



European Merchant Bank UAB

Privacy Policy

DOCUMENT SUMMARY

Current version of the Document:

Title	Privacy Policy
Date	3 Dec 2025
Reference-Version Number	5.1
Classification*	Internal
Document Type	Policy
Status	Approved by Management Board
Prepared by:	Compliance Manager
Reviewed by:	DPO, Legal, Management Board

* Highly Confidential / Confidential / Internal / Public categories

Document version History:

Version No.	Date	Changed by	Changes made
1.0	13 Jun 2019	Legal Counsel	New policy
2.0	14 Jan 2021	Head of Legal	Annual review
2.1	12 May 2021	Head of Legal	
2.2	29 Sep 2021	Head of Legal	
3.0	15 June 2022	Legal Counsel	Amendment due to meeting recording purposes and API integrations
4.0	26 May 2023	Legal Counsel	Annual Review
5.0	26 Feb 2025	Compliance Manager	Periodical Review
5.1	3 Dec 2025	Compliance Manager	Amendment regarding contacting designated persons in case of an employee emergency

Contents

I.	WHAT DOES THIS PRIVACY POLICY MEAN?	4
II.	ABOUT BANK	4
III.	WHAT PERSONAL DATA DO WE PROCESS?	4
IV.	PROCESSING RELATED TO THE AML AND KYC PROCEDURES.....	5
V.	PROCESSING IN THE COURSE OF PROVISION OF THE SERVICES OF THE BANK	7
VI.	PROCESSING IN THE COURSE OF ADMINISTRATION OF THE BANK BUSINESS	13
VII.	PROCESSING IN THE COURSE OF EMPLOYEE SELECTION (RECRUITMENT)	17
VIII.	SOURCES OF DATA.....	21
IX.	CONTACT US.....	21
X.	SOCIAL MEDIA	22
XI.	PERFORMANCE OF BANK AGREEMENTS.....	23
XII.	COOKIES	23
XIII.	DISCLOSURE OF DATA.....	23
XIV.	SECURITY OF YOUR PERSONAL DATA	24
XV.	YOUR RIGHTS	24
XVI.	COMPLAINTS.....	26
XVII.	LIABILITY	26
XVIII.	AMENDMENTS TO THE PRIVACY POLICY	26

I. WHAT DOES THIS PRIVACY POLICY MEAN?

This privacy policy (hereinafter the **Privacy Policy**) provides information on the processing of your personal data carried out by the data controller UAB “European Merchant Bank” (hereinafter referred to as the **Bank**). Privacy Policy provides information on the processing of your personal data that are obtained: (i) in the course of becoming a client of Bank and using the services offered by Bank; (ii) in the course of browsing the Website (iii) as Bank conducts surveys and performs direct marketing activities; (iv) when you participate in Bank employee selections; (v) in the course of performance of agreements with partners and suppliers who are legal persons; (vi) when you submit inquiries to us; (vii) as you visit and (or) perform active actions in Bank social media accounts.

Hereinafter all indicated persons whose data are processed by Bank shall be referred to as **‘Customers’**.

II. ABOUT BANK

UAB “European Merchant Bank” (**Bank**), legal entity number 304559043, office address at 35, Gedimino Av., LT-01109 Vilnius, data of the company collected and stored in the Vilnius branch of the Register of Legal Entities of the Republic of Lithuania. Contact details of Data Protection Officer (DPO): dpo@em.bank.

III. WHAT PERSONAL DATA DO WE PROCESS?

Personal data are any information about the Customer collected by Bank that may be used for the Customer identification and is stored electronically or in any other manner.

Personal data include any information, including the Customer’s name, surname, address and IP address, which are collected by Bank about the Customers for the purposes indicated in this Privacy Policy, or in the agreement with Bank, or in the separate privacy notice that is provided to the Customer.

These data shall also include publicly available personal information of the Customers accessed by Bank when the Customer contacts Bank via any social media networks or performs active actions in Bank social media accounts.

