PRIVACY POLICY

I. GENERAL

1.1. The Privacy Policy (hereinafter referred to as the "Policy") establishes the principles of personal data processing at AB Mano bankas (hereinafter referred to as the "Bank"), the rights of data subjects and the procedure for their implementation, as well as the measures ensuring the security of personal data.

1.2. The Policy has been drawn up in accordance with the General Data Protection Regulation, the Law on the Legal Protection of Personal Data of the Republic of Lithuania and other legal acts governing the legal protection of personal data, the activities of financial institutions and the services they provide.

1.3. **This Policy applies when a Data Subject:**

- Uses, has used or has expressed an intention to use or interest in using the services of the Bank;
- Visits the Bank's website;
- Is a principal or beneficial owner, shareholder, member of the board of directors or other collegiate body of the business Customer;
- Is a representative of the Customer (whether corporate or private);
- Is indirectly related to the Services (e.g. is the Customer's spouse, collateral provider, the Customer's data was provided by the Customer, etc.);
- Is an agent of any third party who is engaged in the legal relationship with the Bank (for example, an agent of a company that provides services or sells goods to the Bank);
- has provided his Personal Data or the Bank has received Personal Data for other legitimate reasons not mentioned at the beginning (for example, Personal Data of third parties in documents submitted to the Bank by the Customer, his representative, as well as regarding the processing of the list of shareholders of the Bank, etc.).

1.4. For the purposes of this Policy, the following definitions shall apply:

1.4.1. **Personal Data** means any information that allows direct or indirect identification of the Data Subject.

1.4.2. Processing of Personal Data means any operation or sequence of operations performed on Personal Data, such as collection, recording, sorting, storage, adaptation or alteration, retrieval, access, use, erasure or destruction.

1.4.3. **Bank's website (homepage)** – www.mano.bank, www.manopaskola.lt.

1.4.4. Data Protection Legislation means any legislation on the protection of Personal Data applicable to the Bank, including Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation (GDPR)) and national legislation implementing and supplementing this Regulation.

1.4.5. **Data Recipient** means a natural or legal person, government or other authority to whom the Bank may disclose or transfer Personal Data. The categories of data recipients are set out in Section 7 of this Policy.

1.4.6. DPO means Data Protection Officer.

1.4.7. **Data Subject** means any natural person who uses, has used, has expressed an intention to use or is otherwise related to the services provided by the Bank, the users of these services or the business relationship with the Bank (hereinafter referred to as the Customer).

1.4.8. Data Processor means a natural or legal person who processes Personal Data on behalf of the Data Controller.

1.4.9. **Data Controller** shall mean a legal or a natural person which alone or jointly with others determines the purposes and means of processing Personal data. When Personal Data is processed in accordance with this Policy, the Bank, i.e. AB Mano bankas, shall be the Data Controller, company registration number 112043081, address S. Moniuškos g. 27, LT-08115, Vilnius, Lithuania, e-mail: hello@mano.bank, tel. +370 5 240 9389.

1.4.10. EU/EEA means European Union/European Economic Area.

1.4.11. **Services** mean any service, advice, product of the Bank provided or rendered at a customer service outlet, on the Bank's website, using the Bank's internet banking, telephone, video transmission or other means and which is related to savings, lending, bank accounts, means of payment and payments.

1.4.12. **Applicable Laws** mean the laws and regulations applicable to the Bank, including, but not limited to, laws governing anti-money laundering and anti-terrorist financing activities, bank secrecy, taxation, accounting, payment services and the provision of payment services, lending, including the provision of consumer loans, and other financial activities.

1.4.13. Other terms used in the Policy shall be understood as defined in the GDPR and the Law on the Legal Protection of Personal Data.

II. PRINCIPLES FOR PERSONAL DATA PROCESSING

2.1 When processing Personal Data, the Bank shall comply with the requirements of the legal acts regulating the protection of Personal Data, shall ensure the confidentiality of Personal Data and shall implement appropriate technical and organisational measures to protect Personal Data against unauthorised access, disclosure or unintentional loss, alteration, destruction or other unauthorised processing of Personal Data.

