finora bank

| | |
|---|---|
| DOCUMENT TITLE | PRIVACY POLICY (PUBLIC) |
| DRAFTED BY | DATA PROTECTION OFFICER |
| APPROVED BY | MANAGEMENT BOARD |
| RESPONSIBLE FOR IMPLEMENTATION | DATA PROTECTION OFFICER |
| DATE OF APPROVAL | 2024.09.06 |
| EFFECTIVE SINCE | 2024.09.06 |
| NEXT REVISION DATE | 2026.01.14 |
| REVISION NO. | III. |

# FINORA BANK UAB
# PRIVACY POLICY

**(PUBLIC)**

## 1. GENERAL

**1.1.** This Privacy Policy (hereinafter referred to as the "**Policy**") governs key principles of personal data processing at Finora Bank UAB (hereinafter referred to as the "**Bank**" or "**we**"), lists the rights of Customers and explains, how these rights may be enforced and exercised, as well as explains what measures are applied to maintain security of personal data.

**1.2.** We will apply this Policy when a customer relationship is established between us (hereinafter referred to as the "**Customer**", or **"you"**), or when you use, have used or intend to use our Services, use our Website, our Digital Channels or visit our Office.

**1.3.** Your personal data shall be processed in accordance with the EU General Data Protection Regulation (**GDPR**), 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.

**1.4.** This Policy applies when a Customer:

**1.4.1.** uses, has used or has expressed an intention to use or interest in using the services or products of the Bank;

**1.4.2.** visits our Website;

**1.4.3.** is a principal, founder, partner, management official, ultimate beneficial owner, shareholder, member of the board of directors or other management body;

**1.4.4.** Is a proxy or representative of the Customer (whether corporate or private);

**1.4.5.** is indirectly related to our services (e.g. is the Customer's spouse, collateral provider, guarantor, seller of the leased object (property), the data was provided by the Customer, etc.);

**1.4.6.** is an agent of any third party who is engaged in the legal relationships with the Bank (by way of example, an agent of a company that provides services or sells goods to the Bank);

**1.4.7.** has provided his/her Personal Data or the Bank has received Personal Data for other legitimate reasons (for example, Personal Data of third parties in documents submitted to the Bank by the Customer, etc.).

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

**1.5.1.** **Personal Data** means any information that allows direct or indirect identification of the Customer.

**1.5.2. Bank's website (homepage)** – https://finorabank.eu/en/.

**1.5.3. 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.

**1.5.4. DPO** means Data Protection Officer.

**1.5.5. Customer** 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).

**1.5.6. Finora Bank, or Bank, or Data Controller** means Finora Bank, UAB, a private limited liability Finora Bank, which is a licensed financial institution, holding specialised bank licences issued by the ECB, established and operating under the laws of the Republic of Lithuania, code: 305156796, address: Žalgirio str. 90, LT-09303 Vilnius, the Republic of Lithuania, including its Estonian branch.

**1.5.7. Group** means Finora global group of companies, consisting of Finora Bank UAB, Finora Bank UAB Estonian branch, AS Finora Group.

**1.5.8. Services** mean any service, advice, product of the Bank provided or rendered at Bank's office, on the Bank's website, using the Bank's internet banking, telephone, video transmission or other means.

**1.5.9. 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 and other financial activities.

**1.5.10.** All other terms used in the Policy shall be understood as defined in the GDPR and the Law on the Legal Protection of Personal Data of the Republic of Lithuania, Personal Data Protection Act of the Republic of Estonia and other Applicable laws.

## 2. PRINCIPLES OF PERSONAL DATA PROCESSING

**2.1.** When processing your Personal Data, the Bank shall comply with the following principles:

**2.1.1.** The Personal Data shall be processed lawfully, legally, reasonably, transparently and fairly.

**2.1.2.** Personal Data shall be collected and processed only for specified, explicit and legitimate purposes.

**2.1.3.** Minimisation of Personal Data processed.

**2.1.4.** Accuracy and relevance of Personal Data.

**2.1.5.** Limited retention of Personal Data.

**2.1.6.** Personal Data Safety and Security.

## 3. TYPES OF PERSONAL DATA PROCESSED

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

| Data category | Description |
|---|---|
| **Personal identity data 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 Republic of Estonia or in other EU/EEA country), registration address, telephone number, e-mail address, address of residence or address for correspondence, country of residence, country of tax residency. |

