it shall immediately deliver or re-deliver such order to the Bank upon becoming aware of the omission.

If the payment order was delivered to the Bank after the deadline agreed between the payee and their payment service provider or the Bank, the payee's payment service provider must ensure that the value date for crediting the payee's account is no later than the date on which the account would have been credited had the payment transaction been executed on time.

If the amount of a payment transaction initiated by the payee or by the payer through the payee has been credited to the account of the payee's payment service provider, that provider shall be liable to the payee for the proper execution of the payment transaction.

If the payee's payment service provider is liable in accordance with paragraph 4 of this Article, it shall ensure that the value date for the crediting of the payee's account is no later than the date on which the account would have been credited had the transaction been correctly executed.

If the payee's payment service provider provides proof to the payee, and if necessary to the Bank, that it is not liable in accordance with paragraphs 1 through 4 of this Article, the Bank, i.e. the payer's payment service provider, shall be liable to the User for the unexecuted or improperly executed payment transaction.

In such cases, the Bank's liability under paragraph 6 shall be governed by Article 6.1.8, paragraphs 2 and 3 of this Annex.

The Bank shall not be liable in accordance with the preceding paragraph if it proves that the payee's payment service provider received the amount of the transaction but there was a minor delay in execution. In that case, the payee's provider must ensure that the amount is credited to the payee's account with a value date no later than the date the transaction should have been completed had it been correctly executed.

A payment service provider liable under this Article must reimburse its payment service user for all fees charged, and refund or pay any interest to which the user is entitled in connection with the unexecuted or improperly executed payment transaction.

6.1.10. Notification or Request as a Condition for Reimbursement or Proper Execution of a Payment Transaction

The Bank shall provide the User with reimbursement or proper execution of a payment transaction if the User notifies the Bank of an unauthorized, unexecuted, or improperly executed transaction, or requests proper execution of the payment transaction, immediately upon becoming aware of it, provided the notification or request is submitted no later than 13 months from the date of the debit.

If the Bank did not provide the User with information about the transaction, it shall be liable for the unauthorized, unexecuted, or improperly executed payment transaction and must reimburse the amount even after the 13-month deadline, provided that the User notified the Bank immediately upon becoming aware of the transaction.

If a payment initiation service provider was involved in the execution of the payment transaction referred to in paragraph 1 of this Article, the User shall submit the reimbursement request to the Bank that maintains the User's account.

6.1.11. Rights and Obligations of Payment Service Providers in Cases of Fraud or Abuse and in Certain Improperly Executed Payment Transactions

If the Bank submits a request for the return of funds along with data, information, and documentation indicating that the transaction was likely the result of fraud or abuse, the payee's payment service provider shall not credit the funds to the payee's account or shall prevent the payee from accessing those funds for a period of three business days from receipt of

such data, information, and documentation.

If during the period mentioned in the previous paragraph, the payee's payment service provider receives from the Bank additional information, including a report to the competent authority, which together strongly indicates that the transaction was fraudulent or abusive, the payee's provider must:

1. Reimburse the funds to the User without delay if the payee fails to prove or make probable the origin of the funds within 15 business days of being notified of the submitted data, information, documentation, and report; or
2. Allow the payee access to the funds after 30 business days from the expiration of the initial period if the payee proves or makes probable the origin of the funds, and if the competent authority has not issued a decision prohibiting the use of those funds.

The payee's payment service provider shall be liable to the payer for losses arising from such transactions if it allowed the payee to access the funds contrary to the provisions of paragraphs 1 and 2, and it is established in the appropriate proceeding that the payee committed fraud or abuse, or participated in the fraud or abuse.

6.1.11. The Bank's Rights and Obligations in Cases of Improper Execution of Domestic Payment Transactions

1. **Overpayment or Multiple Payment Orders:**
 - If the payer's payment service provider transfers an amount that exceeds the amount stated in the payment order, or if it erroneously executes the payment order multiple times, the payee's payment service provider, based on evidence from the payer's provider who made the error, must immediately return the excess funds to the payer's provider.
2. **Underpayment:**
 - If a lower amount is transferred to the payee's provider than the amount stated in the payment order, the payer's provider may transfer the difference to the payee's provider on the same business day without a request from the payment service user for the correct execution of the payment transaction.
3. **Wrong Recipient:**
 - If the funds are transferred to an incorrect payee (other than the one specified in the payment order), the payer's provider may, on the same business day when the order is received, correctly execute the payment

transaction and return the funds without a request from the payment service user for correction. The payee's provider must return the funds to the payer's provider based on evidence that the wrong transaction was made.

The return of funds in cases of overpayment, underpayment, or erroneous transfers takes precedence over other payment transactions from the account that received the funds.

