PRIVACY POLICY

1. Purpose of the Privacy Policy

This Privacy Policy (hereinafter referred to **as the "Privacy Policy")** is intended to ensure that you know to whom you provide your personal data, who is responsible for collecting and storing it, what information we collect and why, how long we store it, what rights you have in relation to your personal data and how you can exercise them, how you can defend your violated rights if you believe that the processing of your personal data is unlawful and/or your rights have been violated, relating to the protection of personal data.

We provide basic information in the Privacy Policy on the processing of personal data, not only relating to the use of the website https://smebank.lt/en/ (hereinafter referred to as 'the **Website**) or a mobile app smeBank, but also about the processing of personal data of candidates for the Bank's employees, the recording of telephone conversations, other information relating to the processing of personal data specific to banks as financial institutions, for example, for the purpose of carrying out the prevention of money laundering and terrorist financing, in order to get to know their customer, assess creditworthiness and etc.

2. About the Data Controller

Data Controller	UAB SME Bank (hereinafter referred to as **the Bank, we**)
Legal entity code	305223469
Address of the Registered Office	Antano Tumėno str. 4-15, Vilnius, Republic of Lithuania
Email address	info@smebank.lt
Phone number	+370 601 88888
Data Protection Officer contacts	dpo@smebank.lt

3. About personal data

Personal data is any information we collect about a natural person that can be used to identify a person and is stored electronically or otherwise.

Personal data includes any information, including your name, address, IP address, biometric data, and other information that we collect about you for the purposes set out in this Privacy Policy.

The person whose personal data we process is also referred to as the data subject in this Privacy Policy. A data subject is considered to be a natural person whose personal data we process. We may process the personal data of such data subjects as: potential, current and former Customers, their representatives, employees, shareholders, members of management bodies, beneficial owners, ultimate beneficiaries, users of our Website, mobile app, self-service portals, participants of the Bank's events and persons visiting the Bank's premises, beneficiaries, representatives and employees of the Bank's business partners, as well as other persons such as followers on social networks, etc.

When processing personal data, we are guided by Regulation No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (**GDPR),** the Law on Legal Protection of Personal Data of the Republic of Lithuania, the Law on Electronic Communications of the Republic of Lithuania and other laws regulating the protection of personal data acts, take into account best practices and the guidance of the supervisory authority.

When we use the term "**processing of personal data**", it refers to any action that is performed on personal data.

4. About the rights of the data subject

In this section, we provide information about your rights in relation to our processing of your personal data and the cases when you can exercise these rights. If you would like to receive more information about your rights

or exercise them, please contact us at the e-mail address of the Bank or its Data Protection Officer specified in this Privacy Policy.

We will provide you with information about the actions taken after receiving your request without undue delay, but no later than within 1 (one) month from the receipt of your request. Taking into account the complexity of the application and the number of applications received, the said deadline may be extended for another 2 (two) months. In this case, we will inform you about such extension of the deadline and its reasons within 1 (one) month from the receipt of the request. We will refuse to enforce your rights only in cases provided for by law.

You will not have to pay any fee to access your personal data (or exercise other rights). If your request is manifestly unfounded or disproportionate, we may charge a reasonable fee or refuse to comply with your request, in which case we will notify you.

You can exercise the following rights:

Right of access to personal data	We aim to ensure that you fully understand how we use your personal data and that you do not experience any inconvenience as a result. We first provide information on how we process your personal data in this Privacy Policy (right to be informed). Nevertheless, you can contact us at any time to inquire whether we are processing any of your personal data. If we store or use your personal data in any way, you have the right to access it. To do this, submit a written request to us at the e-mail address specified in this Privacy Policy, confirm your identity (if such confirmation is required in a particular case). We expect you not to abuse such requests, to adhere to the principles of honesty and reasonableness.
Right to withdraw consent	If you have given us explicit consent to the processing of your data, you can withdraw it at any time. The withdrawal of consent does not affect the lawfulness of data processing based on consent carried out prior to the withdrawal of consent. You can opt out of direct marketing communications by simply clicking on the opt-out link in the marketing communications or by contacting us using the contacts specified in Section 2 of the Privacy Policy. You can revoke your consent to record telephone conversations simply by terminating the telephone conversation or by notifying the Bank about the revocation of such consent using the contacts specified in Section 2 of the Privacy Policy. For more information on how you can withdraw your consent to the use of cookies, how you can reject or delete cookies, please refer to the "Cookies" section of the Privacy Policy.
Right to request erasure of personal data ("right to be forgotten")	Where we do not have a legal basis to process personal data below or in other cases referred to in Article 17(1) of the GDPR, you have the right to request that we erase your personal data. For example, if you withdraw your consent and we have no other reason to process your personal data processed on the basis of consent, we will delete it if

	the legislation does not provide for an obligation for us to store your personal data. Please note that the deletion of your personal data may take several days. Among other things, the deletion of your personal data may be implemented by the depersonalization of your personal data, where appropriate.
Right to request rectification of personal data	If you become aware that we process inaccurate, incomplete personal data about you, regardless of the reasons, you have the right to ask us to correct any inaccuracies in your personal data or, where applicable, to supplement them. In such cases, we have the right to ask you to provide evidence confirming the accuracy of your personal data, where appropriate.
Right to request restriction of processing of personal data	You have the right to ask us to restrict or object to the processing of your personal data: a) during the period for which we need to verify the security of your personal data, when you make claims relating to the accuracy of the data; b) in case of unlawful collection, storage or use of your personal data, where you decide not to request the deletion of the data; c) when we no longer need your personal data, but you need it for the preparation of, exercising or defending lawful claims; d) for the period necessary to determine whether we have an overriding legal basis to continue processing your personal data if you exercise your right to object to the processing of your personal data.
Right to object to the processing of personal data	You have the right to object to our use of your personal data in accordance with the procedure set out in Article 21 of the GDPR, for example when we use your personal data on the basis of our legitimate interest. You have the right to object to the use of your personal data for direct marketing purposes at any time. By exercising this right, you will no longer receive any direct marketing communications from us. If you are using our smeBank app, you need to check your device's settings and permissions related to push notifications and change the settings according to your preferences. We will exercise your right unless we need your data to defend legal claims or we have compelling legitimate reasons to process data that override your interests, rights and freedoms.
Right to data portability	The application of this right is limited. You may exercise this right only in relation to the processing of personal data that satisfies the following conditions:

	a) is carried out with your consent or on the basis of a contract with you, and b) you have provided the personal data to us in a structured, commonly used automated way, such as by e-mail. This means that if we process your personal data on the basis of legitimate interests, this right will not be exercised at your request, just as this right will not be exercised in the event that the personal data will be processed on the basis of consent or contract with you, but will be processed only on paper media. If you exercise this right, we will provide you with a copy of the data you have provided.
Oppose automated decision-making	We do not process personal data based solely on automated decision-making, including profiling, which would have legal or similar significant effects.