2.2 When processing Personal Data, the Bank shall use Data Processors and shall take the necessary measures to ensure that such Data Processors process Personal Data in accordance with the instructions documented by the Bank, in compliance with the necessary and sufficient security measures, and with the requirements of the legislation governing the protection of Personal Data.

2.3 The Bank's employees who process Personal Data are obliged to keep the Personal Data confidential, unless the Personal Data is intended for public disclosure. This obligation shall also apply after the end of the employment relationship.

2.4 The Bank shall ensure that Personal Data is processed in accordance with the following principles:

2.4.1 **The Personal Data shall be processed lawfully, transparently and fairly.**

- Lawfulness of the processing of Personal Data – the Bank shall processes Personal Data only on a legal basis (see section 4 of the Policy).
- Fairness of the processing of Personal Data – the Bank provides the Data Subject with information on who the Data Controller is, the purposes for which the data are processed, how long the data will be stored, with whom the data will be shared, and explains the Data Subjects' rights (e.g. to withdraw consent to data processing for marketing purposes).
- Transparency of processing of Personal Data – the Bank shall provide information and notices relating to the processing of Personal Data to the Data Subject in a concise, transparent, comprehensible and easily accessible form, in clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

2.4.2 Personal Data shall be collected and processed only for specified, explicit, explicit and legitimate purposes (see Section 4 of the Policy.

2.4.3 Reduction of the amount of Personal Data processed. The Personal Data processed and the scope thereof are proportionate and adequate for the purposes of the processing of the Personal Data, i.e. the Personal Data processed by the Bank are not excessive.

2.4.4 Accuracy and relevance of Personal Data. Personal Data must be accurate and periodically updated.

2.4.5 Temporality of the storage of Personal Data. We keep personal data for no longer than is necessary for the purposes for which it was collected or for such period as may be prescribed by law. When Personal Data are no longer required for the purposes of their processing or after the expiry of the data retention periods provided for in this Policy, it shall be destroyed or anonymised in accordance with the procedure and within the time limits laid down by the Bank and the Applicable Legislation, except where the legislation obliges to retain the data for a longer period.

2.4.6 Personal Data Safety Personal Data shall be processed and protected while ensuring their confidentiality, integrity (integrity) and availability. The Bank uses a variety of security technologies and procedures to ensure the security of Personal Data against unauthorised access, use or disclosure.

III. PERSONAL DATA PROCESSED

3.1 The Bank collects and processes the following categories of Personal Data:

3.1.1 Personal identity and contact details – name, surname, personal identification number, date of birth, details of identity document (including the residence permit in the Republic of Lithuania or EU/EEA country), registration address, telephone number, e-mail address, address of residence or address for correspondence, country of residence.

3.1.2 Identification data – data of a person's identity document (including a residence permit in the Republic of Lithuania or in an EU/EEA country), photo, IP address, internet bank login data and other browsing information, including data on when and where the Bank's website was accessed, as well as the taxpayer's identification number.

3.1.3 Financial data – data on the current/former workplace, economic-commercial activities carried out (for example, farmer, self-employment, etc.), data on accounts, assets held, transactions, loans, income, including projected income and their stability, expenses, liabilities, data on financial experience, credit history and creditworthiness, as well as data on the prohibition to conclude consumer credit agreements.

3.1.4 Data about the transactions of the Data Subject with the Bank and other agreements concluded – depending on the Services provided to the Data Subject by the Bank, the following data are processed: bank account number, deposits, payment orders and/or other payment transactions, payee details, payment instruments and the actions taken using them, deposits, withdrawals, etc.

3.1.5 Data relating to the reliability and performance assessment of the Data Subject – data on financial transactions, damage caused to the Bank, data necessary for the Bank to apply the necessary measures in the field of prevention of money laundering and terrorist financing and to ensure the enforcement of international sanctions, including to determine the purpose of the business relationship with the Data Subject and the fact whether the Data Subject is a politically exposed person as well as the source of origin of the assets, data on the parties to the transactions of the Data Subject, business activities, beneficial owners.