6.1.12. Reimbursement of Approved and Properly Executed Payment Transactions to the User

The Bank shall reimburse the User, at their request, the full amount of an approved and properly executed payment transaction (hereinafter: Request for Reimbursement), initiated by the payee or the User via the payee, provided the following conditions are met:

1. The User gave consent for the execution of the payment transaction without a specified exact amount for the transaction.
2. The amount of the payment transaction is higher than what the User could reasonably have expected, considering the amounts of their previous payment transactions, the terms outlined in the Framework Agreement, and the specific circumstances of the case.

The Bank may require the User to provide evidence of the facts related to the fulfilment of the conditions mentioned above. The User cannot claim that the amount of the payment transaction was higher than expected if the higher amount resulted from currency exchange at the reference exchange rate.

The User will not have the right to request reimbursement if the following conditions are met:

1. The User directly provided consent to the Bank for the execution of the payment transaction.
2. The Bank or the payee provided the User with information about the future payment transaction at least 28 days before the due date.

The User can submit a Request for Reimbursement within 56 days from the date of debit, and the Bank must reimburse the full amount of the payment transaction or notify the User of the reasons for the denial within ten business days from the date of receiving the request. The value date of the approval of the User's account may be no later than the date the account was debited for the payment transaction in this case.

If the Bank reimburses the disputed amount to the User, and the card organization's complaint procedure determines that the complaint was unfounded, the Bank will charge the User's account for the amount of the unjustly refunded funds without

additional consent.

If the request for reimbursement is denied, the Bank must inform the User in the notice of the reasons for the denial about:

1. The process for protecting the User's rights and interests, including out-of-court resolution of disputes.
2. The procedures that can be initiated due to violations of the law.
3. The authority responsible for conducting these proceedings.

In the case of a direct debit initiated for a domestic payment transaction in the RSD or a payment transaction within the Single Euro Payments Area (SEPA) in euros, the User has the right to request reimbursement even if the conditions outlined in paragraph 1 of this Article are not met.

7. Execution of Payment Transactions Based on Bills of Exchange

A payment transaction based on a bill of exchange is a payment transaction in which the payee initiates a transaction to debit the User's payment account based on a bill of exchange and a payment order requesting the transfer of funds from the User's account to the payee's account.

The bill of exchange referred to in the first paragraph, including an electronic bill of exchange, is issued in accordance with the law governing bills of exchange and represents the irrevocable consent of the issuer of the bill of exchange to their payment service provider to execute the payment transaction initiated by the holder of the bill of exchange in accordance with this paragraph.

If the bill of exchange referred to in the first paragraph is registered in the bill of exchange and authorization register maintained by the National Bank of Serbia, the payee may initiate a payment transaction to debit the payer's current account with any payment service provider that maintains such an account in accordance with the regulations governing forced collection on funds in the account.

8. Authentication

The Bank is obligated to apply reliable authentication of the User in cases where the User:

1. Accesses the payment account via the internet;
2. Initiates an electronic payment transaction;
3. Uses any remote communication tool to perform activities that may involve the risk of fraud or misuse in relation to executing a payment transaction.

If the payer initiates an electronic payment transaction as mentioned in point 2 of paragraph 1 of this Article remotely, the Bank is required to apply reliable authentication of the User,

including elements to dynamically link the transaction to a specific amount and recipient.

The Bank must establish appropriate security measures to protect the confidentiality and integrity of the User's personalized security elements in cases mentioned in paragraph 1.

The provisions of paragraphs 2 and 3 of this Article apply also to payment transactions initiated through a payment initiation service provider.

The Bank that maintains the User's account is obligated to ensure that the payment initiation service provider and the account information service provider follow the authentication procedure provided by the Bank in accordance with paragraphs 1 and 3, and for the payment initiation service provider, in accordance with paragraph 2.

9. Selection of Payment Brand and Payment Application (Co-branding)

The Bank has the right to include two or more different payment brands or payment applications on a payment instrument based on a payment card. A payment instrument based on a payment card is any payment instrument, including a payment card, computer, mobile phone, or any other technical device that contains a payment application, allowing the payer to initiate a payment transaction based on the payment card.

The Bank is obligated to provide the consumer with clear and objective information about the payment brands associated with the service, including their characteristics, capabilities, applicability, costs, and protective measures, within a reasonable period before concluding the payment service agreement.

10. Confirmation of Availability of Funds

The Bank that maintains the User's account is obligated to respond immediately upon receiving a request from the payment service provider issuing the payment instrument based on the payment card to confirm whether the amount required for executing the payment transaction on the payment card is available in the User's payment account, provided that the following conditions are met:

1. The payment account of the User can be accessed via the internet at the time the request is received;
2. The User has expressly consented to the Bank to respond to such a request from a specific payment service provider to confirm that the amount available in the User's payment account corresponds to a specific payment transaction based on the payment card;
3. The consent referred to in point 2 was given before the first such request is made.