If you believe that your rights as a data subject are and/or may be violated, please contact us immediately by e-mail specified in this Privacy Policy. We ensure that only upon receipt of your complaint will we contact you within a reasonable period of time and inform you about the progress of the complaint investigation and subsequently about the outcome.

If you are not satisfied with the results of the investigation, you may file a complaint with the supervisory authority – the State Data Protection Inspectorate: https://vdai.lrv.lt/, L. Sapiegos str. 17, Vilnius, the Republic of Lithuania or another supervisory authority where your permanent place of residence, place of work or where a suspected violation of the GDPR has been committed.

5. Processing of personal data for the purposes of the prevention of money laundering and terrorist financing

Whose personal data do we process?	**What personal data do we process?**	**What is the legal basis for the processing of personal data?**	**Who receives personal data?**	**How long do we store personal data?**
Identification of potential customers, representatives of potential customers (primary KYC procedure)				
Potential customers of the Bank, representatives of potential customers of the Bank (beneficial owners, director and authorized signatories)	Name, surname, e-mail address, personal identification number, duties/relationship with the customer(ultimate beneficiary, director, authorized signatory), copy of the passport of any country, identity card issued by the EU and EEA Member States, residence permit in the Republic of Lithuania, date and time of identification, image (foto) result of identification (whether the document submitted is real or fake, reasons that led to suspicions regarding the	Article 6(1)(c) GDPR (legal obligation) Article 9(2)(a) GDPR (biometric consent)	Bank of Lithuania Financial Crime Investigation Service Data recipients (data processors): UAB "Ondato"	If the person becomes a customer - 8 years from the termination of the contract. If the person does not become a customer - 12 months from the identification procedure

	authenticity of the document)			
Compliance with anti-money laundering and terrorist financing requirements and implementation of international sanctions (direct customers, parties to transactions, partners)				
Any customer of the Bank, customer manager, shareholder, authorized person, business partner of the Bank, parties to transactions (operations)	Name, email address, personal identification number, date of birth, tax identification number, address, nationality, copy of identity document (information provided in the ID document), income (employment salaries, retirement income, freelance), income from business, inheritance/family gift, insurance income/payout, divorce agreement, investment income/return, winnings (giver/non-governmental lottery), earnings (business sale, sale of property), criminal records, positions held and participation of the customer or family members or close assistants in the policy.	GDPR 6(1)(c) (legal obligation), the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and the related implementing national provisions. Law on the Implementation of International Sanctions of the Republic of Lithuania	Financial Crimes Investigation Service under the Ministry of the Interior, Ministry of Foreign Affairs of the Republic of Lithuania (regarding violation of sanctions) Bank of Lithuania; Data recipients (data processors): Flagright Ltd; Other credit and financial institutions, correspondent banks involved in the execution of customer payments.	Customer information – 8 years from the termination of the business relationship. Additional information received from the customer (correspondence of the business relationship) – 5 years from the termination of the business relationship
Creditworthiness assessment and debt management, including receiving and transmitting data to Creditinfo and Scorify.				
Customer, customer owners, managers, accountants, customer creditors and debtors	Name, surname, e-mail address, personal identification number, address, copy of identity document, property, utility account data, bank statement data, data provided in the Source of Welfare (SOW) form, e-mails (communication)	Article 6(1)(a) GDPR (consent), Article 6(1)(c) (legal obligation) Article 6(1)(f) (legitimate interest)	UAB "Creditinfo Lietuva" UAB “Scorify” UAB COFACE BALTICS SERVICES	10 years from the date of full repayment of the credit and the expiry of the contract. If the contract is not concluded, the data is stored for 12 month from the last day of communication with the customer

6. Data processing in connection with the provision of the Bank's services

Whose personal data do we process?	**What personal data do we process?**	**What is the legal basis for the processing of personal data?**	**Who receives personal data?**	**How long do we store personal data?**
Conclusion of a Bank contract and provision of services				
Parties to the contract, their representatives	Name, surname, citizenship, registration address,	Article 6(1)(b) GDPR (contract –	Probanx, UAB HyperOPs, UAB	10 years from the termination

	correspondence address, date of birth, gender, identity document data, telephone number, e-mail address, place of birth, tax payment country, tax identification number, address of credited, leased property, unique number, car identification number (VIN), personal data of the owner, including personal data of the seller of the leased object (property).	if the customer is a natural person) Article 6(1)(f) GDPR (legitimate interest in performing the contract concluded with the customer – if the customer is a legal person)		of the contract If the contract is not concluded – for 12 month, counting from the last day of communication with the customer
Creation of a user account in the online banking system				
The Bank's customers and their Authorized Persons	Name, surname, personal identification number, company name, position, identity document data, correspondence address, telephone number, e-mail address, account number	Article 6(1)(b) GDPR (contract – if the customer is a natural person) Article 6(1)(f) GDPR (legitimate interest in performing a contract concluded with a customer – if the customer is a legal person)	Probanx, UAB	8 years from termination of the contract
Provision of mandatory information to customers				
Customer, customer contact person	Name, E-mail Address, Phone Number	Article 6(1)(b) GDPR (performance of the contract)	Unforeseen	5 years from the date of termination of the contract
Assessment of the customer's creditworthiness				
Bank customers, customer Managers, Shareholders	Name, surname, personal identification number, e-mail address, telephone number, marital status, education, professional qualifications, financial data (average salary, liabilities, assets)	Article 6(1)(b) of the GDPR (contract – if the customer is a natural person), Article 6(1)(c) of the GDPR (legal obligation) Markets in Financial Instruments Directive, Rules approved by the Bank of Lithuania	Unforeseen	10 years from the end of the contractual relationship

