

Electronic banking agreement

General part

1. Terms used in the agreement

1.1. The following terms shall be used in this Agreement:

1.1.1. **Security and Identification Tools** shall mean an identification code (a unique sequence of digits which is used to identify a person at the time of registration with the Bank's online services system), a temporary password (a unique sequence of digits which is used to verify the identity of a person at the time of registration with the Bank's online services system and which the User must change when he/she logs in to the Bank's online services system for the first time) provided to the User by the Bank, an additional security code sent by the Bank's SMS message or any other identification and/or authentication (action authorisation) tool installed at the Bank as selected by the Customer, satisfying the requirements of legal acts, used to identify the Customer and/or User, authorise payment operations or for other instructions and sign transactions. The Bank shall be entitled to unilaterally decide which Security and Identification Tools will be installed and/or abandoned.

1.1.2. **Electronic Signature** shall mean an electronic equivalent of a regular signature and a person's identity document consisting of certain information in electronic form (Customer name and surname, facial image, device information, time of use, etc.), the whole of which allows the Bank to identify the person using them. An Electronic Signature may be stationary (installed on a chip, USB or other media), mobile (Installed on a SIM card issued by a mobile operator), as well as integrated into the software or otherwise linked with it (e.g. sending a one-time security code by an SMS message, etc.).

1.1.3. **Identification and Action Authorisation Tools** shall mean an electronic signature, an advanced electronic signature or a qualified electronic signature generated using tools provided by the Bank or by third parties acceptable to the Bank, or other tools specified in the Agreement or other documents published by the Bank, including the biometric data (e.g. fingerprints) saved on and/or scanned by the User's device, by means of which the User's identity is confirmed, payment operations are authorised and transactions are signed.

1.1.4. **Bank** shall mean AB Mano Bankas, Company Reg. No. 112043081, registration address: S. Moniuskos st. 27, Vilnius LT-08115, Register of Legal Entities of the Republic of Lithuania, e-mail hello@mano.bank, phone +370 5 2409389, website www.mano.bank.

1.1.5. **Online services system of the Bank** shall mean the electronic system for providing Customers with the Bank's services online, which can be accessed at www.mano.bank.

- 1.1.6. **Customer** shall mean a person, to whom the Bank provides electronic services, whose details are specified in the Special Part of the Agreement and who concludes this Agreement with the Bank and is entitled to perform the actions listed in clause 2.1 of the General Part of the Agreement;
- 1.1.7. **User** shall mean the Customer, the Customer's (legal entity's) representative or other natural person indicated by the Customer, to which the Customer grants the right to execute Operations via the Bank's online services system. The same natural person may act as the User and as the Customer;
- 1.1.8. **Operations** shall mean actions and operations related to the services provided by the Bank, which may be performed or which may be availed of via the Bank's online services system.
- 1.1.9. **Notice** shall mean the User's declarations, instructions regarding disposal of funds and/or accounts and/or other notices and information sent to the Bank via the electronic system.
- 1.1.10. **Account** shall mean the Customer's account opened in the Bank.
- 1.1.11. **Agreement** shall mean this Electronic Services Agreement concluded between the Bank (acting as the service provider) and the Customer (acting as the service recipient).
- 1.1.12. **Other terms used in the Agreement** shall have the meanings provided in the Conditions of Provision of Payment Services, except where otherwise specified in the Agreement.

2. Subject matter of the agreement

- 2.1. The Agreement shall regulate the provision of the Bank's services via electronic channels, i.e. via the Bank's online services system, via which the Customer may perform the following actions:
- 2.1.1. Obtain and print its Account statements;
- 2.1.2. Present payment orders to payees that have accounts in credit and financial institutions operating in
Lithuania;
- 2.1.3. Present payment orders to payees that have accounts in credit and financial institutions operating
outside of Lithuania;
- 2.1.4. Execute other banking operations;
- 2.1.5. Conclude/terminate a deposit agreement;
- 2.1.6. Execute currency exchange operations;
- 2.1.7. Receive and provide information and submit notices and requests;

