ADRIATIC BANK AD PODGORICA

GENERAL TERMS AND CONDITIONS FOR ELECTRONIC BANKING

Version 1.2

Podgorica, 31st January, 2024

Pursuant to authorizations under art. 55 and 206 of the Law on credit institutions, art. 164, 165 and 189 of the Company Law as well as art. 43 of the Articles of Association of Adriatic Bank AD Podgorica, the Management Board of Adriatic Bank AD Podgorica (hereinafter: the Bank) on 31 January 2024, passes the following:

GENERAL TERMS AND CONDITIONS FOR E-BANKING

I INTRODUCTORY NOTES AND GLOSSARY

These General Terms define the manner of establishing, using, and terminating the services of Electronic Banking of Adriatic Bank AD Podgorica, with address: Boulevard of George Washington no. 98, 81000 Podgorica, registered with the Central Registry of Business Entities, under number 40009471, with identification number 03087158 (hereinafter: The Bank), by the Users of the services.

Some terms used in these General Terms have the following meanings:

1. A remote communication-based payment service - Electronic Banking - (hereinafter Electronic Banking) is an online banking service enabling the submission of orders for national and international payment transactions, as well as other services and activities related to clients' accounts and products, utilizing telecommunication, digital, or information technology devices (such as computers, smartphones, etc.).
2. Authentication verification is a process allowing the payment service provider to verify the identity of payment service users or the validity of specific payment instrument usage, including the use of personalized security data by users.
   2a. Reliable client authentication verification involves using two or more independent elements falling into the categories of knowledge, possession, and inherence, known and possessed only by the User, designed to protect data confidentiality.
   2b. Personalized security data are characteristics provided by the payment service provider to users for authentication verification.
   2c. Sensitive payment data are details potentially exploitable for fraud, including personalized security data, excluding the account owner's name and number for payment initiation and account information activities.
3. An electronic payment transaction is initiated and conducted through electronic platforms or devices, excluding paper-based, mail, or telephone-initiated payment transactions.
4. A credit transfer allows the payment service provider holding the payer's account to debit it for one or multiple transactions in favour of the payee's account, based on payment orders issued by the payer.
5. A payment initiation service initiates payment orders upon user requests, involving payment accounts held with other payment service providers.
6. An account information service consolidates information on one or more payment accounts held by the User with other service providers through online connectivity.
7. A payment account holding service provider opens and manages payment accounts for payers.
8. A trusted payee list comprises predefined payees marked by the payer as trusted, exempt from client authentication verification for payments.
9. mToken is a feature within the Bank's mobile application enabling secure user authentication and authorization of remote orders through registration and subsequent PIN determination.
10. Authorization confirms user consent for payment transaction execution, contract conclusion, or other purposes within electronic banking, varying based on the online banking application used and defined within General Terms and application forms.

11. Biometric data refers to unique physical characteristics recorded and stored by users on their devices for biometric authentication and transaction authorization purposes.

II SERVICE USERS

Service users are physical and legal persons that have an account opened with the Bank (hereinafter: the User), residents and non-residents or clients who made request to the Bank to activate e-banking service.

• physical persons – owners and their representatives who have signed the application form authorised by the account holder to use Adriatic Web Bank/or Adriatic Mobile Bank.
• legal persons – users authorised by a person authorised to represent a legal person and who has signed the application form.

III SELECTION OF SERVICE

The User independently selects a desired service in the application form:

• Electronic banking and mobile banking (Adriatic Web Bank and Adriatic Mobile Bank) or
• SMS info

III ACTIVATION OF E-BANKING

The User may activate e-banking services by:

1. Signing the Framework Agreement on Opening and Maintaining a Transaction Account for making national payment transactions by using remote means of communication – E-banking/ mobile banking by selecting a field next to a service type at the beginning of the Agreement, check box

2. Signing the Application Form on Activating the E-banking service

By activating the E-banking service, the User can use:

- Adriatic Web Bank – providing a client to exchange messages and calls over the internet network by using telecommunication means, digital or IT device.

- Adriatic Mobile Bank – over a smart phone application enables instant messaging and calls using the internet network.

Upon client's request for service activation, username and PIN (personal identification number) are generated and submitted to the client. When log in, the Client is allowed to change the assigned PIN.

The User can access their payment account with online connectivity only after successful identification and authentication.

A user who has contracted the use of the Adriatic Web Bank service reliably authenticates when accessing the application by using a dual authentication system (PIN + One-time password). The one-time password is generated via mToken after the User enters their PIN or biometric data.

A user who has contracted the use of the Adriatic Mobile Bank service can authenticate by entering the PIN selected for application access or through biometric authentication.