Internal, SEPA and TARGET2 payments (including scheduled bulk payments)				
Parties to the Bank account contract	Name, surname, address, country, identity document, telephone number, e-mail address, representative of the customer, if the payment is made in the name of another person – name, code, payment code of the person on whose behalf the payment is made, number of the account from which the payment is made, recipient's information (name, code, account number, address), payer code/purpose of payment, payment amount	Article 6(1)(b) GDPR (contract)	Probanx, UAB UAB "INVENTI" Plumery B.V.	10 years from the end of the contractual relationship
International (SWIFT) payments				
Parties to the Bank contract	Name, surname, address, country, identity document, telephone number, e-mail address, representative of the customer, if the payment is made in the name of another person – name, code, payment code of the person in whose name the payment is made, bank information: name, SWIFT code, number of the account from which the payment is made, information of the recipient (name, code, account number), bank information of the recipient (name, SWIFT code) payment amount, Payer's code/purpose of payment	Article 6(1)(b) GDPR (contract)	SWIFT Other financial institutions are used to execute cross-border payments	10 years from the end of the contractual relationship
Conclusion and execution of loan contracts				
Customers, natural persons who have concluded loan contract	Name, surname, personal identification number, address, telephone number, e-mail address, bank account number, data about the representative, if authorized (name,	Article 6(1)(b) GDPR (contract)	Unforeseen	Until the end of the contractual relationship For the purposes of

	surname, contact details, basis for representation), contract conclusion fee, data on the amount of the monthly payment and its payment date, payment schedule, term of the agreement, termination fee, data on the amount and date of payments made, debts incurred during the execution of the loan contract, signature			archiving and protection of the Bank's rights and legitimate interests – 10 years from the end of the contractual relationship
Representatives of legal entities of customers who have concluded loan contracts	Name, name and surname, basis for representation and signature of the legal entity in whose name the contract is concluded	Article 6(1)(f) GDPR (legitimate interest in performing the contract concluded with the customer – if the customer is a legal person)	Unforeseen	Until the end of the contractual relationship For the purposes of archiving and protection of the Bank's rights and legitimate interests – 10 years from the end of the contractual relationship
Conclusion and execution of contracts for the provision of services related to payment cards				
Parties to the Contract, corporate cardholders (natural persons using the Company's corporate cards who have registered for the Bank's services directly or through the partner platform).	Identification data of corporate cardholders (name, surname, personal identification number, date of birth, place of birth, politically exposed person status, citizenship, personal identity card (passport) number, place of issue, date and validity, place of residence, position, contact details (address, , mobile phone number, e-mail address); IBAN number, debit card number, IP addresses, transaction date, transaction amount, currency, location, data about the recipient of funds.	Article 6(1)(b) GDPR (contract) Article 6(1)(f) GDPR (legitimate interest)	Wallester AS Idemia	8 years from the end of the contractual relationship

Conclusion and enforcement of pledge contracts				
Parties to the Contract	Name, surname, personal identification number, e-mail address, bank account number, address of residence, information about real estate, income, marital status, restrictions on assets (interim measures, attachment), income received due to incapacity for work	Article 6(1)(a), (b), (c) and (f) of the GDPR The Civil Code of the Republic of Lithuania - on the identification of the customer, capacity / incapacity, assurance and performance of obligations, debts, conclusion of contracts. The Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania - on the identification of the customer or beneficiary. The Law on banks of the Republic of Lithuania is on the protection of bank secrecy and the interests of customers. The Law on Crediting of Real Estate - on the assessment of the creditworthiness of the guarantor. Regulations on the organisation of internal control and risk assessment (management) - on the assessment of the guarantor. The Law of the Republic of Lithuania on Bills of Exchange and Ordinary Bills of Exchange - on the details of the promissory note.	State Enterprise Centre of Registers	10 years from the end of the contractual relationship

Granting of credits with ILTE guarantee instruments				
Representatives of legal entities applying for credit with ILTE guarantee instruments	Name, surname, grounds for representation of the legal entity on whose behalf the contract is concluded, signature	Article 6(1)(f) of the GDPR (legitimate interest of the Bank in concluding a valid contract with a legal entity) Article 6(1)(c) GDPR Articles 6.30, 6.93, 6.935 of the Civil Code	ILTE	10 years from the end of the contractual relationship
Send late payment reminders to customers				
Customers and customer representatives	Name, surname, e-mail address, position in the company (representative), personal identification number, address, telephone number, account number, information about late payments	Article 6(1)(b) GDPR (contract – if the customer is a natural person) Article 6(1)(f) GDPR (legitimate interest in performing the contract concluded with the customer – if the customer is a legal person)	Service providers providing debt collection services	10 years from the end of the contractual relationship
Restructuring of credit contracts, surety contracts (the purpose is to assess the solvency of the debtor/collateral provider/guarantor and the possibilities to cover the debt), only in cases of restructuring of legal entities				
Owners/shareholders /managers of debtors owned by corporations; guarantors; guarantors (including holders of debt commitments)	Name, surname, personal identification number, address, telephone number, e-mail address, transaction data, property (movable and real)	Article 6(1)(b) GDPR (contract) Article 6(1)(f) GDPR (legitimate interest)	Public authorities, courts, bailiffs	10 years from the end of the contractual relationship
Monitoring of the fulfilment of obligations under signed credit contracts				
Customers, customer representatives	Name, e-mail address, telephone number, address, content of correspondence, other information related to the fulfilment of obligations under the signed credit contracts	Article 6 (1)(c) (legal obligation) of the GDPR, Article 31(6) of the Law on Financial Institutions of the Republic of Lithuania, EBA Guidelines on Granting and Monitoring of Loans	Unforeseen	10 years from the end of the contractual relationship

Customer/Vendor Debt Lists				
Late customers, suppliers whose invoices are late	Name, E-mail Address, Personal Identification Number, Address, Phone Number, Account Number, Overdue Amounts	Article 6(1)(c) GDPR (legal obligation) Law on Accounting of the Republic of Lithuania, Law on Value Added Tax of the Republic of Lithuania	Service providers providing debt collection services	10 years from the date of the specific documents (from the end of the calendar year)

7. Processing of personal data related to the administration of the Bank's business activities

Whose personal data do we process?	**What personal data do we process?**	**What is the legal basis for the processing of personal data?**	**Who receives personal data?**	**How long do we store personal data?**
Litigation				
Debtors, representatives of debtors, other persons potentially infringed the rights of the Bank	Name, surname, e-mail address, telephone number, personal identification number, financial information, marital status, property, income	Article 6(1)(f) GDPR (legitimate interest)	Courts, lawyers, legal service providers	5 years since the final court decision
Processing of requests, requests, complaints submitted by customers or persons related to customers (representatives, etc.)				
Persons submitting an enquiry, request or complaint to the Bank	Name, personal identification number, ID number, place and date of issue, telephone number, e-mail address, recent financial transactions of the customer made on each of the customer's accounts (date, amount, names of payer/recipient, trading/service company), other data related to a particular inquiry, request or requirement	Article 6(1)(c) GDPR (legal obligation) Rules for the Handling of Complaints Received by Financial Market Participants Approved by the Bank of Lithuania	Bank of Lithuania	3 years from the end of the calendar year in which the specific inquiry, request or complaint was received
Organization of virtual events/seminars (Bank Promotion)				
Event participants	Name,surname, company, job title, e-mail address, participation information	Art. 6(1)(a) GDPR (consent)	Manager of the platform through which the event is organized	10 working days from the end of the event
Archiving of paper files				