finora bank

| | |
|---|---|
| **Identification / ID documents data** | Details of person's ID document (including a residence permit in the Republic of Lithuania or Republic of Estonia or in other EU/EEA country), photo. |
| **Family data** | Information about the family of the Customer, his/her marital status, number of dependents, spouse, heirs, other related persons. |
| **Data related to occupation, profession, qualifications and competences** | Data on education and professional activity, occupation, employment, qualification, trainings, competences, roles. |
| **Financial data** | Data on the current/former employment / job / position, activities carried out (for example, farmer, self-employment, etc.), data on accounts, IBAN, Payment reference (if contains identifiable info), tax ID, assets held, transactions, loans, income, including projected income and their stability, expenses, liabilities, data on financial experience, credit history and creditworthiness. |
| **Agreement and transactional data** | Depending on the Services provided to the Customer by the Bank: bank account number, deposits, payment orders and/or other payment transactions, payee details, payment instruments and the actions taken using them, deposits, withdrawals, etc. |
| **Browsing data, teclhnical data** | Browser data, cookie IDs, pixel IDs, IP address, and other browsing information, including data on when and where the Bank's website was accessed, as well as the taxpayer's identification number. |
| **Credit risk, credit score and performance assessment of the Customer** | Data on financial transactions, data necessary for the Bank to apply the necessary measures in the field of AML / CTF and to enforce national, regional and international sanctions, including, to determine the purpose of the business relationship with the Customer and whether the Customer is a politically exposed person (PEP), as well as the source of origin of wealth / source of the assets – such as the data on the parties to the transactions of the Customer, as well as the business activities, products, subject matter of the transactions, key decision makers, management members, ultimate beneficial owners (UBOs). |
| **Data collected in compliance with the legal requirements** | 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. |
| **Data collected by communication and other technical means** | Data provided in e-mails, photographs, video and/or audio recordings; data collected when the Customer visits the Bank's customer service departments or communicates with the Bank, data related to the Customer's visits to the Bank's websites or collected through systems used by the Bank. |
| **Behavioural data, habits, priorities, satisfaction** | Data on the activity using the Services, the Services provided to the Customer, feedback from the Customer on the Services, whether the Customer is satisfied with the Services. |
| **Special categories of Personal Data** | Data related to the health of the Customer, 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 Customer only when the Customer 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. |
| **Demographic data** | Country of residence, date of birth and nationality. |
| **Voice / visual data** | The Bank may also process other Personal Data of the Customer (voice and/or video data; court proceedings; data relating to the imposition of any sanctions, including data relating to any relevant business transactions or activities, including 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. |

**3.2.** The Bank usually does not 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 Customers), except where required by Applicable Law or in special cases, for example, where the Customer discloses such data himself/herself in the course of using the Bank's services (by specifying it in a payment order or similar).

**3.3.** 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 Customer on legitimate grounds when using any of the Bank's Services.

## 4. PERSONAL DATA PROCESSING ACTIVITIES

### 4.1. Onboarding of the Customers for the Services of the Bank

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Conclusion and performance of the contract (Article 6(1)(b) GDPR)** | to conclude agreement on the Services of the Bank;<br><br>to carry out remote verification / identification of the Customer;<br><br>to provide other Services of the Bank;<br><br>to carry out communication to the Customer, to grant and administer access to the Services. | Identity and contact details of the person.<br><br>Special categories of Personal Data.<br><br>Identification data.<br><br>Transactional data with the Bank and other agreements concluded.<br>Data related to the mortgaged assets.<br><br>Data collected using communication and other technical means.<br><br>Bank's website browsing data.<br>Data of interaction with the Bank IT systems and tools | If the contract is concluded – 10 years after the expiry 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 identify and verify the identity of the Customer;<br><br>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" procedures), 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;<br><br>to prevent, detect, investigate and report | In addition, the following Personal Data is collected and processed:<br><br>Credit risk assessment data.<br><br>Demographic data.<br><br>For these purposes, we may also contact you and ask you to provide us with additional information. | If the contract is concluded – 8 years from the expiry of the contract. In the absence of a contract, 1 year from the last day of communication with the Customer. |

| | | | |
|---|---|---|---|
| | possible money laundering or terrorist financing activities. This objective includes monitoring and risk assessment of the entity's activities and payment transactions. | | |
| **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;<br><br>to comply with laws and regulations relating to record-keeping, responsible lending, information for tax administration purposes and risk management. | Financial data.<br>Family data.<br><br>Data related to occupation, profession, qualifications and competences. | If the contract is concluded, for 3 years from expiry of the contract. In the absence of a contract, 3 years 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, tax authorities, law enforcement, regulatory and other authorities). | Data collected and/or created in compliance with the requirements of legal acts. | 10 years from the expiry of the contract with the Customer unless other retention periods are established by the Applicable Legislation or the Bank's internal legislation. |