3.1.6 Data obtained and/or created in compliance with the requirements of legal acts – data which the Bank is required to provide to public authorities such as tax administrations, courts, law enforcement authorities, notaries, bailiffs, other executive authorities, including data on income, financial liabilities, owned property,

uncovered debts, data on the origin of funds, the country of residence for tax purposes, the status of the taxpayer and data on payment transactions and their execution.

3.1.7 Data collected by means of communication and other technical means – data which are provided in e-mails, photographs, video and/or audio recordings; data collected when the Data Subject visits the Bank's customer service departments or communicates with the Bank, data related to the Data Subject's visits to the Bank's websites or collected through the Bank's internet banking.

3.1.8 Data on behavioural habits, priorities and satisfaction with the Services – data on the activity using the Services, the Services provided to the Data Subject, personal settings in the Bank's Internet bank, feedback from the Data Subject on the Services, whether the Data Subject is satisfied with the Services.

3.1.9 Special categories of Personal Data – data related to the health of the Data Subject, biometric data (when performing remote identification, during which a unique identification of the person is confirmed, such as a facial image). The Bank shall use biometric data for remote identification of the Data Subject only when the Data Subject has expressly given his consent to the use of such an identification method by a service provider of this kind engaged by the Bank. In certain cases, in order to provide the Services, the Bank is required to process special categories of Personal Data.

3.1.10 Family data – information about the family of the Data Subject, his marital status, number of dependents, heirs, other related persons.

3.1.11 Data related to profession – data on education and professional activity.

3.1.12 Demographic data – country of residence, date of birth and nationality.

3.2 The Bank may also process other Personal Data of the Data Subject (voice and/or video data, such as recordings of conversations by telephone or other online means where the Data Subject chooses to communicate with the Bank by means of remote communication; court proceedings; data relating to the imposition of any sanctions, including data relating to any relevant business transactions or activities, including any possible publication of negative information in the media, etc.), in so far as this is necessary for the legitimate and defined purposes of the processing of Personal Data.

3.3 The Bank does not normally process Special Categories of Data (i.e. data relating to the health, ethnic origin, religious, political or philosophical beliefs, trade union membership, data concerning sex life or sexual orientation of Data Subjects), except where required by Applicable Law or in special cases, for example, where the Data Subject discloses such data himself in the course of using the Bank's services (by specifying it in a payment order or similar).

3.4 The Bank collects data on minors only if the minors use the Bank's Services or if the data on minors is provided to the Bank by the Data Subject on legitimate grounds when using any of the Bank's Services.

IV. PERSONAL DATA PROCESSING ACTIVITIES

4.1. Provision of Services

4.1.1. The main purpose of the processing of Personal Data by the Bank is to conclude, execute and administer agreements with the Data Subjects who use or intend to use the services of the Bank. For this purpose, Personal Data shall be processed on the following grounds, for the following purposes and to the following extent:

Basis	Aim	Personal Data processed and categories of Personal Data	Data storage term
Conclusion and performance of the contract (Article 6(1)(b) GDPR)	• to conclude service contracts, i.e. the scope of actions at the request of the Data Subject prior to the conclusion of a contract for entering into, performing or terminating a contract to which the Data Subject is a party; • to carry out remote identification of the Data Subject; • to execute domestic and international payments through financial institutions and payment systems, to provide other Services of the Bank;	**Identity and contact details of the person:** name, surname, personal identification number, date of birth, details of identity document (including the residence permit in the Republic of Lithuania or in an EU/EEA country), registration address, telephone number, e-mail address, residence address or address for correspondence, country of residence. Special categories of Personal Data – biometric personal data collected during remote identification, such as a facial photograph, video. The Bank shall use biometric data for remote identification of the Data Subject only when the Data Subject has expressly given his consent to the use of such an identification method by a service provider of this kind engaged by the Bank. Identification data – data of a person's identity document (including a residence permit in the	If the contract is concluded – 10 years after the end of the contract. In the absence of a contract, 1 year from the last day of communication with the Customer.