- 2.1.8. Perform other actions.
- 2.2. The User appointed by the Customer, the rights granted to the User, the Operation limits and other information shall be specified in the Special Part of the Agreement and/or annexes to the Agreement, which shall constitute an integral part of the Agreement. The Customer shall be entitled to appoint one or several Users and grant them either identical or different rights and Operation limits.
- 2.3. The Agreement shall qualify as an arrangement of the Bank and the Customer that may not be revoked unilaterally and that confirms that such agreements concluded (amended, terminated) via electronic channels by the Customer/User, the Customer's instructions regarding disposal of the Customer's funds, sent Notices and payment order execution and other actions performed and approved using, according to the procedure prescribed by the Agreement, the Security and Identification Tools provided by or satisfactory to the Bank, including the Identification and Action Authorisation Tools, shall have the same legal effect as signed written documents and may be used as means of evidence in court.
- 2.4. The Customer may only present payment orders in respect of funds available in current accounts.
- 2.5. The relationship regulated by the Agreement shall also be regulated by the Civil Code and other legal acts of the Republic of Lithuania, the Conditions of Provision of Payment Services of the Bank and other documents published by the Bank, which the User can consult on the internet website of the Bank and at customer service centres of the Bank.
- 2.6. The Bank shall be entitled to suspend the use of the online services system of the Bank for important reasons (technical maintenance, software upgrade or expansion, etc.).
- 2.7. The Bank shall notify the Customer that the Bank may record the actions performed and the Operations executed by the User in the online services system of the Bank, which, if need be, may be used as evidence of Operations executed via the online services system of the Bank. Where the Customer presents notice verbally, the Bank shall be entitled, according to the procedure prescribed by legal acts, to record the conversation subject to prior notice given to the Customer.

3. Identification of the user and identification tools

- 3.1. The parties agree that Operations may be authorised/signed with the Identification and Action Authorisation Tools where the User expresses his/her will by an electronic signature, using codes and passwords sent by the Bank's SMS message to the mobile phone of the User, as well as the biometric data read and/or saved on the User's smart device and other tools installed by the Bank, or combinations of the means specified in this clause.

To ensure the secure Operations of the Customer, the Bank shall provide the User with the following Security and Identification Tools:

- 3.1.1. An identification code; and
- 3.1.2. A temporary password.

- 3.2. The Security and Identification Tools required for logging in to the online services system of the Bank shall be provided to the User for the fee set by the Bank and specified in the price list published on the internet website of the Bank at www.mano.bank.
- 3.3. The Bank must replace the Security and Identification Tools provided by the Bank for the fee specified in the price list published on the internet website of the Bank at www.mano.bank, if the Customer or the User claims that the confidentiality of the tools has been impaired at the fault of third parties or that the tools have been lost.
- 3.4. When logging in to the online services system of the Bank for the first time, the Customer may use the Security and Identification Tools provided by the Bank or a qualified electronic signature to confirm its identity. Where, at subsequent logins, the Bank provides such an opportunity and the Customer wishes to use other identification and action authorisation tools (Security and Identification Tools), the Customer must, upon logging in to the online services system of the Bank using the Security and Identification Tools provided by the Bank, activate, in the settings section, the Security and Identification Tool that the Customer wishes to use and implement the other conditions prescribed by the Bank and required for using the tools. Upon completion of the above procedure, the Customer will be able to use the chosen Security and Identification Tool when it subsequently logs in to the system.
- 3.5. At the time of concluding the Agreement, the Customer (legal entity) may indicate up to 2 (two) Users (natural persons) who will handle the Customer's accounts in the online services system of the Bank. The Customer that is a natural person may only be the User himself/herself. The Users registered with the online services system of the Bank may be granted different Operation execution rights and different limits. The Customer must indicate which Operation execution rights are granted and which limits are set to a specific User, which accounts the User will be entitled to handle and what requests the User will be entitled to submit. 3.6. The Customer must deem that the User has been duly identified and recognise and deem as signed and approved the Notices and documents sent to the Bank via the online services system of the Bank, if the appropriate Security and Identification Tools have been used.
- 3.7. The Customer hereby agrees to ensure that the Customer/User use the services of the Bank provided via electronic channels in adherence to legal acts of the Republic of Lithuania regulating settlement, disposal of funds and conclusion of transactions and the Conditions of Provision of Payment Services of the Bank and that the Customer/User do not exceed the authorisations enjoyed by, or granted to them.
- 3.8. The Customer hereby agrees to take all the required steps to ensure the confidentiality and security of all and any information received in the process of the Customer using the online services system of the Bank. 3.9. The Customer and/or the User may not contest an Operation (e.g. a payment order, a concluded agreement, etc.), if the Operation was executed by the User using the Security and Identification Tools.
- 3.10. The Customer must protect the Security and Identification Tools and notify the Bank immediately about the loss of these tools or any violations of the confidentiality of the tools according to the procedure prescribed by the Conditions of Provision of Payment Services of the Bank. Where the loss of the Security and Identification Tools is related to unlawful actions of third parties, the Customer must immediately notify law enforcement

institutions of that. The User shall be responsible for the Security and Identification Tools provided by the Bank from the moment the User receives them. The Security and Identification Tools provided by the Bank shall be owned by the Bank by right of ownership.