IV. PROCESSING RELATED TO THE AML AND KYC PROCEDURES

Whose personal data are processed?	What personal data are processed?	What is the legal basis for such processing?	Who receives the personal data?	How long do we keep the data?
Face-to-face identification of prospective clients, representatives of prospective clients (primary KYC procedure)				
Prospective clients of the Bank, representatives of prospective clients of the Bank (beneficial owners, director and authorised signatories)	Name, Surname, Email Address, Personal Code, Position / connection to the client (beneficial owner, director, authorised signatory), Copy of passport of any country, ID card, issued by an EU and EEA Member Country, residence permit in Republic of Lithuania, Date and time of identification, the Result of identification (is the provided document real or false, the reasons that led to the suspicion of the authenticity of the document)	Article 6(1)(c) of GDPR (legal obligation)	Database of non-valid documents of the Ministry of the Interior	If a person becomes a client - 8 years after the termination of a contract: If a person does not become a client - 3 months from identification procedure
Remote identification of prospective clients, representatives of prospective clients (primary KYC procedure)				
Prospective clients of the Bank, representatives of prospective clients of the Bank (beneficial owners, director and authorised signatories)	Name, Surname, Email Address, Personal Code, Position / connection to the client (beneficial owner, director, authorised signatory), Copy of passport of any country, ID card, issued by an EU and EEA Member Country, residence permit in Republic of Lithuania, Image (photo), Date and time of identification, Result of identification (is the provided document real or false, the reasons that led to the suspicion of the authenticity of the document)	Article 6(1)(c) of GDPR (legal obligation), 9(2)(a) (consent for biometric data - image)	No one	If a person becomes a client - 8 years after the termination of a contract: If a person does not become a client - 3 months from identification procedure

Compliance with anti-money laundering requirements of term deposit clients (Raisin and CHECK24 platforms)

Clients of the Bank (term deposit service)	Name and Surname, Unique customer number, customer investment identifier, POS costumer number, Gender, Salutation, Marital Status, Date, place and country of birth, Nationality, Address, German Tax ID, Whether the person is taxable Germany only, Other tax residencies, additional tax Ids, ID document type, number, and date of expiry, Telephone number, Email address, FATCA (Foreign Account Tax Compliance Act) status, PEP condition, Service bank BIC, Customer service bank IBAN, Product type, Addition screening data (conviction data)	Articles 6(1)(c) (legal obligation), 10 of GDPR (for conviction data)	No one	If a person becomes a client - 8 years after the termination of a contract; If a person does not become a client - 3 months from completing AML procedure
--	---	---	--------	---

Compliance with anti-money laundering and terrorist financing prevention requirements and enforcement of international sanctions (direct clients)

Any client of the Bank, client's manager, shareholder, authorized person, client's business partner	Name and Surname, Email address, Personal code, Date of birth, Taxpayer Identification Number, Address Citizenship, Copy of Identity Document (information provided in Identity Document), Income (employment (salaries, retirement income, self-employed), business earnings, inheritance/family gift, insurance proceeds/settlement, divorce settlement, investment income/returns, winnings (giver mane / non-	Articles 6(1)(c) legal obligation), 6(1)(e) (public interest), 10 (for conviction data) of GDPR, Law on the prevention of money laundering and terrorist financing of the Republic of Lithuania and related implementing legislation	Financial Crime Investigation Service under the Ministry of the Interior, Ministry of Foreign Affairs of the Republic of Lithuania (regarding the breach of sanctions), Database of non-valid documents of the Ministry of the Interior	KYC information of the client - 8 years after termination of business relationship (the last transaction). Additional information received from the client - 5 years after termination of business relationship (the last transaction).
---	--	--	---	--

	government lottery), earnings (sale of business, sale of property), Conviction data			
Creditworthiness assessment and debt management, including obtaining and transferring data to Creditinfo and Scorify				
Client, owners, managers, accountants, of the client, creditors, debtors of the client, employees of the bank	Name, Surname, Email Address, Personal Code, Address, Copy of ID document, Assets, Utility Bill Bata, Bank Statement data, Data provided in Source of Wealth (SOW) Form, Emails (communication), data related to debts and payment history	Articles 6(1)(b) (contract), 6(1)(f) (legitimate interest) of GDPR	UAB "Creditinfo Lietuva", UAB "Scorify"	10 years after the full repayment of the credit

V. PROCESSING IN THE COURSE OF PROVISION OF THE SERVICES OF THE BANK

Whose personal data are processed?	What personal data are processed?	What is the legal basis for such processing?	Who receives the personal data?	How long do we keep the data?
Identification and authentication of individuals				
Clients, representatives of the clients	Personal code, information regarding an individual's consent to perform a specific operation	Articles 6(1)(b) (contract), 6(1)(f) (legitimate interest), 6 (1) (legal obligation) of GDPR; Article 9, paragraph 1 and Article 19, paragraphs 10 and 12 of the Law	SK ID Solutions AS	The personal code will not be retained after the verification/authentication process is complete, but information regarding a

		of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing		person's consent will be stored for a minimum of 8 years in accordance with the provisions of Article 19, paragraph 10 and 12 of the Law of the Republic of Lithuania on the Prevention of Money Laundering and Terrorist Financing
--	--	--	--	---