Parties to the Treaties, Representatives of the Parties	Customers documents with various personal data	Article 6(1)(c) GDPR (legal obligation)	Unforeseen	According to the Bank's Documentation Plan
Reporting to the supervisory authority				
Bank customers	Name, surname, personal identification number, customer code, account number	Article 6(1)(c) of the GDPR, CIR Regulation 575/2013; Regulation 680/2014 - Technical standards for reporting to supervisors	European Central Bank	10 years
Bank customers, customers' ultimate beneficiaries	Name, surname, citizenship, date of birth, personal identification number, identity document data (type, number, place of issue, other information specified in the Order No. VA-61 of the Director of the State Tax Inspectorate	Article 6(1)(c) GDPR (legal obligation) Article 55 of the Law on Tax Administration, Order No. VA-61 of the Director of the State Tax Inspectorate, description of the XML scheme of the MAI55 notification subsystem of the STI	State Tax Inspectorate	The data transmitted to the STI as an XML file is not automatically stored
Independent AML audit (provision of information to external auditors)				
Customers of the Bank, persons related to the Bank's customers (shareholders, members of board bodies), other representatives of customers	Name, personal identification number, customer code, account number, other information collected for the purposes of prevention of money laundering and terrorist financing and "know the customer"	Article 6(1)(c) GDPR (legal obligation), Article 6(1)(f) (legitimate interest of the Bank in improving the Bank's anti-money laundering procedures)	Service providers providing audit services	Information submitted for external audit is no longer retained. The information from which the data was obtained is stored for another 10 years
Independent financial audit (provision of information to external auditors)				
Customers related to an ongoing audit	Name, information about the banking services used by the customer, customer's internal code, account number, first and last name, personal identification number,	Article 6(1)(c) GDPR (legal obligation) Article 39 of the Financial	Service providers providing audit services	Information submitted for external audit is no longer retained. The information from which the

	customer's internal code, e-mail address, account number, account balance, telephone number	Statements Audit Act		data was obtained is stored for another 10 years
Transfer of data on loan contracts (performance of contracts) to third parties				
Parties to loan contracts	Name, personal identification number, country of residence, specific customer loans or loans for which he guarantees or is the manager of the lending company, information about the customer's mortgaged assets	Article 6(1)(c) GDPR (legal obligation) Loan Risk Database Management Rules approved by the Bank of Lithuania	Bank of Lithuania	5 years
Debt Collection (Assessment of Debt Collection Options)				
Persons who are late in making payments	Name, personal identification number, address, telephone number, e-mail address, property (movable and immovable), employer and income	Article 6(1)(f) GDPR (legitimate interest)	Courts, bailiffs, public authorities	10 years from the end of the contractual relationship
Persons whose contracts with the Bank have been terminated due to outstanding obligations, persons against whom debt collection proceedings have already been initiated	Name, personal identification number, address, telephone number, e-mail address, marital status, account number, transaction details, assets (movable and immovable), employer and income	Article 6(1)(f) GDPR (legitimate interest)		
Owners/shareholders/managers of debtors owned by corporations; guarantors; guarantors (including holders of debt commitments)	Name, surname, personal identification number, address, telephone number, e-mail address, transaction data, property (movable and immovable)	Article 6(1)(f) GDPR (legitimate interest)		
Internal investigations and operational risk events (analysis)				
Customers related to an ongoing internal investigation and/or operational risk event	Name, e-mail address, identity document data, telephone number, address, account numbers/statements, services provided by the Bank to a particular	Art. 6(1)(f) GDPR (legitimate interest), Art. 6(1)(c) (legal obligation) Regulations for the Organisation	External auditors, Bank of Lithuania	10 years

	customer, customer code in the Bank's systems	of Internal Control and Risk Assessment (Management) of the Board of the Bank of Lithuania Rules for the Provision of Information on Banks' Internal Governance and Activities to the Bank of Lithuania			
Identification and investigation of violations of work duties, confidentiality, intellectual property rights, management of data protection violations, ensuring smooth operation of the Bank when an employee is unable to perform his/her work functions					
Contractors of communication with the Bank	Name, date and time of action, content of communication, actions taken online (on-line)	Article 6(1)(f) GDPR (Legitimate interest of the Bank in preventing and detecting irregularities)	Law enforcement authorities State Data Protection Inspectorate (in case of personal data breach)	4 years	
Drafting and administration of powers of attorney, representation contracts					
Third parties authorized to represent the Bank	Name, surname, personal identification number/date of birth, position, telephone number, e-mail address, signature, power of attorney number	Article 6(1)(b) GDPR (contract)	State Enterprise Centre of Registers (in case of registration of notarial powers), third parties to whom a power of attorney is issued; Notary offices certifying notarial powers of attorney	Powers of attorney - 3 years after their expiration or termination, contracts - 10 years after their termination.	
Attorneys and/or lawyers	Name, Title, Lawyer's License Number, Phone Number, E-mail Address, Signature, Bank Account Number	Article 6(1)(b) GDPR (contract)	External auditors for the analysis of Bank litigation cases (representative is indicated as the lawyer responsible for the case)	3 years after the expiry of the powers of attorney or after their termination, contracts - 10 years after their termination.	
Assessment of the possibility of selling the Bank's business or part thereof (including legal due diligence of the Bank in such cases)					
Members of the Board of the Bank, their relatives, customers of the Bank	All information held by the Bank, except for special categories of personal data	Article 6(1)(f) GDPR (legitimate interest in assessing the possibility of transferring a Bank's business or part thereof)	Potential investors Auditors	Prior to the decision not to invest, and in the case of investments, within the data retention periods set for	

				individual purposes
Accounting of Bank participants (shareholders)				
Bank participants (shareholders)	Name, surname, email address, personal identification number and/or name and number of identity document, address, nationality, telephone number, number of shares or units, nominal value of shares or size of units, any other identifying information (type, class, issue number, registration number) and property and non-property rights granted.	Article 6(1)(c) GDPR (legal obligation) Article 15 of the Law on Financial Institutions of the Republic of Lithuania Regulation (EU) No 10/2014 of the European Parliament and of the Council 600/2014; Delegated Regulation (EU) 2017/590	State Enterprise Centre of Registers	10 years from the transfer of shares
Formation of payment orders based on submitted invoices, when the invoice is submitted by a person with a business license/sole proprietorship/license. Payments under copyright contracts. Submission of data to the State Tax Inspectorate (Class B income, declarations)				
Suppliers of goods and services	Name, surname, e-mail address, personal identification number, address, business license number, individual activity certificate number	Article 6(1)(b) GDPR (contract), Article 6(1)(c) GDPR (legal obligation)	State Tax Inspectorate	10 years from the end of the calendar year in which the invoice was paid
Internal audit				
Customers, customer representatives that will be checked during the audit	All information held by the Bank	Article 6(1)(c) GDPR	Bank of Lithuania External auditors	10 years from the date of the report (counting from the end of the calendar day)
Preparation of minutes of meetings of the Supervisory Board, Board of Directors and Banking Committees				
Providers	In the content of the minutes of the meeting, the information, name, surname, voice, and image of the service providers are indicated and	Article 6(1)(f) GDPR (legitimate interest)		Until the minutes are drawn up (no longer than 20 days after the relevant meeting)