### 4.2. Provision of the Services

**4.2.1.** The main purpose of the processing of Personal Data by the Bank is to prepare, draft, execute and exercise the conduct under the agreements with the Customers 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:

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Conclusion and performance of the contract (Article 6(1)(b) GDPR)** | to conclude agreement on the Services of the Bank;<br><br>to carry out remote verification / identification of the Customer; | Identity and contact details of the person.<br><br>Special categories of Personal Data.<br><br>Identification data. | If the contract is concluded – 10 years after the expiry of the contract.<br><br>In the absence of a contract, 1 year from the last day of communication with the Customer. |

| | | | |
|---|---|---|---|
| | to provide other Services of the Bank;<br><br>to carry out communication to the Customer, to grant and administer access to the Services. | Transactional data with the Bank and other agreements concluded.<br><br>Payment data related to payment services.<br><br>Current account data.<br><br>Data related to deposits held with the Bank.<br><br>Data related to the mortgaged assets.<br><br>Data collected using communication and other technical means.<br><br>Bank's website browsing data.<br><br>Data of interaction with the Bank IT systems and tools | 8 years after the end of relationship for AML purposes |
| **Compliance with legal requirements (Article 6(1)(c) of the GDPR)** | to identify and verify the identity of the Customer;<br><br>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" procedures), 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;<br><br>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, the following Personal Data is collected and processed:<br><br>Credit risk assessment data.<br><br>Demographic data.<br><br>For these purposes, we may also contact you and ask you to provide us with additional information. | If the contract is concluded – 8 years from the expiry of the contract. In the absence of a contract, 1 year from the last day of communication with the Customer. |

finora bank

| | | | |
|---|---|---|---|
| **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;<br><br>to comply with laws and regulations relating to record-keeping, responsible lending, information for tax administration purposes and risk management. | Financial data.<br><br>Family data.<br><br>Data related to occupation, profession, qualifications and competences. | If the contract is concluded, for 3 years from expiry of the contract. In the absence of a contract, 3 years 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, tax authorities, law enforcement, regulatory and other authorities). | Data collected and/or created in compliance with the requirements of legal acts. | 10 years from the expiry of the contract with the Customer unless other retention periods are established by the Applicable Legislation or the Bank's internal legislation.<br><br>8 years after the end of relationship for AML purposes |
| **Compliance with legal requirements (Article 6(1)(c) of the GDPR)** | to examine complaints and requests from customers. | Personal identification and contact details and other data relating to the complaint or request. | If the contract has been concluded – 10 years after the expiry 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 to ensure smooth operations of the Bank and improve Bank's activities (Article 6(1)(f) of the GDPR)** | to analyse, develop and improve the Bank's activities, Services and the Customer experience in conducting opinion polls, analysis and compiling statistics;<br><br>Enhancing and improving service quality;<br><br>Protecting the legitimate interests of the Customer, the Bank and/or the Bank's employees or third parties by implementing appropriate security measures;<br><br>prevent and investigate unauthorised use of the Services or disruption of the | Behavioural data, habits, priorities, satisfaction. | Period of the last 3 years. |

| | | | |
|---|---|---|---|
| | provision of the Services, prevent fraud, scams and related illegal activities;<br><br>to ensure the quality of the provision of the Services, security of information relating to the provision of the Services to the Customer, as well as to improve, develop and maintain the information technology systems. | | |

### 4.3. Debt collection, recovery and management

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| Legitimate interest of the Bank to defend its rights (Article 6(1)(f) of the GDPR) | Debt management, filing claims, demands, lawsuits;<br><br>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. |

### 4.4. Marketing

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **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.<br><br>Online identifiers (cookie IDs, pixel IDs), IP address, interaction with ads and website | 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. |

