PERSONAL DATA PROCESSING RULES

Mano Bankas cares about the privacy of its customers and personal data protection and therefore seeks to ensure a fair and transparent processing of personal data and comprehensively inform customers about the processing of their personal data.
These Personal Data Processing Rules (hereinafter **the Rules**) determine the key aspects relating to the processing of customer personal data by Mano Bankas. Please read these Rules carefully. Should you have any questions regarding the processing of your personal data, please contact us using the contact information provided in these Rules.

I. GENERAL PROVISIONS

1.1. The Rules on Personal Data Processing (hereinafter referred to as the "Rules") shall establish the principles of the processing of personal data by AB "Mano bankas" (hereinafter referred to as the "Bank"), the rights of the data subjects, the measures to ensure the security of the personal data, the procedure for the registration of the controller of the personal data in the State Register of Controllers of Personal Data, and the procedure for the provision of personal data.
1.2. The Rules have been drawn up in accordance with the General Data Protection Regulation (EU) 2016/679, the Law on Legal Protection of Personal Data of the Republic of Lithuania and other legal acts, as well as other legal acts regulating the processing and security of personal data.
1.3. Terms used in these Rules:
Data Subject means any natural person who uses, has used, has expressed an intention to use, or is in any other way connected with the services provided by the Bank, the users of these services or the business relationship with the Bank.
Data Processor means a natural or legal person who processes Personal Data on behalf of the Data Controller.

Data Controller means a natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of Personal Data. Where Personal Data is processed in accordance with these Rules, the Bank shall be deemed to be the Data Controller.

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

EU/EEA means European Union/European Economic Area.

Applicable Laws means 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 provision of payment services, lending, including provision of consumer loans, insurance and investment services and other financial activities.

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

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.

Data Recipient means a natural or legal person, government or other authority to which the Bank may disclose Personal Data. The categories of Data Recipients are set out in Section 11 of these Rules.

Services means any service, advice, product of the Bank provided or rendered at a customer service department, on the Bank's website, through the Bank's online banking, by telephone, video transmission or other means, and relating to savings, investments, lending, bank accounts, means of payment and payments.

Bank's website (homepage) - www.mano.bank, www.manopaskola.lt.

II. PRINCIPLES OF PROCESSING OF PERSONAL DATA

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

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 Bank's documented instructions, in

compliance with the necessary and sufficient security measures, and in accordance with the requirements of the legislation governing the protection of Personal Data.

2.2. The Bank's employees who process Personal Data are obliged to keep Personal Data as a secret, unless such Personal Data is intended for public disclosure. This obligation also applies after the end of the employment relationship.

2.3. The Bank shall ensure that Personal Data are processed in accordance with the following principles:

2.3.1. **Personal data is processed lawfully, transparently and fairly.**

Lawfulness of the processing of Personal Data - The Bank processes Personal Data only on a legal basis (see Part IV of the Rules).

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 their rights (e.g., to withdraw their 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 plain and simple language. The information shall be provided in writing or by other means, including, where appropriate, in electronic form.

2.3.2. **Personal data shall be collected and processed only for specified, explicit, expressed and legitimate purposes (see Part IV of the Rules)**.

2.3.3. **Minimising the processing of personal data.** The processed Personal Data and its scope must be proportionate and adequate for the purposes of the processing, i.e. the Personal Data processed by the Bank must not be excessive;

2.3.4. **Accuracy and relevance of Personal Data.** Personal Data must be accurate and, where necessary, updated;

2.3.5. **Temporariness of storage of Personal Data.** Personal Data shall be kept only for as long as necessary to achieve the purpose of the processing of Personal Data. The data shall be retained as long as the following conditions are met:

a) The Bank has a statutory obligation to process Personal Data;

and/or

b) The Bank has a legitimate business interest in processing Personal Data.

Personal data must be destroyed or made anonymous when they are no longer necessary for the purposes of their processing (except for data transferred to public archives).

2.3.6. **Security of personal data**. Personal data must be processed in a way that ensures their confidentiality and integrity.

III. THE BANK'S PERSONAL DATA PROCESSING ACTIVITIES

3.1. Collection of personal data and data sources

Personal Data is collected directly from Data Subjects, generated by the use of the Services by Data Subjects, and obtained from external data sources such as private and public institutions and registers (e.g., the Bank of Lithuania, the Ministry of Finance, the Lithuanian Agricultural Advisory Service, the Statistics Department, the State Social Insurance Fund Board, the National Health Insurance Fund, the National Paying Agency, the State Enterprise Centre of Registers, State Enterprise "Regitra", law enforcement authorities, other registers and state authorities), from persons administering joint debtor data files (e.g. UAB "Creditinfo Lietuva"), other database managers, from legal entities where the Data Subject is in one way or another related to these legal entities (e.g. is a representative, employee, contractor, founder, shareholder, participant, etc. of these legal entities), from various other natural or legal persons, in compliance with contractual or legal requirements, from documents provided to the Bank (e.g. information in property valuation reports, certificates, etc.), as well as from the Data Recipients referred to in Section 11 of the Rules. The Bank may also record telephone conversations, video and/or audio recordings, store correspondence received by email or otherwise document relationships and communications with the Data Subject.