	• to carry out communication to the Data Subject, to grant and administer access to the Services.	Republic of Lithuania or in an EU/EEA country), photo, IP address, internet bank login data and other browsing information, including data on when and where the Bank's website was accessed, as well as the taxpayer's identification number. Data about the transactions of the Data Subject with the Bank and other agreements concluded – depending on the Services provided to the Data Subject by the Bank, the following data are processed: bank account number, deposits, payment orders and/or other payment transactions, means of payment and the operations carried out using them, data on the deposit, withdrawal of funds and other payment transactions. Data collected using communication and other technical means – data which are provided in e-mails, electronic messages (SMSes or other electronic means), photos, video and/or audio recordings; data collected when the Data Subject visits the Bank's customer service departments or communicates with the Bank, data related to the Data Subject's visits to the Bank's websites or collected through the Bank's internet banking.	
Compliance with legal requirements (Article 6(1)(c) of the GDPR)	• to identify and verify the identity of the Data Subject; • to ensure that Personal Data are correct and complete by verifying and correcting them using data from public registers and internal data sources (to carry out the "Know Your Customer" activities), i.e. identification of the person, determination whether the entity is a politically exposed person, determination of the origin of money, identification of the activities carried out, verification of the implementation of the applicable sanctions requirements; • to prevent, detect, investigate and report possible money laundering or terrorist financing activities. This objective includes monitoring and risk assessment of the entity's activities and payment transactions.	In addition to the above Personal Identity, Identification and Transaction Data of the Data Subject, the following Personal Data is collected and processed: Data relating to the reliability and performance assessment of the Data Subject – data on financial transactions, damage caused to the Bank, data necessary for the Bank to apply the necessary measures in the field of prevention of money laundering and terrorist financing and to enforce international sanctions, including, to determine the purpose of the business relationship with the Data Subject and whether the Data Subject is a politically exposed person, as well as the source of origin of the assets – such as the data on the parties to the transactions of the Data Subject, as well as the business activities, beneficial owners. Demographic data – country of residence, date of birth and nationality. For these purposes, we may contact you and ask you to provide us with additional information.	If the contract is concluded – 8 years from the end of the contract. In the absence of a contract, 1 year from the last day of communication with the Customer.

Compliance with legal requirements (Article 6(1)(c) of the GDPR)	• to carry out a creditworthiness or other risk assessment for the purpose of providing a loan or other Services, to limit risk and to meet capital adequacy requirements applicable to the Bank; • to comply with laws and regulations relating to record-keeping, responsible lending, information for tax administration purposes and risk management.	Financial data – data on the current/former workplace, economic-commercial activities carried out (for example, farmer, self-employment, etc.), data on accounts, assets held, transactions, loans, income, including projected income and their stability, expenses, liabilities, data on financial experience, credit history and creditworthiness, as well as data on the prohibition to conclude consumer credit agreements. Family data – information about the family of the Data Subject, his marital status, number of dependents, heirs, other related persons. Data related to profession – data on education and professional activity.	If the contract is concluded, for 3 years from the end of the contract. In the absence of a contract, 3 year from the last day of communication with the Customer.
Compliance with legal requirements (Article 6(1)(c) of the GDPR)	• to comply with the requirements of other legal acts (e.g. compliance with international tax data exchange requirements, collection and transmission of information at the request of supervisory authorities, law enforcement and other authorities).	Data obtained and/or created in compliance with the requirements of legal acts – data which the Bank is required to provide to public authorities such as tax administrations, courts, law enforcement authorities, notaries, bailiffs, other executive authorities, including data on income, financial liabilities, owned property, uncovered debts, data on the origin of funds, the country of residence for tax purposes, the status of the taxpayer and data on payment transactions and their execution.	10 years from the end of the contract with the Data Subject, unless other retention periods are established by the Applicable Legislation or the Bank's internal legislation.
Compliance with legal requirements (Article 6(1)(c) of the GDPR)	• to examine complaints and requests from customers and other data subjects.	Personal identification and contact details and other data relating to the complaint or request.	If the contract has been concluded – 10 years after the end of the contract. If the contract has not been concluded – for 1 year, counting from the last day of communication with the Customer.
Legitimate interest of the Bank (Article 6(1)(f) of the GDPR)	• to analyse, develop and improve the Bank's activities, Services and the Data Subject experience in conducting opinion polls, analysis and compiling statistics; • Ensuring and improving service quality; • Protecting the legitimate interests of the Customer, the Bank and/or the Bank's employees by implementing appropriate security measures; • prevent and investigate unauthorised use of the Services or disruption of the provision of the Services;	Data on behaviour habits, priorities and satisfaction with the Services – data on the activity using the Services, the Services provided to the Data Subject, personal settings in the Bank's Internet bank, feedback from the Data Subject on the Services, whether the Data Subject is satisfied with the Services. Also, the IP address, internet bank login data and other browsing information, including data on when and where the Bank's internet bank and/or website was accessed.	Period of the last 3 years.