- 3.11. The Customer hereby agrees to adhere to the applicable Bank services agreements when performing any actions (presenting payment orders, Notices and/or requests, concluding agreements and performing other actions) using the online services system of the Bank.
- 3.12. The Customer shall be responsible for the protection of any other Security and Identification Tools (issued by parties other than the Bank) that the Customer chooses to use. The Customer must immediately notify the Bank according to the procedure prescribed by the Conditions of Provision of Payment Services of the Bank, if the Customer is aware of, or has grounds to believe that any information related to these tools (username, password, etc.) or other tools (mobile phone, USB data holder, etc.) have become known to, or have been misappropriated by third parties.
- 3.13. Where the Bank is not notified about the loss of the Security and Identification Tools and/or violation of the confidentiality of the Security and Identification Tools, which occurred either at the fault of, or through negligence of the Customer or third parties, the Bank shall qualify as lawful and implementable any one instruction that is given using such Security and Identification Tools.
- 3.14. Where, in the process of executing Operations, the Security and Identification Tools were used and/or the Bank reasonably suspects that the respective instruction has been given by a party other than the User, the Bank shall be entitled to refuse to execute the Operation and/or demand that the User or the Customer execute the Operation in another manner acceptable to the Bank.
- 3.15. The Bank shall recognise and deem as signed and approved by the Customer the Notices received via the Bank's system about the use of funds available in the Account, the conclusion of agreements and other information, if, at the start of the communication session and at the time of confirmation, where so required by the online services system of the Bank, the appropriate Security and Identification Tools have been used.

4. Operation limits

- 4.1. The limit per Operation, the daily Operation limit and the monthly Operation limit shall be set for the User:
 - 4.1.1. The limit per Operation shall mean the maximum amount of money that the User may use to execute one Operation. The standard limit per Operation approved remotely shall be EUR 3 000;
 - 4.1.2. The daily Operation limit shall mean the maximum amount of money that the User may use to execute Operations in the course of one business day of the Bank;
 - 4.1.3. The monthly Operation limit shall mean the maximum amount of money that the

User may use to execute Operations in the course of one month. The standard monthly Operation limit approved remotely shall be EUR 10 000.

- 4.2. The specific limit per Operation, daily Operation limit and monthly Operation limit granted to a specific User shall be specified in the Special Part of the Agreement and/or annexes to the Agreement. The limits specified in the Special Part of the Agreement and/or annexes to the Agreement may be adjusted: for this purpose, the Customer or its duly authorised representative must visit a customer service centre of the Bank and submit an application to adjust the limits; the User that has the administrator rights may also adjust the limits via the Bank's online services system. The specific maximum limit per Operation, daily Operation limit and monthly Operation limit granted to the Customer in respect of one current Account shall be specified in the Special Part of this Agreement.
- 4.3. The limits specified in the Agreement shall be calculated by adding up the amounts of the executed Operations. Where the respective limit applies to all the Accounts of the Customer, then the use of such limit shall be calculated by adding up all the Operations executed in all the Accounts of the Customer which are governed by the Agreement.
- 4.4. Where a set limit is exceeded in the process of executing an Operation, the Bank shall not execute the Operation.
- 4.5. The Bank shall be entitled to set the general limits unilaterally for Operations carried out via the electronic channels, as well as the limits for the used Identification and Action Authorisation Tools (e.g. the maximum limit using the biometric data for identification).

5. Blocking of access

- 5.1. The Bank shall block the Customer's access to the system, if:
 - 5.1.1. The Customer demands this according to the procedure prescribed by the Conditions of Provision of Payment Services of the Bank. An officer of the Bank may ask additional control questions for identification purposes.
 - 5.1.2. The User, after entering its identification code, enters an incorrect password in the system five consecutive times or fails to implement the procedure of signing with a mobile signature three times.
- 5.2. Where the User forgets its password, or the access to the system is blocked following entry by the User of an incorrect password five consecutive times or the User commits three failed attempts to implement the procedure of signing with a mobile signature, the User shall visit the Bank to have a new password and a new card with an identification code issued.
- 5.3. The Customer's application to block the User or revoke the User's right to execute Operations shall be submitted in writing by visiting the Bank or by phone, following provision of responses to the control questions asked by an officer of the Bank.