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 clients, payers, trustees, insolvency administrators, intermediaries, representatives of legal persons,

signatories of documents, shareholders and other participants of legal persons, contact persons of a client (legal person), members of the board, beneficiaries, and visitors of the Bank's customer service units, as well as from the representatives of the Data Subjects and the Data Subjects' successors.

3.2. Personal data processed

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

Identity and contact details - name, surname, personal identification number, date of birth, identity document details, address, telephone number, email address, country of residence.

Financial data - data on accounts, assets held/possessed, transactions, deals, loans, income, liabilities, data on financial experience. This data is collected when the Services are provided to Data Subjects or the Data Subject has requested the provision of the Services.

Data relating to the reliability and performance assessment of the Data Subject - data relating to financial transactions, damage caused to the Bank, data necessary for the Bank to take the necessary measures in the field of the 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 whether the Data Subject is a person involved in politics, as well as the source of the origin of assets, such as the data on the counterparties to the Data Subject and the business activities of the Data Subject.

Data obtained and/or generated in compliance with legal requirements - data obtained in response to requests from law enforcement authorities, notaries, tax administrators, enquiries of courts and bailiffs, data on income, financial obligations, property holdings and outstanding debts.

Data collected by means of communication and other technical means - 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 online banking or applications.

Data on behavioural habits, preferences and satisfaction with the Services - data on activity of using the Services, the Services provided to the Data Subject, personal settings in the Bank's online bank or application, the Data Subject's feedback on the Services, the Data Subject's satisfaction with the Services.

Special categories of Personal Data - data relating to the health of the Data Subject, biometric data (in the case of remote identification which confirms the unique identification of a person, such as facial images or fingerprints). The Bank shall use biometric data for remote identification of the Data Subject only when the Data Subject has expressly consented to the use of such identification method. In certain cases, in order to provide the Services, the Bank is required to process special categories of Personal Data.

Family data - information about the Data Subject's family, heirs, other related persons.

Occupational data - data on education and occupation.

The Bank may also process other Personal Data of the Data Subject in the course of its business (voice and/or video data, such as recordings of telephone, Skype or other online conversations where the Data Subject chooses to interact with the Bank by means of remote communication; legal proceedings; data relating to the imposition of any sanctions, including data relating to any relevant business transactions or activities, including any possible disclosure of negative information in the media, etc.), provided that this is necessary for the fulfilment of the legitimate and specified purposes of the processing of Personal Data.

"Mano bankas" 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 the sex life or sexual orientation of the Data Subjects), except where required by law or in special cases, where, for example, the Data Subjects disclose the data themselves in the course of the use of the Bank's services (by indicating it in the purpose of a payment or similar).

3.3. Profiling and automated decision-making

3.3.1. 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, such person's economic situation, personal preferences, interests, or place of residence. Profiling is used to carry out the analysis necessary to provide the Data Subject with advice, for marketing purposes, for the improvement of information systems, for automated decision-making, such as credit scoring, risk management, transaction monitoring, fraud prevention.

The Bank also carries out profiling and automated decision-making to improve the Data Subjects' experience of the Services, e.g. by customising the Services to their devices or by designing Service offers that are relevant to Data Subjects.

3.3.2. The Bank shall not make a decision on the characteristics (creditworthiness, trustworthiness, etc.) of a Data Subject if such characteristics have been assessed only by automated means, where such a decision is likely to result in legal consequences for Data Subject or otherwise affect the Data Subject, except in the following cases:

(a) The decision is adopted in accordance with the statutory procedure;

(b) The decision is made in the context of the conclusion or performance of a contract with the Data Subject.

3.3.3. 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 or her opinion on the inadequacy of the assessment of his or her characteristics. The Bank shall take into account the views of the Data Subject and, if necessary, repeat the assessment non-automatically.

IV. LEGAL GROUNDS AND PURPOSES FOR PROCESSING PERSONAL DATA

4.1. Fulfilment of a contract

The main purpose of the Bank's processing of Personal Data is to enter into, perform and administer contracts with Data Subjects who are clients of the Bank. This processing of Personal Data includes the processing of Personal Data for the following purposes:

to take action at the request of the Data Subject prior to the conclusion of a contract, and in order to enter into, perform or terminate a contract to which the Data Subject is a party;

for making domestic and international payments through financial institutions and payment systems;

to communicate with the Data Subject, provide and administer access to the Services;

to ensure access to and control the use and operation of the Services.