	named during the meeting			
Reporting and handling of whistleblowers				
Whistleblower	Name, contact details (telephone number and e-mail address), personal data related to the provision of information (fact, date, time (where applicable) of the provision of information to the company), content of the message (and the personal data of the whistleblower contained therein or its annexes) and, where applicable, fact, date, time (where applicable) of the response to the message; other data at the choice of the whistleblower (correspondence (where the natural person can be identified) and signature)	Article 6(1)(c) GDPR (legal obligation)	The Prosecutor General's Office of the Republic of Lithuania (upon the request of the rapporteur to acquire the status of rapporteur or in the event of a violation of the provisions of Article 3 of the Law on Whistleblowers of the Republic of Lithuania public interest) Competent authorities (where information may reasonably suspect that a criminal offence, administrative or other legal offence is being prepared, committed or has been committed) infringement)	5 years from the examination of the report
Witnesses	Name, surname, contact details (telephone number and e-mail address), other data (place of employment and duties, fact and content of the submission of the report to which the person may testify, correspondence (where it can be identified a natural person)			
Fraud prevention				
Customers, customer representatives	Customer Name, IP Address, Location, Device Information, Traffic Log Data, Event ID, Channel, Action Performed	Article 6(1)(c) of the General Data Protection Regulation (legal obligation); Resolution of the Bank of Lithuania on	Law enforcement authorities UAB "Ondato" UAB Probanx Flagright Ltd	8 years

		the Approval of the Description of Information and Communication Technologies and Security Risk Management Requirements; Bank of Lithuania Fraud Prevention Guidelines	Plumery B.V.	

8. Processing of candidates' personal data

We search for candidates for employees not only by posting job offers, but we also actively search for potential candidates on professional social networks, such as LinkedIn and other websites/portals dedicated to recruitment. For the purpose of searching for candidates on the social network LinkedIn, job advertisement portals and other public sources, the Bank processes the following personal data of potential candidates (persons meeting the search criteria): name, surname, other information provided in the profile of the social network LinkedIn or another search platform. Personal data is processed on the basis of the Bank's legitimate interest. Personal data is not stored separately, the selected persons are simply asked for their consent to participate in the selection of the Bank's employees.

What personal data we process as a candidate will depend not only on whether you apply yourself according to the Bank's job advertisements or if we contact you through professional social networks, but also on what position you will apply for. If you apply for the positions of management and key employees (members of the Bank's Board, Head of the Bank, positions related to compliance enforcement, risk management, prevention of money laundering and terrorist financing, provision of financial services, internal auditor, etc.), we will process more information about you than we would if you were a candidate for another position at the Bank.

We provide specific legal bases for the processing of personal data in the tables below, however, when we process your personal data on the basis of consent, you express your consent by sending your CV and/or motivation letter to the Bank. For other consents, such as consent to apply to an existing employer, we will apply separately.

If you fail to provide your personal data that is necessary for the selection, we will not be able to assess your suitability for the position you want/offer.

For the purpose of selecting candidates, we also process data of third parties. On the basis of our legitimate interest (Article 6(1)(f) of the GDPR), we will process the data on the person indicated by the candidate (name, surname, e-mail, telephone, information provided by the person) – former or current employer or person making a recommendation, the information provided by him or her – for the purpose of selecting the candidate. In this case, our legitimate interest is to choose the right candidate for the position we are looking for. We will destroy this data within 3 months after the signing of the contract with the selected candidate or the decision to complete the selection. When selecting candidates for the Bank's management and main positions, we process the personal data of the candidates' close relatives (family relationship, name, surname, year of birth, place of employment, position).

Below in this Privacy Policy, we provide more detailed information about the processing of your personal data as a candidate.

8.1. Processing of personal data of candidates for non-managerial and non-main positions at the Bank

What personal data do we process?	On what legal basis do we process data?	To whom will we transfer your data?	How long will we keep your data?
Name, surname, personal identification number, identity document information (mandatory), address,	Art. 6(1)(a) GDPR (consent), Art. 6(1)(b) (pre-contractual action)	Bank of Lithuania	3 months after the end of the selection procedure (when you have not been selected for the position), unless you give your separate consent

telephone number, nationality, information provided in the CV (education, languages, qualifications, previous employers)			to the storage of your personal data for the period specified in the consent for future job offers (administration of the candidate database) 10 years after the end of the employment relationship (when you have been selected and an employment contract has been concluded with you)
Information about qualifications and reputation, sufficient experience and skills to perform job duties, avoidance of conflicts of interest, publicly available information (LinkedIn account data, other information found in an online search)	Article 6(1)(f) GDPR (legitimate interest)		
Conviction data	Article 6(1)(c) (legal obligation), Article 10 of the GDPR, Law on the Market in Financial Instruments of the Republic of Lithuania, Article 34(10), Article 34(12) of the Law on Banking, Item 8.3 of the Regulations on the Organisation of Internal Control and Risk Assessment (Management) of the Bank of Lithuania		
Data from a previous employer	Article 6 – paragraph 1 – point f GDPR (Legal interest of the Bank in assessing the candidate's suitability for the job)		
Data obtained from an existing employer	Art. 6(1)(a) GDPR (consent)		