### 4.5. IT security and communications

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Legitimate interest of the Bank to prevent disruption of Bank's activities (Article 6(1)(f) of the GDPR)** | Enforcement of IT security and cybersecurity policies, monitor, prevent, detect, investigate, and respond to cyber threats around the clock | Data collected using communication and other technical means.<br><br>Bank's website browsing data.<br><br>Data of interaction with the Bank IT systems and tools | Up to as longs as is required under the Finora IT security policies, depending on the security event and control. |

### 4.6. Accounting, tax administration, other

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Compliance with legal requirements (Article 6(1)(c) of the GDPR)** | Complying with legal obligations and requirements of legal acts (Article 6(1)(c) of the GDPR):<br>accounting, taxes, other public obligations;<br>prevention of money laundering;<br>protection of consumer rights;<br>product safety;<br>information security;<br>other areas relevant for us. | First name, surname, address, personal ID number, VAT number (when a person is registered as a VAT payer), data about the Service (Service description;<br>price/amount/interest paid), issued accounting documents and their details, source of income, business earnings, other accounting and tax data that we must collect, process and store under laws and other legal acts. | Up to 10 years after invoicing or relevant accounting event. |

### 4.7. Transfer of Bank's business or getting funding for its activities

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Legitimate interest of the Bank to assess the possibility to transfer Bank's business of part thereof of get funding for Bank's activities (Article 6(1)(f) of the GDPR)** | to assess the possibility to transfer Bank's business of part thereof of get funding for Bank's activities (including legal due diligence of the Bank in such cases) | Customer's Personal Data, identification data, data on the Customer's assets, income, liabilities and other data necessary to assess Bank's customers' portfolio and Bank's business. | Until the decision not to buy/ invest is made; if the business is transferred/ investment is made, 10 (ten) years from the date of such decision. |

### 4.8. Statistics, analytics, Customer behaviour research

**4.8.1.** In order to monitor, evaluate, analyse, improve and further the quality of Services provision, Website, offer new Services or new quality Services, increase the availability of Services, improve the security of use of the Services, improve user experience when using the Services, we analyse various statistical data.

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **Our legitimate interest to improve Bank's activities (Article 6(1)(f) of the GDPR).** | to analyse data, install and use data analysis and processing modules and methods in order to create, increase value both for you as a customer and for our business. | Agreement and transactional data<br>Service usage history, browsing, IP data, etc. | No longer than 36 months after the data is generated. |

**4.8.2.** We use **automated data analysis** tools based on the latest scientific achievements to conduct these data research, introduce and use data analysis and processing modules and methods.

**4.8.3.** Data analysis actions, performed for the purposes described in this chapter, do not have any legal or comparable significant effect on you.

**4.9. Recruitment**

| Legal basis | Purpose | Categories of Personal Data | Retention |
|---|---|---|---|
| **With the consent of the Data Subject (Article 6(1)(a) of the GDPR).**<br>**Consent is expressed by submitting candidate's job application containing personal data** | Select suitable candidates for vacant positions | Identity (name, surname) and contact details (e.g. e-mail address, telephone number) of the person.<br>Other data provided in candidate's CV, motivation letter, communication with the candidate via email or Linkedin, publicly available information (LinkedIn account data, other information found by internet search) and other information provided by candidate. | For the period of recruitment procedure regarding particular vacant position. |

**4.9.1.** Without the submission of candidate's personal data, the Bank will not be able to assess candidate's suitability for vacant position.

**4.9.2.** Candidates are advised not to provide excessive information to comply with personal data protection requirements.

**4.9.3.** The Bank may contact candidate's former employers that were indicated for their recommendations and may ask them about candidate's professional skills and qualifications. The Bank may request this information from the current employer of the candidate only after receiving candidate's separate consent.

**4.9.4.** In fulfilment of the legal obligation stipulated in the Law on Banks of the Republic of Lithuania, the Bank may ask the selected candidates to provide information related to their criminal record.

**4.10. Other cases when the Bank may be processing Personal Data**

**4.10.1.** The Bank also processes Personal Data where it is necessary to protect the vital interests of the Customer 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 and safety at work, occupation and professional risk management, monitoring and alerting purposes, for the prevention or control of communicable diseases and other serious health threats.

**4.10.2.** The Bank is also obliged to fulfil other legal obligations, for example, processing of the list of shareholders of the Bank, processing of data related to the management members, processing of the data related to the Finora Group companies and their management members, 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 and other related information.