4.2. Fulfilment of legal obligation

In order to ensure compliance with the Bank's legal obligations, the Bank is obliged to process Personal Data in accordance with the requirements of the Applicable Law. Such processing of Personal Data includes, for example, the processing of Personal Data to:

-determine and verify the identity of the Data Subject, ensuring that the Personal Data is correct and complete by verifying and correcting it by using data from public registers and internal data sources (to carry out "Know Your Customer" activities);

-prevent, detect, investigate and report possible money laundering or terrorist financing activities;

-to carry out 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;

-comply with laws and regulations relating to record-keeping, responsible lending, providing information for tax administration purposes and risk management;

-comply with the requirements of the legislation applicable to insurance activities;

-provide evidence of a commercial transaction or other business communication. For this purpose, the Bank records telephone conversations;

-investigate complaints from clients and other Data Subjects.

4.3. Legitimate interest

The Bank processes Personal Data of Data Subjects for legitimate interest purposes. Such processing of Personal Data is necessary for the legitimate interest of the Bank, which, in the Bank's assessment, overrides the Data Subject's interest relating to his or her right to privacy. Such processing of Personal Data includes, for example, the processing of Personal Data to:

- offer and provide the Data Subject with additional Services and the services of carefully selected partners and personalised offers;

- analyse, develop and improve the Bank's activities, the Services and the Data Subject's experience by conducting opinion surveys, analysis and statistics;

- organise and carry out promotions and campaigns for Data Subjects;

- protect the legitimate interests of a Client, the Bank and/or the Bank's employees by implementing appropriate security measures;
- maintain relationships with Data Subjects;
- prevent and investigate unauthorised use of the Services or disruption to the Services;
- ensure the quality of the provision of Services, the protection of information related to the provision of Services to a Client, as well as to improve, develop and maintain the software, systems of technical and information technology tools;
- carry out creditworthiness or other risk assessment for the purpose of providing a loan or other Services to a legal entity, and to maintain a relationship with such legal entity;
- make, pursue and defend legal claims.

4.4. Consent

In certain cases, the Bank asks for the Data Subject's consent to process their Personal Data. Such request shall include information about the Personal Data processing activities for which consent is requested. For example, the Bank processes the Personal Data of the Data Subject for the purpose of direct marketing and carries out the recording of telephone conversations in order to ensure the quality of the Services provided and to protect the interests of the Bank and the Data Subject, on the basis of the consent given by the Data Subject for such processing of Personal Data. The Data Subject may withdraw the consent given at any time and shall be informed of the consequences of such withdrawal.

For direct marketing purposes, Personal Data may be processed subject to the consent of the Data Subject (Annex 7), except for the exceptions provided for by law. The Bank shall provide the Data Subject with a clear, free and easily enforceable opportunity to withdraw his/her consent to the use of his/her Personal Data for direct marketing purposes.

4.5. Other legal bases for processing of Personal Data

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

V. RIGHTS OF DATA SUBJECTS

5.1. The Data Subject shall have the following rights guaranteed to him/her by the legislation governing the protection of Personal Data in relation to the processing of his/her Personal Data:

5.1.1. to request the rectification of his or her Personal Data if it is incorrect, incomplete or inaccurate;

5.1.2. to object with the processing of his/her personal data;

5.1.3. to request the erasure of his or her Personal Data;

5.1.4. to restrict the processing of his or her Personal Data;

5.1.5. to receive information about the processing of his/her Personal Data and to have access to his/her Personal Data being processed;

5.1.6. to receive the Personal Data provided by him/her which is processed on the basis of his/her 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);

5.1.7 to withdraw your consent to the processing of your Personal Data (if the data is processed on the basis of consent);

5.1.8. to object to being subject to a fully automated decision, including profiling, where such decision-making has legal implications or similar significant effects for the Data 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.

5.2. If the Bank does not receive personal data from the Data Subject, the Bank shall inform the Data Subject thereof. If the Bank intends to provide Personal Data to third parties, it is obliged to 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.

VI. EXAMINATION OF DATA SUBJECTS' REQUESTS

6.1. The Data Subject shall have the right to contact the Bank to make enquiries, to withdraw given consent, to submit requests for the exercise of the Data Subject's rights and to lodge complaints regarding the processing of Personal Data.

The Bank shall also provide the Data Subject with the possibility to change his/her preferences and to refuse 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.

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

The Bank's contact details are published on the Bank's website. The client may contact the designated data protection officer by email: **data.protection@mano.bank.**

6.2. The Bank shall only process Data Subject's request if the identity of the requesting Data Subject can be established.