6. Relationship of the customer and the user

- 6.1. Under this Agreement, the Customer shall grant to the User the right to execute Operations on behalf of the Customer. Any changes in the relationship of the Customer and the User (e.g. termination of employment relations, etc.) shall not affect the validity of the Agreement, i.e. if the Customer does not visit the Bank and does not terminate the Agreement or does not, according to the procedure prescribed by the Agreement, submit to the Bank an application to revoke the User's right to execute Operations on behalf of the Customer, the User will be entitled to continue to execute Operations on behalf of the Customer via the online services system of the Bank. The Customer shall assume full liability for all and any Operations executed by the User via the online services system of the Bank.
- 6.2. The provisions of the Agreement shall be binding both on the Customer and the User. The Customer must familiarise the User with the provisions of the Agreement and the Conditions of Provision of Payment Services of the Bank, familiarise the User with the use of the online services system of the Bank and notify the User that the User can contact the Bank according to the procedure prescribed by the Agreement in order to obtain additional information on the use of the online services system of the Bank. After the User signs the provisions of the Agreement it shall be deemed that the User has familiarised himself/herself with the provisions of the Agreement and agrees to abide by them.
- 6.3. Should the User violate the provisions of the Agreement, it will be deemed that the provisions of the Agreement have been violated by the Customer (where the Customer and the User are different persons). The Customer may not, in respect of the Bank, rely on the fact that the User rather than the Customer has violated the provisions of the Agreement or on the fact that the User has not been familiarised with the provisions of the Agreement.
- 6.4. All the Security and Identification Tools provided by the Bank shall only be provided to the User that is a natural person and, in case the Customer and the User are different persons, the Customer shall not have any rights to the Security and Identification Tools provided by the Bank to the User.

7. Fees payable to the bank

- 7.1. The Customer shall pay to the Bank for the Operations executed and other services provided via the online services system of the Bank the fee set by the Bank and published on the internet website of the Bank at www.mano.bank. The fee rates and payment date and periodicity shall be determined based on the rates valid on the respective payment date.
- 7.2. The blocking of execution of Operations by the User shall not suspend the calculation of fees for the services of the Bank provided under the Agreement and shall not affect the Customer's duty to pay such fees.
- 7.3. The User shall use hardware and software at his/her own and/or Customer's expense and risk. All the costs related to the use of the telecommunications or other services chosen

by the User and required for executing Operations via the online services system of the Bank shall be borne by the Customer and/or User.

- 7.4. The Customer hereby agrees to ensure that the Customer's Account specified in the Agreement contain sufficient funds for paying the fees payable to the Bank.
- 7.5. The Customer hereby confirms its consent that the Bank may withdraw the fees payable to the Bank from the Customer's accounts specified in the Agreement without any separate arrangement for the Security and Identification Tools provided by the Bank to the Customer or for the replacement of such tools and for the use of the online services system of the Bank.

8. Liability of the parties

- 8.1. The Customer shall be responsible for the safe use of hardware, software or other equipment used to identify Users and present Notices and hereby agrees to regularly update the Customer's antivirus software, e-mail anti-spam software and privacy assurance software. Should the Customer fail to adhere to these requirements, the Bank shall be exempt from any liability or from the duty to fulfil its obligations related to this Agreement.
- 8.2. The Bank shall not assume any liability for instances where the User is unable to use the online services system of the Bank due to the fact that the Customer does not have the required hardware, software or other equipment or due failures of such hardware, software or other equipment.
- 8.3. The Bank shall not assume any liability for instances where, due to failures in telecommunications networks or at the fault of companies providing telecommunications services, the User is unable to use the online services system of the Bank or information is lost, distorted, etc. due to failures in telecommunications networks.
- 8.4. Since the Bank, prior to accepting the Customer's order for execution, only verifies the information provided in the User's Notices and the fact whether the appropriate Security and Identification Tools are used, the Customer shall be responsible for the Notices presented both by the Customer itself and by any third parties on behalf of the Customer via the online services system of the Bank, if accurate and correct Notice information is provided and the appropriate Security and Identification Tools are used.
- 8.5. The Bank shall not be liable for any erroneous information specified in the Customer's Notice, if such information is accurate and technically correct and is appropriately provided using the Security and Identification Tools.
- 8.6. The Customer shall be responsible for the security of the Security and Identification Tools and for the non-disclosure of information to third parties. The Customer hereby agrees, as soon as it becomes aware that any third parties have access to information of the Customer's Security and Identification Tools, to notify the Bank of this according to the procedure prescribed by the Conditions of Provision of Payment Services of the Bank.