## 5. SOURCES OF OBTAINING PERSONAL DATA

**5.1.** Personal Data is collected and received directly from Customers and is created when Customers use or intend to use the Services.

**5.2.** The Bank collects Personal Data about Customers who have entered into contracts with the Bank or have expressed their intention to do so directly from them, in particular, from Customers, debtors, persons who ensure the proper performance of the obligations of the Customers 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 Customers, and heirs of Customers.

**5.3.** Personal Data is also obtained from other sources:

**5.3.1.** 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, tax authorities, law enforcement agencies, other registers and public institutions);

**5.3.2.** From public registries and information systems;

**5.3.3.** From credit bureau and credit scoring providers (for example, UAB Creditinfo Lietuva);

**5.3.4.** From other database managers;

**5.3.5.** From other financial service providers;

**5.3.6.** From legal entities, where the Customer is related to these legal entities (for example, is a representative, employee, contractor, founder, shareholder, participant of these legal persons, etc.);

**5.3.7.** From partners engaged by the Bank for provision of its Services;

**5.3.8.** 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 7of the Policy;

**5.3.9.** From natural persons when they provide data on their family members, relatives, spouses, children, other persons related by kinship or affinity, co-borrowers, guarantors, collateral providers, etc.

**5.3.10.** From telephone conversations, video and/or audio recordings, correspondence received by email or other means of communication with the Customer.

**5.3.11.**

## 6. PERSONAL DATA RECIPIENTS

**6.1.** The Bank's Personal Data processing activities also include the disclosure of Personal Data to Data Recipients such as public authorities, service providers, vendors and 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.

**6.2.** 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 Customers of such processing of Personal Data by it.

**6.3.** The Bank has involved various service providers (e.g. providers of server hosting, data centres, cloud computing, support, IT, payment, identity verification, document validity verification, intermediation, payments, audit, accounting, legal, tax advisory services, administration of damages, debt collection, analytics, direct marketing, e-mail, SMS messaging, customer service, call centre and other services). Data processors can process your personal data only according to our instructions. Besides, they must ensure security of your data in accordance with applicable legal acts and agreements concluded with us.

**6.4.** The Bank shall provide Personal Data to Data Recipients, which act as independent data controllers, such as:

**6.4.1.** 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);

**6.4.2.** Finora Group companies;

**6.4.3.** Partners engaged by the Bank for the provision of its Services;

**6.4.4.** Other payment service providers in the event that the Bank is obliged to grant access to the Personal Data of the Customer to such payment service provider;

**6.4.5.** Credit and financial institutions, correspondent banks, payment service providers, custodians, insurance providers and financial intermediaries;

**6.4.6.** Persons providing financial and legal advice, auditing the Bank or providing other services to the Bank;

**6.4.7.** Third parties who maintain registers (including, but not limited to, databases of financial obligations, the State Enterprise Centre of Registers, 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;

**6.4.8.** Participants and/or parties involved in national, European and international payment systems;

**6.4.9.** Persons who ensure the proper performance of the customer's obligations to the Bank, such as guarantors, guarantors, collateral providers;

**6.4.10.** potential purchasers of claim rights and collection service providers;

**6.4.11.** 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 Customer, for the services provided by which the Customer orders electronic billing;

**6.4.12.** To any person if the Customer has given consent to the disclosure of his data.

**6.5.** If necessary and legally justified, we also provide your data to service providers that are separate data controllers, also to competent authorities, institutions, organisations, also other data controllers who are entitled to receive information in accordance with applicable legal acts and/or our legitimate interests (Article 6(1)(b) of the GDPR, Article 6(1)(c) of the GDPR, Article 6(1)(e) of the GDPR, Article 6(1)(f) of the GDPR).

**6.6.** The Bank shall have the right to provide the Personal Data of the debtors to the Data Controllers, which manage the data files of the debtors. The Bank shall provide the Personal Data of debtors if the Bank has issued a written reminder to the Customer 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 Customer.

## 7. GEOGRAPHICAL AREA OF PROCESSING OF PERSONAL DATA

**7.1.** Personal Data is generally processed within the EU/EEA, but in certain cases it may be transferred and processed outside the EU/EEA. Data processors we use are usually located in the Member States of the European Union or store data entrusted to them by the Bank in the European Union. Only a few carefully selected data processors process data outside the European Union. In addition, when we manage our social media accounts, we receive and provide data to social network platform operators, which may also operate outside the European Union, e.g. in the USA. We closely follow practices of data protection supervisory authorities and the guidelines on the transfer of data outside the European Union, and we diligently consider conditions, under which data are transferred and may be subsequently processed and stored after the transfer outside the European Union. To ensure an adequate level of security of data and to guarantee legitimate transfer of data, we conclude Standard Contractual Clauses approved by the European Commission for data transfer outside the European Economic Area (EEA) or follow other grounds and conditions set out in the GDPR.