6.3. The Bank, upon receipt of the Data Subject's request, shall respond and provide information on the actions taken upon receipt of the request in accordance with Paragraph 5.1 of the Rules 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.

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

6.5. Information to Data Subjects about the processing of their Personal Data is provided free of charge. Where the Data Subject's requests are manifestly unfounded or disproportionate, in particular because of their repetitive content, the Bank may:

(a) charge a reasonable fee, taking into account the administrative costs for providing the requested information or the notifications or actions; or

(b) may refuse to act on the request.

6.6. 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 or her Personal Data is being processed in violation of his or her rights and legitimate interests under the legislation governing the protection of Personal Data.

VII. PERIOD OF RETENTION OF PERSONAL DATA

7.1. Personal Data shall not be processed for longer than is necessary for the purposes for which the Personal Data was collected or as required by applicable laws or the Personal Data Protection Laws. In the event that the business relationship with the Data Subject has ended, the Bank shall continue to process Personal Data for the purpose of asserting, exercising and defending legal claims. Personal data may be stored for the protection of Bank's legitimate interest, as well as to comply with Applicable Law. Personal data shall be retained by the Bank for 10 years from the end of the business relationship with the Data Subject, unless the Applicable Laws or the Bank's internal regulations provide for different retention periods.

7.2. In the event that the Bank refuses to provide a financial service in accordance with the Data Subject's request, the Data Subject's data shall be retained for no longer than **12 months.**

7.3 Video/audio of the Bank's premises shall not be processed for more than **21 days** after the recording of such data or for as long as it is necessary for the purpose of processing.

7.4. Recordings of conversations shall be kept by the Bank for 3 years from the date of the conversation if the service was provided, or for **1 year** from the date of the conversation if the service was not provided to the Client.

7.5. Personal data contained in the archived documents of the Bank shall be stored for archiving purposes for a period specified by the Office of the Chief Archivist of Lithuania, which may be longer than the retention periods specified in this Section of the Rules.

VIII. COOKIES

The Bank uses cookies when a 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.

IX. VIDEO SURVEILLANCE

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.

The Personal Data processed by the Bank in the context of video surveillance includes the Client's facial image and video footage of the Data Subject inside or outside the premises. The Bank may also carry out audio recording at the Bank's customer service department.

The Bank's processing of Personal Data through video surveillance is based on a legitimate interest in ensuring the safety of employees and clients and the protection of the Bank's assets. Video and/or audio information may be provided to law enforcement authorities where it is necessary for the investigation of criminal offences or violations, as well as made available to a video surveillance equipment maintenance and security service provider that processes Personal Data on behalf of the Bank.

X. RECORDING OF CONVERSATIONS

The Bank may record conversations of clients and potential customers requesting financial services provided by the Bank and other Data Subjects.

XI. PROVISION OF PERSONAL DATA AND DATA RECIPIENTS

11.1. The Bank's Personal Data processing activities also include the disclosure of Personal Data to recipients such as public authorities, the Bank's suppliers, 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 compliance with the requirements of the Applicable Laws and the legislation governing the protection of Personal Data.

11.2. 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.

11.3. The Bank provides Personal Data to Data Recipients such as:

-government bodies and institutions, and other persons exercising functions assigned to them by law (e.g. law enforcement authorities, tax administration, banking supervision, financial crime investigation authorities);

-Companies belonging to the Bank Group, such as subsidiaries;

-other payment service providers in case 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 services 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 databases of financial obligations, the Population Register, the Register of Legal Entities, securities registers, joint debtors' files or other registers in which Personal Data are processed) or who act as intermediaries in the provision of Personal Data from such registers, persons and companies involved in the collection of debts, the 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 client's obligations to the Bank, such as guarantors and collateral providers;

-other persons related to the provision of the Services, such as providers of video surveillance, information technology, telecommunications, hosting, archiving, mailing services, providers of services to the Data Subject for which the Data Subject subscribes electronic invoices.

11.4. The Bank shall have the right to provide Personal Data of debtors to data controllers processing joint debtor data files (hereinafter referred to as “Joint Files”).

XII. Geographical area of personal data processing

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

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:

-a contract 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;

-the recipient is certified in accordance with the requirements of the Data Protection Agreement between the EU and the United States of America (USA) (also known as the "Privacy Shield") (applicable for recipients located in the USA).

XIII. FINAL PROVISIONS

The Bank shall review and update the terms and conditions, for example, when Personal Data is processed for new purposes, additional categories of Personal Data are collected, or Personal Data are provided to recipients of Personal Data other than those specified above. The latest version of the Principles is published on the Bank's website.