	• to ensure the quality of the provision of the Services, the protection of information relating to the provision of the Services to the Customer, as well as to improve, develop and maintain the software, technical and information technology tools systems.		

4.2. Recording conversations

Basis	Aim	Personal Data processed and categories of Personal Data	Data storage term
With the consent of the Data Subject (Article 6(1)(a) of the GDPR)	Quality assurance of general consultations	Record of the conversation by telephone or other means of telecommunication. The Bank may also perform audio recording in the Customer Service Department of the Bank.	3 years from the date of the interview if the service is provided, or 1 year from the date of the interview if the service is not provided to the subject.
Conclusion and performance of the contract (Article 6(1)(b) GDPR)	provision of information to the Data Subject and answering questions.	Record of the conversation by telephone or other means of telecommunication. The Bank may also perform audio recording in the Customer Service Department of the Bank.	3 years from the date of the interview if the service is provided, or 1 year from the date of the interview if the service is not provided to the subject.

4.3. Video Surveillance

4.3.1. The Bank carries out video surveillance of the locations where the Services are provided. The locations where such video surveillance is carried out are marked with special signs containing information about the video surveillance and its purpose, the name of the Bank and its contact information.

Basis	Aim	Personal Data processed and categories of Personal Data	Data storage term
Legitimate interest in ensuring the security of the Bank's assets and the safety of its employees, visitors and their property (Article 6(1)(f) of the GDPR)	• To ensure security and preserving evidence of incidents. • video and/or audio recording information may be provided to law enforcement authorities where it is necessary for the investigation of criminal offences or violations, as well as to the service provider providing maintenance and security services for video surveillance equipment, which processes Personal Data on behalf of the Bank.	A facial image and video of the Customer's face while the Data Subject is inside or outside the premises.	21 days after the recording of such data or for as long as necessary for the purpose of processing.

4.4. Debt management

Basis	Aim	Personal Data processed and categories of Personal Data	Data storage term
Legitimate interest of the Bank (Article 6(1)(f) of the GDPR)	• Debt management, filing claims, demands, lawsuits; • Submission of customers' arrears documents to debt collection companies.	Customer's Personal Data, identification data, data on the Customer's assets, income, liabilities and other data related to the circumstances of debt formation.	10 (ten) years from the date of repayment of the debt.