8.2. Processing of personal data of candidates for managerial and key positions at the Bank

What personal data do we process?	On what legal basis do we process data?	To whom will we transfer your data?	How long will we keep your data?
Name, surname, personal identification number, identity document information (mandatory), address, telephone number, nationality, information provided in the CV (education, languages,	Art. 6(1)(a) GDPR (consent), Art. 6(1)(b) (pre-contractual action)	Bank of Lithuania	3 months after the end of the selection procedure (when you have not been selected for the position), unless you give your separate consent to the storage of your personal data for the period specified in the consent

qualifications, previous employers)			for future job offers (administration of the candidate database) 10 years after the end of the employment relationship (when you have been selected and an employment contract has been concluded with you)
Financial obligations, data about close relatives (family relationship, first name, surname, year of birth, place of employment, position), information about personal interests (name, surname, relationships), information about the provision of services to other companies (if any), publicly available information, real estate, other information about the good reputation, qualifications and experience necessary to properly perform the duties, avoid conflicts of interest, ensure independence and be able to devote time to fulfilling their obligations	Article 6(1)(c) of the GDPR (legal obligation), Article 6(1)(f) of the GDPR (legitimate interest of the Bank to ensure compliance with legitimate requirements when the legal acts do not specify any specific data necessary for the implementation of legal obligations), Articles of the Law on Banking Article 34(10), Article 34(12), Clause 8.3 of the Regulations on the Organisation of Internal Control and Risk Assessment (Management) of the Bank of Lithuania		
Health data	Article 6(1)(c) of the GDPR (legal obligation), Article 9(2)(b) (employer's obligations in the field of labour law), Article 34(2) of the Banking Act		
Conviction data	Article 6(1)(c) (legal obligation), Article 10 of the GDPR, Law on the Market in Financial Instruments of the Republic of Lithuania, Article 34(10), Article 34(12) of the Law on Banking, Item 8.3 of the Regulations on the Organisation of Internal Control and Risk Assessment (Management) of the Bank of Lithuania		
Data from a previous employer	Article 6 – paragraph 1 – point f GDPR (Legal interest of the Bank in assessing the candidate's suitability for the job)		
Data obtained from an existing employer	Art. 6(1)(a) GDPR (consent)		

Questionnaire of the manager and other information and documents related to the assessment and issuance of a permit by the Bank of Lithuania approved on the basis of the requirements of the Bank of Lithuania	Article 6(1)(c) of the GDPR (legal obligation), Article 34(2) of the Law on Banking, Regulations for the Assessment of Managers of Financial Market Participants and Persons Performing Key Functions supervised by the Bank of Lithuania	Bank of Lithuania	

9. Direct marketing, asking for the opinion of customers

We send direct marketing messages, including newsletters, to persons who have given consent to direct marketing, as well as ask for your opinion on the Bank's services. For the purpose of sending direct marketing messages, we process the following personal data: name, surname, telephone number, e-mail address, information about the Bank's services ordered and used. Your data will be processed for the purpose of sending direct marketing communications for 3 years from the date of giving consent or until the withdrawal of consent. Direct marketing communications are sent (your contact details are processed) on the basis of consent.

If you are our customer and you have not objected to the direct marketing of our services similar to the services you have purchased at the time of ordering the services you have purchased, we may send direct marketing communications to the e-mail address specified in the contract on the basis of a legitimate interest. In this case, direct marketing communications will be sent to the email address specified in the contract for a period of 3 years, but in any case not longer than during the period of validity of the contract, unless you object to the further processing of data for the purpose of direct marketing by then. In this case, we will immediately stop sending direct marketing messages to you.

Personal data processed for the purpose of direct marketing may be transferred to data processors who provide software, information systems or assist in carrying out direct marketing to the Bank.

You have the right to opt out of receiving direct marketing communications at any time by contacting us at the email specified in Section 2 or by clicking on the opt-out link in the direct marketing communications.

IMPORTANT! Please note that not every message sent by the Bank is considered to be direct marketing, in some cases, we are obliged to send you mandatory information in compliance with a legal obligation (Article 6(1)(c) of the GDPR), for example, by informing you about changes in the rules of service provision. For this purpose, we process your name, surname and e-mail address. For the purpose of sending mandatory notifications, we will process it until the end of the contractual relationship.

---

10. Recording phone conversations

In order to ensure the quality of the Bank's services and to protect the rights and legitimate interests of the Bank, the Bank records telephone conversations conducted by its contact consultation telephone number published on the Bank's website https://smebank.lt/en/. Telephone conversations are recorded on the basis of your consent when you continue the conversation after the text of the warning about the recording of telephone conversations has sounded. You can object to the recording of telephone conversations and exchange with us in other ways, such as by e-mail info@smebank.lt. You can withdraw your consent by interrupting the conversation or by notifying us of the withdrawal of consent by e-mail info@smebank.lt.

For the purpose of ensuring the quality of the Bank's services and protecting the rights and legitimate interests of the Bank, we will process your personal data: name and surname, voice, record of the conversation, the date and time of the start and end of the telephone conversation, the telephone number to which the call is made and from which the call is made.

For the purpose of ensuring the quality of the Bank's services, we will store your personal data for 12 (twelve) months from the date of recording the conversation, except for the exceptions provided for in the Rules for Recording Telephone Conversations. If, within the specified period, we receive your complaint regarding the circumstances discussed during the telephone conversation, or the official appeal of the authorities regarding the circumstances related to the specific telephone conversation and the recording of the telephone conversation and its preservation is necessary for the protection of the rights and legitimate interests of the Bank, the specific recording of the telephone conversation and your personal data will be stored until the expiry

of the statute of limitations for lodging a complaint against the Bank's actions or until the final decision of your court decision of the authority hearing the complaint/application, other authorities dealing with disputes.

11. Conclusion and execution of contracts with partners, service providers

The Bank processes the data of partners or service providers (legal persons) and the data of partners or service providers (natural persons) in order to perform the contract concluded between the Bank and the specified persons.

The Bank will process the **following data of the above-mentioned** partners or service providers (natural persons): name, surname, personal identification number, address, business license/individual activity certificate number (service provider), bank account number, information about the services provided, other information related to the performance of the contract. The legal basis for the processing of such personal data is Article 6(1)(b) of the GDPR (contract).

The Bank will process the personal data of the Bank's partners or service providers (representatives of legal entities): name, surname, position, basis of representation, e-mail address, telephone number, content of correspondence. The basis for the data processing is the Bank's legitimate interest in the performance of the contract concluded with the Bank's partner or service provider (legal entity) (Article 6(1)(f) of the GDPR).

The personal data specified in this paragraph will be processed for as long as the contract is in force. If the personal data is specified in the contract, it will be stored for 10 years from the date of expiry of the contract in accordance with the archiving obligation (Article 6(1)(c) GDPR).

12. Administration of social media accounts

The Bank has the following accounts on social media networks (hereinafter referred **to as the "Social Account**"):

- Facebook: https://www.facebook.com/SMEBankas
- LinkedIn: https://www.linkedin.com/company/sme-bank/

The information you provide to us via social media (including messages, use of the "Like" and "Follow" boxes, and other communications) is controlled by the social network operator. We process the information contained in the social account for the purpose of account administration on the basis of your consent. We do not store the information contained in the social account separately (when the data is processed for the purpose of administering the social account, but the data may be stored if it needs to be processed for another purpose, for example, to protect the rights and legitimate interests of the Bank).