**7.2.** 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:

**7.3.** 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.

**7.4.** 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.

**7.5.** More information regarding the transfer of Personal Data outside the EU/EEA may be provided upon request using contact details indicated in Section 11 of this Policy.

## 8. YOUR RIGHTS AS A DATA SUBJECT

**8.1.** You have the following rights guaranteed to you by the legislation governing the protection of Personal Data in relation to the processing of your Personal Data:

**8.1.1.** to request the rectification of your Personal Data if it is incorrect, incomplete or inaccurate;

**8.1.2.** to object to the processing of Personal data;

**8.1.3.** to request the erasure of your Personal Data, unless the law provides for the necessary retention of such Personal Data;

**8.1.4.** to restrict the processing of your Personal Data;

**8.1.5.** to receive information about the processing of your Personal Data and have access to your Personal Data processed;

**8.1.6.** to receive the Personal Data provided by you which is processed on the basis of your 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);

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

**8.1.8.** to object to the application of a completely automated solution, including profiling, in respect of you, if the adoption of such solution has legal effects or a similar significant effect to you. This right shall not apply where such decision-making is necessary for the purposes of entering into or performance of a contract with you, is permitted under Applicable Law or you have expressly consented to it.

**8.1.9.** to lodge a complaint with the State Data Protection Inspectorate of the Republic of Lithuania or the Data Protection Inspectorate of the Republic of Estonia (for more information, see www.vdai.lrv.lt or www.aki.ee) if you consider that your Personal Data have been processed in violation of your rights/legitimate interests.

**8.2.** The rights of data subjects are not absolute and may be limited in certain circumstances. In this regard, you will be provided with such information as the Bank may provide to you 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 you 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.

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

## 9. DATA SUBJECT REQUESTS

**9.1.** The Customer 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 Customer's rights and submit complaints regarding the processing of Personal Data.

**9.2.** The Bank shall also provide the Customer with the opportunity to change his/her 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.

**9.3.** The Bank's contact details are published on the Bank's website. The Customer may contact the appointed Data Protection Officer by email: dpo@finorabank.eu or by post at the address of Finora Bank’s office. To ensure confidentiality, in cases where the DPO is contacted by post, the envelope must be addressed to the DPO.

**9.4.** Customer’s request for the implementation of data subject’s rights shall be legible and signed, and must contain:

**9.4.1.** Data subject’s name, surname, birth date, address and/or other contact details for communication purposes or for replying to the data subject’s request. If Bank does not process data subject's name, surname and/or date of birth, these Personal Data may not be specified in the request, however, data subject must provide other Personal Data, which unambiguously identify data subject, and which can be verified by the Bank.

**9.4.2.** Information on what right data subject wants to exercise.

**9.4.3.** Reasons based on which data subject seeks to exercise their right (only applicable when exercising right to erasure or right to object).

**9.4.4.** Information about the way in which data subject wishes to receive a response to their request (e. g. by post at the residence address, by email, personally upon arrival to Bank's office.

**9.4.5.** If request is made by the representative, the request shall additionally contain representative's name, surname and contact details, which will be used for communication purposes or for replying to data subject's request. The request must be accompanied with a document confirming the representation or its copy, approved in accordance with the procedure established by legal acts.

**9.5.** Request for implementation of data subject's rights shall be submitted in the official language (Lithuanian or Estonian). This requirement does not apply if data subject is not a citizen of the Republic of Lithuania or the Republic of Estonia and does not understand Lithuanian or Estonian. In such cases the request may be submitted in English, and in case of submission in other languages, a translation into Lithuanian, Estonian or English must be provided together with the request.

**9.6.** If the data subject's request has been submitted in writing personally, data subject shall confirm their identity by submitting the ID document. Failure to do so will prevent the rights of the data subject from implementation. This Clause shall not apply to cases where the request is related to the implementation right to get information about Personal Data processing according to art. 13 and 14 of the GDPR.