4.5. Direct marketing, profiling and automated decision making

Basis	Aim	Personal Data processed and categories of Personal Data	Data storage term
With the consent of the Data Subject (Article 6(1)(a) of the GDPR)	• Conducting direct marketing.	Identity (name, surname) and contact details (e.g. e-mail address, telephone number) of the person. The Bank shall provide a free and easily implemented opportunity for the Data Subject to withdraw his consent to the use of his Personal Data for direct marketing purposes.	3 years from the receipt of the consent (please note that upon expiry of this period, the Bank may ask to extend the consent for a longer period), or until the receipt of a request to withdraw the consent or a request to delete data.
With the consent of the Data Subject (Article 6(1)(a) of the GDPR), i.e. additional consent is requested to the execution of direct marketing.	• Personalised offers – for this purpose, the Bank will carry out profiling actions with regard to the Data Subject in order to submit personally tailored offers to the Data Subject	Profiling is the processing of Personal Data by automated means for the purpose of assessing certain personal characteristics of the Data Subject and analysing or predicting, for example, his economic situation, personal preferences, interests, place of residence. Profiling is used for the purpose of carrying out the analysis necessary to provide the Data Subject with advice, for marketing purposes, for the improvement of information systems, for automated decision-making, for example, for credit scoring, risk management, transaction monitoring, and fraud prevention. The Bank also carries out profiling and automated decision-making in order to improve the experience of Data Subjects when using the Services, for example, when adapting the Services to devices or preparing Service offers relevant to Data Subjects. The Bank shall not take a decision on the characteristics of the Data Subject (creditworthiness, reliability, etc.) if such characteristics have been assessed only in an automatic manner, where such a decision may have legal consequences for the Data Subject or otherwise affect him, except in the following cases: (a) the decision is adopted in accordance with the procedure laid down by law;	3 years from the receipt of the consent (please note that upon expiry of this period, the Bank may ask to extend the consent for a longer period), or until the receipt of a request to withdraw the consent or a request to delete data.

		(b) the decision is adopted in the context of the conclusion or performance of a contract with the Data Subject. If the Bank assesses the Data Subject's characteristics automatically and the Data Subject disagrees with such assessment, the Data Subject shall have the right to express his opinion on the inappropriate assessment of his characteristics. The Bank shall take into account the views of the data subject and repeat the assessment non-automatically, if necessary.	

4.6. Other legal grounds and purposes for the processing of Personal Data

4.6.1. The Bank also processes Personal Data when it is necessary to protect the vital interests of the Data Subject or another natural person. On these grounds, Personal Data may be processed, for example, in the event of acute health problems or accidents, for health security, monitoring and alerting purposes, for the prevention or control of communicable diseases and other serious health threats.

4.6.2. The Bank is also obliged to fulfil other legal obligations, for example, the processing of the list of shareholders of the Bank, during which it receives and processes Personal Data such as the name, surname, personal identification number, residential address and the number of shares held by the shareholder.

V. COOKIES

5.1. The Bank uses cookies when the Data Subject visits the Bank's website. A list of the cookies used is provided in the Bank's Cookie Policy, which is published on the Bank's website.

VI. SOURCES OF OBTAINING PERSONAL DATA

6.1. Personal Data is collected and received directly from Data Subjects and is created when Data Subjects use or intend to use the Services.

6.2. The Bank collects Personal Data about Data Subjects who have entered into contracts with the Bank or have expressed their intention to do so directly from them, in particular, from Data Subjects, debtors, persons who ensure the proper performance of the obligations of the Data Subjects to the Bank. The Bank also collects Personal Data from potential customers, payers, trustees, insolvency administrators, intermediaries, representatives of legal entities, signatories, shareholders and other participants of legal entities, contact persons of the customer (legal entity), members of the board of directors, beneficial owners, and visitors of the Bank's customer service units, as well as representatives of Data Subjects, and heirs of Data Subjects.

6.3. Personal Data is also obtained from other sources:

- From private and public institutions and registers (for example, the Bank of Lithuania, the Ministry of Finance, the Ministry of the Interior, the State Social Insurance Fund Board, the State Sickness Fund, the National Paying Agency, the State Enterprise Centre of Registers, the State Enterprise Regitra, law enforcement agencies, other registers and public institutions);
- From entities administering joint debtors' data files (for example, UAB Creditinfo Lietuva);
- From other database managers (e.g. Scorify UAB);
- From other financial service providers;
- From legal persons, where the Data Subject is in one way or another related to these legal persons (for example, is a representative, employee, contractor, founder, shareholder, participant of these legal persons, etc.);
- From partners engaged by the Bank for the provision of its Services;
- From various other natural or legal persons, in fulfilment of contractual or legal requirements, documents provided to the Bank (for example, information in property valuation reports, certificates, etc.), as well as from the Data Recipients referred to in section 7 of the Policy;
- From natural persons when they provide data on spouses, children, other persons related by kinship or affinity, co-borrowers, guarantors, collateral providers, etc;
- From telephone conversations, video and/or audio recordings, correspondence received by email or other means of communication with the Data Subject.