When you visit Social Accounts, social media managers install cookies on your device, and these cookies collect your personal data. Cookies are installed on your device both when you are a registered user of the relevant social media network and when you do not have an account with the relevant social media network. We do not have access to the personal data collected and only receive statistical information about visitors to the social media network provided by the operators of the social media networks.

We recommend that you read the privacy notice of the social media networks Facebook and LinkedIn and contact them directly if you have any questions about how they use your personal data.

The Website uses plugins for social networks Facebook and LinkedIn icons. We have installed the plugins on the Website in order to enable you to be redirected from our Website to the Bank's social media accounts. Managers of the plugins used on the Website:

a) Facebook – Meta Platforms Ireland Limited (4 Grand Canal Square, Grand Canal Harbour, Dublin 2 Ireland);

b) LinkedIn – LinkedIn Ireland Unlimited Company (Wilton Plaza, Wilton Place, Dublin 2, Ireland).

By clicking on the plugin icon, you are redirected to the plugin manager page and the plugin manager is provided with data from which page the request was made, the time and date of the request. The plugin is recognizable by Facebook, LinkedIn logos.

The information that an individual provides on the Plugin Manager's page or that is obtained when a person visits the plugin links on our Website is under the control of the plugin managers. Information on the personal

data collected and stored, the legal bases for data processing, data storage terms, applied technical and organisational security measures are provided in the privacy notices of the plugin managers: https://lt-lt.facebook.com/privacy/explanation/; https://www.linkedin.com/legal/privacy-policy.

13. Information on the use of cookies

Our Website uses cookies and other tracking technologies. A cookie is a small file made up of letters and digits that we place on your browser or hard drive on your computer with your consent. We use different cookies for different purposes. Cookies also help us to distinguish you from other users of the Website, thus providing a more pleasant experience on the Website and allowing us to improve the Website.

The first time you visit the Website, we will ask you to consent to the use of cookies, allowing you to choose which cookies you allow or allow the use of all cookies. Cookies will only be used if you give us your consent. We will keep the consent you have given and it will be valid for one year or until you revoke or change the consent given.

If you do not agree with the use of cookies, click on the option "**I do not agree**".

How do I withdraw my consent?

To withdraw your consent to the use of cookies, you can do so by clicking on the icon at the bottom of the Website, in the left corner

 or  and clicking on the "**I disagree**" option. If you want to change the consent given to individual cookies, click on the option "**Save choices**".

You can also change your browser settings on your computer, tablet or smartphone at any time so that cookies are not accepted or deleted if cookies are already saved. Detailed instructions depend on what browser you are using and what device, more detailed information can be found here:

- „Internet Explorer“ – https://support.microsoft.com/en-us/windows/delete-and-manage-cookies-168dab11-0753-043d-7c16-ede5947fc64d#ie=ie-11
- „Microsoft Edge“ – https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09
- „Mozzila Firefox“ – https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox?redirectslug=delete-cookies-remove-info-websites-stored&redirectlocale=en-US
- „Google Chrome“ – https://support.google.com/chrome/answer/95647?hl=en
- „Opera“ – https://help.opera.com/en/latest/web-preferences/#cookies
- "Safari" – https://support.apple.com/en-us/HT201265
- "Apple" – https://support.apple.com/en-us/HT201265
- „Android“ – https://turbofuture.com/cell-phones/How-to-delete-internet-cookies-on-your-Droid-or-any-Android-device
- „Chrome“ „Android“ – https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DAndroid&hl=en

Please note that rejecting all cookies may have a negative impact on the use of the Website, such as slowing down the speed of web browsing, limiting the operation of certain functions of the Website or blocking access to the Website.

Stored information about you and your preferences will also be lost, i.e. if you refuse cookies that store your settings, such as your language preference, Website layout, or other personalized information that you can delete when you delete it. This means that the Website will no longer be tailored to your needs, and you will have to re-make these settings every time you visit. No personalized advertising: If you delete or disable cookies that are used for personalized advertising, you may no longer receive personalized advertising. Instead, you'll see generic advertising that may be less relevant to your interests.

We may use the types of cookies described below.

Strictly necessary cookies.
Cookies are necessary for the availability and operation of the Website, which help to analyze the content of the Website and the mobile application on the visitor's device. Necessary technical cookies ensure the functionality of the Website and the mobile application, adaptation to the needs of the visitor. Without these cookies, the operation of the Website may be disrupted and without them it is impossible to use the Website completely freely, therefore there is no possibility to refuse them. Necessary technical cookies do not collect information about visitors that can be used for marketing. The basis for the use of such cookies is Article 73(4) of the Law on Electronic Communications of the Republic of Lithuania, therefore your consent is not required for their use.
Analytical and statistical cookies.
Cookies are used to get to know the visitors of the Website better and to tailor its operation to the needs of visitors. These Cookies enable you to see the most popular offers, news and similar useful information on the Website, help to analyze the activities of the Website, evaluate what has been done correctly, what works perfectly, and what should be improved, therefore they cannot be refused. The information collected by analytical cookies is not individualized, it is used in a generalized way, but such cookies may be used to evaluate the expediency of advertising campaigns available on the Website.

List of cookies used by the bank:

Name of the cookie	Description and type	Moment of creation	Shelf life	Data used
Necessary technical (mandatory) cookies				
wordpress_test_cookie	Cookie to check if your browser accepts cookies	At the moment of opening	While the browser window closes	Not
cookielawinfo	Cookie to remember cookie settings	At the moment of opening	1 year	Not
JSESSIONID	Cookie for session support	At the moment of opening	While the browser window closes	Session ID
Analytical-statistical cookies				
gtm list	The cookie is intended to perform the function of a container from which data is transmitted to Google Tag Manager	At the moment of opening	While the browser window closes	User ID
_gid	A cookie from Google Analytics cookies, used to store a unique ID, to create statistical information	At the moment of opening	Day 1	User ID
_g a	One of the Google Analytics cookies, used to analyze information about how the user uses the website	At the moment of opening	2 years	User ID
_ga_*	Google Analytics sets this cookie to store and count page views. It is	At the moment of opening	2 years	Session ID

	used to persist session state and distinguish unique visits.			
_g at	This cookie is used to collect statistical information about website traffic by Google Analytics	At the moment of opening	1 minute	User ID
_gac _	This cookie is used to collect statistical information about website traffic by Google Analytics	At the moment of opening	90 days	User ID

_glc_au	Google Tag Manager sets the cookie to experiment advertisement efficiency of websites using their services.	At the moment of opening	3 months	Unique Ad Identifier