- 8.7. Should the Customer or User fail to abide by the provisions of the Agreement or any other agreements concluded between the Bank and the Customer, the Bank shall be entitled to prohibit the use of the online services system of the Bank without prior notice.

9. Confidentiality and data processing

- 9.1. The fact of conclusion of this Agreement, the General Part and the Special Part of the Agreement, the Conditions of Provision of Payment Services, annexes to the Agreement and all and any information obtained by the Parties in the process of implementing this Agreement shall qualify as confidential and shall not be disclosed to any third parties without the other Party's prior written consent, except in cases envisaged in the Agreement and/or laws of the Republic of Lithuania. The disclosure of information shall not qualify as violation of this clause, if information is provided:

9.1.1. To the audit company that conducts an audit of the operations and/or financial statements of the Bank or the Customer;

9.1.2. To the main shareholder of the Bank, which owns more than one half of all the shares of the Bank, and to companies related to the main shareholder of the Bank or to the Bank;

9.1.3. To attorneys-at-law who provide legal services to a Party;

9.1.4. To other persons, if, by reason of the particularities of cooperation with the Bank and such persons, confidential information must be disclosed.

- 9.2. The Bank shall act as a controller of the personal data of the Customer (and/or its representatives). The Bank shall process the personal data of the Customer (and/or its representatives) pursuant to the provisions of the General Data Protection Regulation (EU) 2016/679, other applicable legal acts and the Personal Data Processing Rules approved by the Bank that can be consulted at customer services centres of the Bank and on the internet website of the Bank at <https://mano.bank/privacy-policy>.

The Customer (or its representative) hereby confirms that it has familiarised itself with the Personal Data Processing Rules approved by the Bank.

Full name of the Customer (the Customer's representative):

10. Miscellaneous

- 10.1. The Agreement shall become effective from the date it is concluded and shall remain effective for an unlimited term. Each of the Parties shall be entitled to terminate the Agreement in writing or via the online services system of the Bank by giving the other Party notice to that effect 30 calendar days prior to termination. Upon termination of the Agreement, the Bank shall not refund to the Customer the fees paid for the Security and Identification Tools provided by the Bank.

- 10.2. The rights of the Customer and the User to use the services of the Bank provided via the

online services system of the Bank shall be valid until one of the Parties terminates this Agreement unilaterally according to the procedure prescribed by this Agreement.

- 10.3. The Bank shall be entitled to immediately terminate the Agreement and discontinue the provision of electronic services in writing and/or via the online services system of the Bank in case the Customer uses the services of the Bank provided via electronic channels in violation of the conditions prescribed by the Bank or performs any actions that harm or may harm the operation of the information systems of the Bank.
- 10.4. In case of any changes in the Customer's address, phone number, mobile phone number, e-mail address or other details specified in the Special Part of the Agreement or the User's details specified in the Special Part of the Agreement, the Customer must immediately notify the Bank about that according to the procedure prescribed by the Conditions of Provision of Payment Services. Should the Customer fail to adhere to this requirement, the Customer may not present any claims or counterclaims that the Bank's actions performed using the last known details of the Customer and, accordingly, the User, do not comply with the Agreement or that it has not received any notices sent using such last known details.
- 10.5. The Agreement shall be concluded in two counterparts, with each Party receiving a counterpart. Both counterparts shall be equally binding. Where the Agreement is concluded via the online services system of the Bank, it shall be deemed that the Bank and the Customer have each received one counterpart of the Agreement, irrespective of whether a copy of the Agreement is printed on paper or not.
- 10.6. One Security and Identification Tool of the Bank may be provided to one User of the system.
- 10.7. The Bank shall be entitled to unilaterally amend and/or supplement the provisions of the General Part of this Agreement according to the procedure prescribed by the Conditions of Provision of Payment Services of the Bank.
- 10.8. The Customer has been informed and agrees that, in the process of executing a transfer to an account opened in another credit institution, the Bank may act as the sender of money and the Customer in this case shall be specified as the payer in the payment details.
- 10.9. In case the provisions of the Agreement are amended, the new wording of the entire Agreement shall be prepared and the number of the Agreement shall remain unchanged. The most recent wording of the Agreement shall be valid.
- 10.10. The pre-contractual relationship of the Parties and the relationship of the Parties related to the conclusion, implementation and termination of the Agreement, liability, jurisdiction, etc. shall be governed by law and legal acts of the Republic of Lithuania.
- 10.11. The Agreement shall be concluded and information related to the Agreement shall be provided to the User in the Lithuanian language; the Lithuanian language shall also be used in other relations between the Bank and the User.