VII. PROVISION OF PERSONAL DATA AND RECIPIENTS

7.1. The Bank's Personal Data processing activities also include the disclosure of Personal Data to Data Recipients such as public authorities, suppliers of the Bank, payment service providers and business partners. The Bank shall not disclose more Personal Data than is necessary for the purpose for which the Personal Data is provided and only in accordance with the requirements of the Applicable Laws and the legislation governing the protection of Personal Data.

7.2. The Data Recipients may process Personal Data in their capacity as Data Processors and/or Data Controllers. Where the Data Recipient processes Personal Data in its capacity as Data Controller, the Data Recipient shall be responsible for informing Data Subjects of such processing of Personal Data by it.

7.3. The Bank shall provide Personal Data to such Data Recipients as:

- Public bodies and institutions, and other persons performing the functions assigned to them by law (for example, law enforcement authorities, tax administration, supervisory authorities of the Bank, institutions carrying out financial crime investigation activities);
- Companies belonging to a banking group, such as subsidiaries;
- Partners engaged by the Bank for the provision of its Services;
- Other payment service providers in the event that the Bank is obliged to grant access to the Personal Data of the Data Subject to such payment service provider;
- Credit and financial institutions, correspondent banks, custodians, insurance providers and financial intermediaries, third parties involved in the execution, settlement and reporting cycle of trading in investment instruments;
- Persons providing financial and legal advice, auditing the Bank or providing other services to the Bank;
- Third parties who maintain registers (including, but not limited to, databases of financial obligations, the Population Register, the Register of Legal Entities, the Register of Contracts and Foreclosures, the securities registers, the Joint Debtors' Files, or any other registers in which Personal Data is processed) or who act as intermediaries in the provision of Personal Data from such registers, persons and companies involved in debt collection, administration of insolvency proceedings, bailiffs, notaries;
- Participants and/or parties involved in national, European and international payment systems;
- Persons who ensure the proper performance of the customer's obligations to the Bank, such as guarantors, guarantors, collateral providers;
- Other persons involved in the provision of the Services, such as providers of Customer remote identification services, providers of video surveillance, information technology, telecommunications, hosting, archiving, postal services, providers of services provided to the Data Subject, for the services provided by which the Data Subject orders electronic billing;
- To any person if the Data Subject has given consent to the disclosure of his data.

7.4. The Bank shall have the right to provide the Personal Data of the Debtors to the Data Controllers, which shall manage the joint data files of the Debtors (hereinafter the joint files). The Bank shall provide the Personal Data of debtors if the Bank has issued a written reminder to the Data Subject about the default and the outstanding debt has not been settled within 30 calendar days from the date on which the Bank sent (provided) the reminder to the Data Subject.

VIII. GEOGRAPHICAL AREA OF PROCESSING OF PERSONAL DATA

8.1. Personal Data is generally processed within the EU/EEA, but in certain cases it may be transferred and processed outside the EU/EEA.

8.2. Personal Data may be transferred and processed outside the EU/EEA where there is a legal basis for such transfer of Personal Data and where appropriate safeguards are in place. Examples of appropriate safeguards include:

- an agreement has been concluded containing standard terms and conditions approved by the European Commission, or the transfer is carried out in accordance with other accepted terms and conditions, such as codes of conduct, certificates, etc., which are approved under the General Data Protection Regulation;
- the non-EU/EEA country in which the recipient of the Personal Data is located ensures an adequate level of protection of Personal Data as decided by the European Commission.

IX. RIGHTS OF DATA SUBJECT

9.1. The Data Subject has the following rights guaranteed to him by the legislation governing the protection of Personal Data in relation to the processing of his Personal Data:

9.1.1. To request the rectification of his Personal Data if it is incorrect, incomplete or inaccurate;

9.1.2. To object to the processing of Personal data;

9.1.3. To request the erasure of his Personal Data, unless the law provides for the necessary retention of such Personal Data;