The payment service provider issuing the payment instrument based on the payment card may submit the request mentioned in paragraph 1 of this Article if the following conditions are met:

1. The payer has expressly consented to the submission of such a request;
2. The payer has initiated a payment transaction based on the payment card using the payment instrument;
3. The payment service provider issuing the payment instrument has authenticated itself to the payment service provider maintaining the account before submitting each such request and establishes communication and exchanges messages and data securely.

The response to the request in paragraph 1 of this Article shall only contain a 'yes' or 'no' answer without disclosing the state of the payment account and cannot be stored or used for any purpose other than executing the payment transaction.

The Bank that maintains the User's account cannot prevent the use of funds in the User's payment account based on the response in paragraph 1 of this Article.

The Bank maintaining the User's account must inform the User, upon request, about the payment service provider who made the request and the response provided.

The provisions of paragraphs 1 to 5 of this Article do not apply to a payment instrument based on a card where electronic money is stored.

11. Termination and Expiry of the Agreement

11.1.1. Entry into Force of the Agreement and Amendments to the Agreement

All amendments to the Agreement must be made exclusively in writing and properly signed by authorized representatives of both parties, except for those in favour of the User that can be changed and applied immediately without their prior consent, in accordance with the law.

If the Bank proposes amendments to the provisions of the Agreement, it must provide the User with the proposal in writing at least two months before the proposed implementation date for entrepreneurs or at least 15 (fifteen) days before the proposed implementation date for legal entities, and the User may accept or reject them before the proposed date.

Exceptionally, if the Bank proposes a change in fees for providing payment services in favour of the User or introduces a free new service or functionality to an existing service, such a change can be applied immediately without prior delivery of the proposal to the User for amendments to the framework agreement related to that change.

The User is considered to have agreed to the proposed

amendments to the Agreement if they do not notify the Bank that they disagree before the date of implementation, and the Bank must inform the User in an easily noticeable way when delivering the proposal.

The Bank is obligated to inform the User simultaneously with the proposal about the right to terminate the Agreement without paying fees or other costs before the proposed amendments come into effect if the User does not accept the proposal.

The Bank is obligated to inform the payment service user simultaneously with the proposal about their right to terminate the framework agreement without paying fees or other costs at any time before the proposed amendments come into effect and establish the date before the start of the proposed amendments when the termination will take effect.

11.1.2. Conditions for Unilateral Termination of the Agreement

The User has the right to terminate the Agreement at any time with a notice period of one month, without penalty. The User also has the right to terminate the Agreement in other cases specified by the law governing obligations or other applicable laws.

The Bank has the right to terminate the Agreement concluded for an indefinite period, with a notice period of 2 (two) months, as well as in other cases specified by regulations, by delivering written notice to the other party through the agreed communication channels. In the event of termination, the User is required to pay the Bank only for the payment services provided up to the date of termination, and if such a fee was paid in advance, the Bank is obligated to return the proportional part of the paid fee to the User.

The User may request that provisions of the Agreement that conflict with the information provided during the pre-contractual phase in accordance with the Law, or provisions relating to mandatory elements of the Agreement that were not previously provided, be deemed null and void.

The Bank, except in the cases mentioned above, may unilaterally terminate the Agreement and close the User's accounts in the following cases:

The Bank, except in the cases mentioned above, may unilaterally terminate the Agreement and close the User's accounts in the following cases:

- If it is determined that the User is listed on official terrorist and other negative lists, in accordance with domestic and international regulations on preventing money laundering and the financing of terrorism;
- If the User fails to provide data about themselves, their ultimate owners, their business operations, the origin of funds, or the nature/purpose of the business relationship with the Bank and/or transactions

conducted through the Bank, upon the Bank's request within the specified or reasonable time frame;

- If the User's account has been inactive for a period of 6 (six) consecutive months, meaning there are no recorded activities in the application.

12. Confidentiality and Protection of Personal Data in Relation to Payment Services

The Bank processes the User's personal data in accordance with the applicable Personal Data Protection Law of the Republic of Serbia and the General Terms and Conditions of AikBank a.d.

Personal data of the User are processed in order to execute the contractual relationship between the User and the Bank, fulfil legal obligations of the Bank, and for processing for marketing purposes if the User has given explicit consent.

Further details on personal data processing, the data controller, the data protection officer, and the rights of the individuals whose data is processed are available in the General Terms and Conditions (GTC) and the Notice on Personal Data Processing, which can be found on the Bank's website and in the Bank's branches and is regularly updated.

The Bank and participants in the payment system may collect, process, and exchange data related to the payment service user, including personal data and data about the payment transaction and the status and changes in the user's payment account, for the purpose of preventing, investigating, or detecting fraudulent activities or abuses in relation to payment services.

13. ENTRY INTO FORCE

This Annex 6 of the General Terms and Conditions enters into force upon adoption and will be applied starting from 6 May 2025.