The Bank will be considered to have authenticated the User at the moment when the User

positively confirms the use of the same fingerprint or facial biometric characteristics stored on the device when accessing the application, utilizing one of the offered biometric authentication options.

IV TRANSACTION EXECUTION

All types of e-banking usage, including the entry of payment orders from the User's account electronically entered by using a prescribed user's identification are equal to hand written signature and binding to the User.

E-banking service is available to the User 24 hours a day, seven days a week. Payment orders received are processed every working day from 08:00 to 15:30 h. Orders received after this period are processed the following business day.

A payment transaction is considered authorized only if the payer has given consent for the execution of the payment transaction. Consent can be given before or, if agreed between the client and the Bank, after the execution of the payment transaction. The consent to execute a payment transaction or a series of payment transactions must be given in the manner agreed upon between the payer and their payment service provider and can also be given through the payee or the payment initiation service provider. Otherwise, the payment transaction is considered unauthorized.

The Bank is required to apply reliable authentication verification of the User when initiating an electronic payment transaction.

Authorization or confirmation of transactions is provided in one of the following ways:

a) Authorization of payment transactions initiated through the Adriatic Web Bank service - it is conducted by the User signing the payment order with mToken using the dual authentication system (PIN + One-time password). The one-time password is automatically generated via mToken after the User has been identified by entering their PIN or biometric data.
b) Authorization of payment transactions initiated through the Adriatic Mobile Bank service – it is conducted by the User signing the payment order by entering the PIN used for identification or by using biometric data.

V PAYMENT ORDERS

Payment is made when the User makes initiation to the telecommunication, network or IT system operator.

The User is solely responsible to fill out and check if the filled-out orders are correct.

The User shall perform e-banking services in line with the applicable regulations and legal acts of the Bank regulating the payment operations. In addition, the User shall initiate executing of transactions in line with the law and guarantee that the information entered into the order are accurate. The User shall bear full responsibility if the entered information is incorrect.

Payment order shall be executed within a deadline in line with a business policy, the Bank's practice and the applicable legal regulations.

The Bank shall only execute the authorized payment orders of the User related to the transaction account opened in line with the agreement and within the available funds in the account.
The Bank shall manage the account and execute payment orders in line with legal and other positive regulations applied in Montenegro.

Transactions from domestic into the account abroad are executed in line with the international standards, regulations and acts of the Bank regulating the international payment operations. The User is required to provide the Bank with the necessary accompanying documentation along with the payment order, which represents the basis of the transaction (invoice, proforma invoice, agreement, order, etc.), via email to payments@adriaticbank.com, attaching scanned copies of the above listed documentation.

The User shall be held responsible for the data identity from the previously sent order and the documentation submitted later. In case of disagreement or failure to submit the above-mentioned documentation, the Bank is entitled to suspend execution of the following order until the documentation for the previously realized order is submitted.
The Bank shall not be held responsible for the User's orders rejected in the payment operations due to the User's error or if incorrectly filled out order has been executed.

The Bank shall not assume responsibility if the e-banking services are not available due to technical problems on the User's computer equipment or phone, failure or disturbances in telecommunication channels, failures or interferences in telecommunication channels, power system failures or as a result of force majeure i.e. for other circumstances out of the Bank's control.

In case of a suspected abuse, the Bank shall temporarily block execution of the remote access service to the Bank's account and notify the User. The Bank shall unilaterally suspend the remote access service to the its account if the User fails to comply with all provisions of the Agreement governing the use of electronic banking and other legal acts of the Bank. The User may request a temporarily suspension of certain remote access services to the Bank's accounts by submitting a written request to any branch of the Bank.

The Bank shall not be held responsible for the User's orders rejected in the payment operations due to the User's error or failure to execute improperly filled out order.

The Bank prescribes a timeframe for sending the orders within the Banking day. The orders sent after a timeframe shall be processed in currency the following business day if the User itself does not choose a currency by own choice to execute transactions. Payment order electronically sent and received by the e-banking service has the same legal power as a paper payment instrument signed by hand. The Bank guarantees proper recording of all properly sent orders and their safekeeping in line with the law.

VI REVOCATION OF PAYMENT ORDERS

The User can revoke the payment order, i.e. withdraw the authorization through the Electronic Banking application in the payment order overview section, provided that the Bank has not executed the payment order and that the order was initiated via electronic banking.

A payment order shall be deemed irrevocable after it has been executed.

If the User initiates a payment order but does not have sufficient funds in their account to execute the payment transaction, the Bank will begin processing the order on the day when the User provides additional funds to the Bank, within a time frame of 30 days for domestic payment orders or 3 days for cross-border and international payment orders. If the User fails to provide additional funds to the Bank within the specified time frames, it will be considered that the User has revoked the order, which the Bank will record in its records, and the Bank is not obliged to inform the User in particular about the revocation.
If the payment transaction is initiated by or through the payee, the User cannot revoke the payment order.