9.1.4. To restrict the processing of his Personal Data;
9.1.5. To receive information about the processing of his Personal Data and have access to his Personal Data processed;
9.1.6. To receive the Personal Data provided by him which is processed on the basis of his consent or for the performance of a contract, either in writing or in a standard computer-readable format, and, where possible, to transmit such data to another service provider (the right to data portability);
9.1.7. To withdraw your consent to the processing of his Personal Data (if the data is processed on the basis of consent);
9.1.8. To object to the application of a completely automated solution, including profiling, in respect of the subject, if the adoption of such solution has legal effects or a similar significant effect to the subject. This right shall not apply where such decision-making is necessary for the purposes of entering into or performance of a contract with the Data Subject, is permitted under Applicable Law or the Data Subject has expressly consented to it.
9.1.9. To lodge a complaint with the State Data Protection Inspectorate (for more information, see www.vdai.lrv.lt) if he considers that his Personal Data have been processed in violation of the Data Subject's rights/legitimate interests.

9.2. The right to the protection of Personal Data is not absolute and may be limited in certain circumstances. In this regard, the Customer will be provided with such information as the Bank may provide to the Data Subject to ensure that the exercise of the right of access to Personal Data does not adversely affect the rights and freedoms of others, including in relation to the protection of trade secrets, intellectual property and copyright protection for software. In cases where Applicable Laws provide, the Bank may delay or restrict the provision of information to the data subject or withhold it if it may hinder or impair the detection or investigation of unlawful acts or the enforcement of sanctions, infringe the rights and freedoms of other persons, endanger national security or public order, or hinder the investigation of the unlawful acts or the prosecution of the persons responsible for the acts.

9.3. If the Bank does not receive Personal Data from the Data Subject, it shall inform the Data Subject thereof. If the Bank intends to provide Personal Data to third parties, it must inform the Data Subject thereof, except where laws or regulations specify the procedure for collecting and providing such data and the recipients of the data.

X. EXAMINATION OF REQUESTS FROM DATA SUBJECTS

10.1. The Data Subject shall have the right to apply to the Bank in order to submit inquiries, withdraw the consents given, submit requests for the exercise of the Data Subject's rights and submit complaints regarding the processing of Personal Data.

10.2. The Bank shall also provide the Data Subject with the opportunity to change his preferences and to opt-out of the processing of Personal Data for the purposes of personalised offers and profiling for marketing purposes, where such processing of Personal Data is based on legitimate interest.

10.3. The Data Subject may change certain information, make choices or provide confirmations through online banking, at the Bank's customer service department or by calling the Bank.

10.4. The Bank's contact details are published on the Bank's website. The Customer may contact the appointed Data Protection Officer by email: data.protection@mano.bank or by phone +370 5 240 9389.

10.5. The Bank shall only examine a Data Subject's request if the identity of the requesting Data Subject can be established.

10.6. Upon receipt of the Data Subject's request, the Bank must respond and provide information on the actions taken upon receipt of the request in accordance with Clause 9.1 of the Policy no later than within one month from the date of the Data Subject's request. The information shall be provided to the Data Subject in writing, unless the Data Subject requests the information otherwise.

10.7. If the Bank decides not to act on the Data Subject's request, the Bank shall, no later than within one month of receipt of the request, inform the Data Subject of the reasons for not taking the requested action and the possibility of lodging a complaint with the State Data Protection Inspectorate.

10.8. Information about the processing of their Personal Data shall be provided to the Data Subjects free of charge. Where requests from the Data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Bank may:
10.8.1. Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
10.8.2. Refuse to act on the request.

10.9. The Data Subject shall have the right to lodge a complaint regarding the processing of Personal Data with the State Data Protection Inspectorate, whose website address is www.vdai.lrv.lt, if the Data Subject considers that his Personal Data is processed in violation of his rights and legitimate interests in accordance with the legal acts regulating the protection of Personal Data.

XI. FINAL PROVISIONS

11.1. The Bank shall periodically review and update the Policy in the light of changes in legal requirements and in the Bank's operations. The latest version of the Policy and previous versions of this Policy are published on the Bank's website.

11.2. Having made substantial changes to this Policy, the Bank will inform the Data Subjects through the usual channels of communication with the Data Subjects and will publish the latest version on its website,