**9.7.** If the data subject's request has been submitted in writing by post, it shall be accompanied with a certified copy of data subject's ID document (certified according to the procedure provided in the legal acts) or other information that unambiguously identifies the data subject in cases where the Bank does not process data subject's name, surname or other information of the data subject specified in the ID document. This Clause shall not apply to cases where the request is related to the implementation right to get information about Personal Data processing according to art. 13 and 14 of the GDPR.

**9.8.** If the data subject's request has been submitted in writing by electronic means, it shall be signed with a qualified electronic signature, or it must be formed by electronic means that ensure integrity and immutability of the text or provide other information that unambiguously identifies the Data Subject. If the request is submitted by email by a non-citizen of the Republic of Lithuania or of the Republic of Estonia who objectively is unable to confirm their identity pursuant to the procedure set forth in this Clause and for objective reasons is unable to submit the request in the manner specified in Clauses 9.6-9.7 of this Policy, data subject shall confirm their identity in the manner specified in Clause 9.7 of this Policy.

**9.9.** To avoid unlawful disclosure of Personal Data to third persons, the Bank shall use reasonable efforts to verify the identity of data subject (their representative), who submits respective request. In case of any doubts as to the identity of the data subject (their representative), the Bank shall ask for additional information necessary for respective verification. In such a case the deadline for examining the request is suspended. If data subject (their representative) does not provide additional information within the specified deadline and it is not possible to verify their identity, in accordance with art. 12(3) of the GDPR, the request submitted by the data subject will not be considered.

**9.10.** Customers are advised to use the recommended form of a request for implementation of their rights, which can be found here.

**9.11.** The Bank shall only examine a Customer's request if the identity of the requesting Customer can be established.

**9.12.** Upon receipt of the Customer's request, the Bank must respond and provide information on the actions taken upon receipt of the request in accordance with Section 9 of the Policy no later than within one month from the date of the Customer's request. The information shall be provided to the Customer in writing unless the Customer requests the information otherwise.

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

**9.14.** Information about the processing of their Personal Data shall be provided to the Customers free of charge. Where requests from the Customer are manifestly unfounded or excessive, in particular because of their repetitive character, the Bank may:

**9.14.1.** Charge a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested; or

**9.14.2.** Refuse to act on the request.

**9.15.** The Customer 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 or to the Data Protection Inspectorate, whose website address is www.aki.ee (in Estonia), if the Customer considers that his/her Personal Data is processed in violation of his/her rights and legitimate interests in accordance with the legal acts regulating the protection of Personal Data.

**9.16.** When processing Personal Data, the Bank shall employ and 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.

**9.17.** 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.

## 10. SECURITY OF PERSONAL DATA

**10.1.** We employ appropriate organizational and technical personal data security measures, including protection against unauthorized or unlawful processing of data and against accidental loss, destruction or damage. Such measures have been selected taking into account the risks that may arise for your rights and freedoms as those of a data subject.

**10.2.** We strictly control access to your personal data, providing it only to those employees who need personal data for the performance of their work duties, and monitor how they use the access provided. Employees who have access to personal data shall be made aware of the personal data protection requirements and shall ensure the confidentiality of the personal data processed. We provide access to personal data with passwords of the required level and prepare agreements for the protection of confidential information with individuals or partners who are given access to your personal data.

**10.3.** We regularly monitor our systems for possible breaches or attacks, but it is not possible to guarantee full security of information transmitted online. You provide us with information by use of the internet connection at your sole discretion and assuming any associated risks.

**10.4.** In order to ensure the security of customers' data, we constantly assess and strengthen applicable security requirements.

**10.5.** In order to ensure your data security, the Bank will continue performing regular IT security audits in the future.

finora bank

## 11. CONTACTS

**11.1.** The data controller that processes your personal data indicated in this Policy is:

**11.2.** Finora Bank UAB, code: 305156796, address: Žalgirio str. 90, LT-09303 Vilnius, the Republic of Lithuania.

**11.3.** You can contact us on all issues concerning this Policy in person or by post at: Finora Bank UAB, Žalgirio str. 90, LT-09303 Vilnius, the Republic of Lithuania; or by e-mail: dpo@finorabank.eu.

## 12. VALIDITY AND CHANGES TO THIS POLICY

**12.1.** If we change this Policy, we will publish its updated version on our website, besides, you will be additionally informed about the most important changes via e-mail and/or otherwise.