In the case that the User does not make additional funds available to the Bank, a reservation will be made on the account for the amount of the previously entered payment order.
To release the account from reserved funds, the User must cancel the payment order on his own initiative, through the Bank's application.

VII USER'S RESPONSIBILITY

The User is obliged to safeguard devices and authentication data to prevent their damage, destruction, loss, theft, and bears all the risk of their misuse.

The User shall be held liable for the confidentiality and security of each user identification and accept full responsibility for all obligations arising from its user identification.

The User shall immediately notify the Bank on non-authorized usage of its user identification and on any other form of breaking the security.

The User must have a licensed operating system on the computers or smartphones where e-banking services will be used from. The Bank shall not be held responsible for non-executing the orders due to an unlicensed and improperly configured operating system and improper using of e-banking.

The User agrees that the Bank can charge a fee in line with the Bank's tariffs and/or provisions of the applicable Catalogue of Products for services and transactions processed by e-banking.

Any damage arising out of non-compliance with these regulations shall be borne by the User.

If unauthorized payment transactions result from the use of a lost or stolen payment instrument or misuse of the payment instrument, the User may be liable for losses associated with these unauthorized payment transactions up to a maximum of 50 euros.

However, the User is not liable for losses up to the aforementioned amount if:

1. The loss, theft, or misuse of the payment instrument could not have been detected before the unauthorized payment transaction was executed.
2. Unauthorized payment transactions are a result of actions or omissions of an employee, agent, or branch of the payment service provider, or a person to whom the activities of the payment service provider are outsourced.
3. The payment service provider did not provide appropriate means for notifying the loss, theft, or misuse of the payment instrument, in accordance with the provisions of the Payment System Law.
4. The payment service provider of the payer does not require reliable customer authentication.
5. The payment service provider of the payee does not apply the required reliable customer authentication.

The payee or the payment service provider of the payee who fails to apply the required reliable customer authentication is obliged to compensate the payment service provider of the payer for the damage suffered as a result.

However, the User bears all losses associated with unauthorized payment transactions if the payer acted with fraudulent intent or intentionally or with gross negligence failed to fulfil one or more obligations, namely, to use the payment instrument in accordance with the terms of issuance and use of that payment instrument specified in the contract, which must be objective, non-discriminatory, and proportionate and/or immediately upon learning of the loss, theft, or misuse of the payment instrument, or its unauthorized use, notifies the Bank or the person designated by the payment service provider.

The User is not liable for the amount of unauthorized payment transactions executed after promptly informing the Bank or the person designated by the payment service provider upon learning of the loss, theft, or misuse of the payment instrument, or its unauthorized use unless they acted with fraudulent intent.

VIII WARRANTIES AND CLAIMS

The Bank guarantees the User of the Adriatic Web Bank services free disposal of funds in all accounts in accordance with the General Terms and Conditions, opened pursuant to the agreement signed with the Bank up to amount of funds in the account including the allowed overdraft in these accounts.

The Bank shall not assume responsibility for the cases where the User is not allowed to use E-banking services, occurred as a result of technical problems on the User's computer equipment or phone, interruptions and interferences caused by telecommunication channels or interruptions caused by the interruption of power supply and all other events the Bank cannot influence on but which can be considered a case or force majeure.

The User undertakes to file a possible complaint in writing no later than 3 days after the bank statement or other notification is made available for inspection or disposal, or within 8 days after dispatch if they are sent by post. Otherwise, it is considered that the statement or other notification is not disputed.

Any disputes or complaints regarding the provision of services will be resolved amicably between the User and the Bank.

A complaint regarding the provision of services can be submitted by the User to the Bank in person, via the Bank's email address kvalitet@adriaticbank.com accessible also through the Bank's website, or by mail to the Bank's address. The Bank will respond to the complaint within a maximum of 8 days. If the User disagrees with the Bank's decision regarding the complaint, they can submit the complaint to the Central Bank of Montenegro at the following address: Bulevar Svetog Petra Cetinjskog br. 6, 81000 Podgorica.
The complaint should be in written form and should contain a brief request and all the facts on which the User bases their complaint.

Information about the authority responsible for alternative dispute resolution is displayed on the Bank's official website and in the Bank's premises.

The User's right to initiate alternative dispute resolution procedures in accordance with special laws regulating alternative dispute resolution and arbitration, as well as in accordance with the law on consumer protection, does not affect their right to initiate legal proceedings in accordance with the law.

IX LIMITATIONS

If the User fails to pay due obligations arising from the use of services specified in these General Terms and Conditions, or if the User does not comply with any of the provisions of these General Terms and Conditions, the Bank shall temporarily block at its sole discretion the electronic banking services.