_hjSessionUser_*	Hotjar sets this cookie to ensure data from subsequent visits to the same site is attributed to the same user ID, which persists in the Hotjar User ID, which is unique to that site.	At the moment of opening	1 year	User ID

_hjSession_*	"Hotjar sets this cookie to hold current session data. This ensures that subsequent requests and interactions within the session window are correctly attributed to the same Hotjar session."	At the moment of opening	1 hour	Session ID

hjViewportId	Hotjar sets this cookie to store the user's viewport dimensions. This ensures that heatmaps and	At the moment of opening	Session (expires when the browser is closed)	Viewport dimensions

	screen recordings are rendered correctly based on the specific screen size of the visitor.			

hjActiveViewportIds	Hotjar sets this cookie to store an ID string for the current session's active viewports. It helps ensure that session recordings and heatmaps remain consistent even if the user has multiple tabs or windows of the website open.	At the moment of opening	Session (expires when the browser is closed)	Viewport ID string

_hjTLDTest	Hotjar sets this cookie to determine the most generic cookie path it should use. This is necessary to ensure that tracking works correctly across different subdomains of the website.	At the moment of opening	Session (expires when the browser is closed)	Test value

_fbp	Facebook sets this cookie to display advertisements when either on Facebook or on a digital platform powered by Facebook advertising after visiting the website.	At the moment of opening	3 months	Unique browser identifier

Marketing cookies

receive-cookie-deprecation	Google sets this cookie to enable Privacy Sandbox testing and preview how site behaviour and functionality work	At the moment of opening	6 months	Testing label

	without third-party cookies.			

ar_debug	DoubleClick sets this cookie to debug and troubleshoot the ads served by DoubleClick. It helps verify that ad conversions are being reported correctly.	At the moment of opening	1 month	Debug signal

IDE	Google DoubleClick IDE cookies store information about how the user uses the website to present them with relevant ads according to the user profile.	At the moment of opening	1 year	Unique identifier
test_cookie	doubleclick.net sets this cookie to determine if the user's browser supports cookies.	At the moment of opening	15 minutes	Check signal

You can control the use of cookies by changing your web browser settings. Every browser is different, so if you don't know how to change your cookie settings, we recommend that you check out its user manuals and instructions.
If you do not want cookies to collect information, please refuse the use of cookies in your browser settings. However, some types of cookies (for example, necessary cookies) are necessary for the proper functioning of the Website, so if these cookies are refused, the Website may lose functionality.

14. Data Acquisition and Disclosure

We **receive** your data directly from you, but depending on the services provided or requested to receive, we may also receive data from other data sources (recipients) listed below. In order to "get to know your customer", we may collect data not only directly from you, but also through the Google search engine, rekvizitai.lt, state information systems and registers (Register of Legal Entities, Information System for Participants of Legal Entities, Information System for Ultimate Beneficiaries of Legal Entities, Population Register, Website of the Chief Official Ethics Commission, World-check database, etc.

When assessing creditworthiness, we receive data from UAB Creditinfo Lietuva and UAB Scorify. We can also verify and receive data from the Real Estate Register and other registers managed by the State Enterprise Centre of Registers.

We also receive data from legal entities when you are a representative, employee, founder, shareholder, participant, beneficiary, management body, etc.;

When we make payments, we receive data from other financial service providers.

Certain of your personal data **may be transferred** to the data processors employed by us (e.g. companies providing data storage services, companies that develop and maintain software, companies providing debt administration services, companies providing communication services, companies providing archiving services, etc.) to whom your personal data may be transferred. We require our data processors to ensure appropriate

protection of your data and ensure that your personal data is processed by the data processors only to the extent that we oblige them and only for the specified purposes.

Personal data may also be transferred to data recipients who act as data controllers, such as the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania, the Bank of Lithuania, law enforcement institutions and other public authorities that we have specified for the specific purposes of personal data processing.

If you have any questions about our data processors, please contact us at the email address provided in the Privacy Policy.

In addition to the specific categories of data recipients set out in this Privacy Policy, we may also disclose information about you:

- if we are required to do so by law (e.g. if we receive an order from a court or law enforcement authority);
- intending to sell a part of the Bank's activities or its assets, disclosing your personal data to a potential buyer of the activity or part thereof;
- in the event of the sale of the Bank's activities or a substantial part of its assets to third parties;
- persons administering joint debtors' data files (e.g., UAB Creditinfo Lietuva);
- Where it is necessary to defend our rights and legitimate interests.

Except as provided for in this Privacy Policy, we do not provide your personal data to any third parties.

15. Transfers to third countries (outside the EU/EEA)

The Bank makes every effort to store your personal data within the EU/EEA. In cases where we need to transfer your processed personal data to a data recipient located outside the EU/EEA, we will seek to ensure that at least one of the following measures is implemented:

- The decision of the European Commission recognises that the state (in which the data recipient is located) ensures a sufficient level of protection of personal data (adequacy decision has been adopted);
- a contract concluded with the data recipient in accordance with the standard contractual clauses approved by the European Commission;
- safeguards are implemented in accordance with the applicable codes of conduct or certification mechanism, and other safeguards are ensured under the GDPR.

In all cases, reasonable efforts are made to ensure that personal data is not lost or unlawfully used in the implementation of the requirements of legal acts.

16. Security of personal data

Your personal data will be processed in accordance with the requirements set out in the GDPR, the Law on Legal Protection of Personal Data of the Republic of Lithuania and other legal acts. When processing your personal data, we implement organizational and technical measures that ensure the protection of personal data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing. However, the security of the transmission of information by e-mail or other means may sometimes not be ensured for reasons beyond our control, so you should exercise caution when providing us with confidential information outside of the systems used by the Bank. Read more about the safe use of the Bank's services and possible fraudulent methods on our **Website**.

17. Responsibility

You are responsible for the confidentiality of the data you provide and for ensuring that the data you provide to us is accurate, correct and complete. If the data you provide changes, you must immediately inform us by e-mail. Under no circumstances will we be liable for any damage caused to you as a result of your provision of incorrect or incomplete personal data or failure to inform us of any changes.

18. Changes to the Privacy Policy

We may update or revise this Privacy Policy at any time. The updated or revised Privacy Policy will come into force from the moment it is published on our Website.

After updating the Privacy Policy, we will notify you of any changes that we consider important by posting them on the Website. If, after posting such notice, you log in to the Website, you will agree to the new requirements set forth in the update. The following "update" date means the date of the last update of the Privacy Policy.

The Privacy Policy was last updated on 11 August 2025. You can consult those earlier versions of the Privacy Policy in our Website.