The Bank reserves right to cancel e-banking services without a written explanation or announcement if the User has not had regular payments into the account opened with the Bank more than six months.

The Bank is obliged to have valid identification documents of clients in accordance with regulations. The User is required to update their information at the nearest bank branch before the expiration of the identification document held by the Bank. Otherwise, the Bank will temporarily suspend the User's transactions until the conditions for their regular execution are met, or until the User updates the information held by the Bank.

The Bank has the right to block the payment instrument for objectively justified reasons related to:

1. the security of the payment instrument;
2. suspicion of unauthorized or fraudulent use of the payment instrument, or
3. in the case of a payment instrument with a credit line, due to a significant increase in the risk that the payer will not be able to meet the payment obligation.

Before blocking the payment instrument, the Bank must inform the User of the intention and reasons for blocking the payment instrument by calling the User's contact phone registered with the Bank. If the Bank is unable to inform the User in accordance with the previous paragraph, it must do so immediately after blocking the payment instrument.

The Bank is not obliged to notify the User as defined in the previous paragraphs if giving such notice contradicts objectively justified security reasons or is not in accordance with the law.

The Bank is obliged to unblock the payment instrument or replace the blocked payment instrument with a new one when the reasons for blocking that payment instrument cease.

The Bank maintaining the account must not deny access to the account for payment service providers or payment initiation service providers, except for proven and objectively justified reasons related to unauthorized access by that service provider or its access for fraudulent purposes, including unauthorized initiation of a payment transaction or initiation of a payment transaction for fraudulent purposes. In the aforementioned case, the Bank maintaining the account must inform the payer in the agreed form of the denial of access to the payment account and the reasons for the denial of access, provided that, if possible, this information is provided to the payer before denying access, and at the latest immediately after denying access, unless providing such information would jeopardize objectively justified security reasons or is not in accordance with the law.

The Bank maintaining the account must enable access to the payment account immediately after the reasons for denying access cease.

The User has the right to terminate the use of services, and they can do so by submitting a written request at any branch of the Bank. Upon submitting a written request for termination, the User is obliged to return all assigned user identifications.

X FEE

All fees for using e-banking services are charged according to the Tariffs for national and international payment transactions.
The User pays monthly fee and agrees that the Bank could charge the fee by indebting the transaction account of the electronic banking User at the end of the month. The electronic banking User must have available funds in the account to cover commitments under the Framework agreement.

By signing the Framework Agreement, the User confirms that he/she is familiar with the General Terms and Conditions of using E-banking and authorises the Bank according to the applicable Tariffs and Catalogue of Products to indebt the client’s accounts for all services based on using electronic payment platform for applicable fee without issuing individual orders.

Applicable tariffs for national and international payment transactions are published on the Bank's website and are available at a visible location within the Bank's branches designated for that purpose.

XI NOTIFICATION ON TRANSACTIONS

The User is informed on completed transactions over the Bank statement contained in the application or through other manner agreed for every individual account or by email.

The Bank notifies the User on terms and conditions for e-banking services on its official website www.adriticbank.com or in the Bank's business network by placing notification of change and the amended General Terms and Conditions for E-Banking in a visible designated place.

The Bank notifies the User on completed transactions of funds and other transactions made from the account as well as on its balance at User's request by means of a bank statement on completed transactions.

By signing the Agreement, the E-banking User agrees to receive additional information and other messages by the Bank.

XII SIGNATURE

By signing the application form to use the electronic banking service, the User has accepted these General Terms and Conditions to be binding.

XIII SERVICE CANCELATION

The User may request for cancellation of e-banking services in writing or in person in the Bank's branch. The cancelation is made effective the first day after the Bank receives the User's notification on service cancellation.
Service cancellation is recorded by delating an existing User based on his/her request.

XIV FINAL PROVISIONS

The Bank shall notify the User on any amendments made to the General Terms and Conditions, tariffs or fees in writing and/or by any of the info channels (SMS, e-mail, Viber etc.) and by publishing on its website before they are made effective.
The User shall not be entitled to claim indemnification in case of changing the context of E-banking services.

Any amendments made to these General Terms and Conditions shall be in writing and approved by the relevant Bank's authority. Afterwards, the Bank shall post them on its website.

If the User continues to use E-banking services after these amendments have been published and does not cancel their using in writing, he/she shall be deemed to have accepted these amendments.

These General Terms and Conditions for Electronic Banking refer to legal and physical persons and will be applicable starting April 8, 2024.

In Podgorica, January 31, 2024.

CHAIRMAN OF THE MANAGEMENT BOARD

Enesa Bekteši