Concluding a bank account agreement and providing the service

Counterparties to the agreement, their representatives	Name, Surname, Personal Code, Citizenship, Registered address, Correspondence address, Date of birth, Gender, ID document data, Telephone number, Email address, Place of birth, Country of payment of taxes, Taxpayer code	Article 6(1)(b) of GDPR (contract - in case the client is natural person), Article 6(1)(f) of GDPR (legitimate interest to perform contract with the client - in case the client is legal person)	No one	10 years after the termination of a contract
--	---	---	--------	--

Providing mandatory information to the clients

Clients, contact persons of the clients	Name, Surname, Email address	Article 6(1)(c) of GDPR (legal obligation)	No one	Until the end of the contractual relationship
---	------------------------------	--	--------	---

Evaluation of credit awareness of the client

Clients of the Bank, managers, shareholders of the clients	Name, Surname, Personal code, Email address, Phone number, Marital status, Education, professional qualifications, financial data (average salary, obligations, assets)	Article 6(1)(b) (contract - in case the client is natural person) of GDPR, article 6(1)(c) of GDPR (legal obligation) Markets in Financial Instruments Directive, Rules	No one	10 years after the termination of agreement with the client
--	---	--	--------	---

		approved by the Bank of Lithuania		
Issuance of Letter of Guarantee				
Clients of the Bank	Name, Surname, Personal code, Address, Email address, Telephone number, Information about the particular transaction (for which the Letter of Guarantee is necessary): counterparty, amount of transaction, payment date	Article 6(1)(b) of GDPR (contract)	No one	10 years after the end of guarantee term
Creation of the user account in online banking system				
Clients of the Bank, authorized persons of the client	Name and Surname, Personal code, Position, Company, ID document data, Correspondence address, Telephone number, Email address, Account number	Article 6(1)(b) of GDPR (contract - in case the client is natural person), Article 6(1)(f) of GDPR (legitimate interest to perform contract with the client - in case the client is legal person)	No one	Until the deletion of the user account
Cash deposit / withdrawal operations				
Clients, authorised persons of the client	Name, surname, Personal code, Position, company (of representative), Amount of deposit / withdrawal, Date and time of deposit / withdrawal, Number of the respective account	Article 6(1)(b) of GDPR (contract - in case the client is natural person), Article 6(1)(f) of GDPR (legitimate interest to perform contract with the client - in case the client is legal person)	No one	10 years after the end of contractual relationship
Provision of term deposit account service				
Clients, authorised persons of the client	Name, Surname, Personal Code, Company, position (of representative), Deposit account number, Date and time of creation of deposit account,	Article 6(1)(b) of GDPR (contract - in case the client is natural person), Article 6(1)(f) of GDPR (legitimate	No one	10 years after the end of contractual relationship

	Transactional data (amount of deposit, interest (rate and amount), settlement dates (pay-in, pay-out), other relevant transactional data)	interest to perform contract with the client - in case the client is legal person)		
Provision of term deposit service (via Raisin and CHECK24 platforms)				
Clients of the Bank (term deposit service)	Name, Surname, Name of the Service Bank, Transactional data (amount of deposit, interest (rate and amount), settlement dates (pay-in, pay-out), other relevant transactional data)	Article 6(1)(b) of GDPR (contract)	No one	Data stored in Raisin and Check24 platforms – 365 days after Settlement Day; Data stored in the systems of the Bank - 10 years after the settlement date
Internal, SEPA, and Target2 payments (including scheduled bulk payments)				
Counterparties to the bank account agreement	Name, Surname, Address, country, ID document, Telephone number, Email address, Representative of the client, in the event payment is made on behalf of another person - person/'s on behalf of which payment is made, name, code, payment code), Number of the account from which payment is made, Receiver's information (name, code, account number, address), Payer code / purpose of payment, Payment amount	Article 6(1)(b) of GDPR (contract)	No one	10 years after the end of contractual relationship
International (SWIFT) payments				
Counterparties to the bank account agreement	Name, Surname, Address, country, ID document, Telephone number, Email address, Representative of the client, In the event payment is made on	Article 6(1)(b) of GDPR (contract)	Intermediary bank	10 years after the end of contractual relationship

	behalf of another person - person/'s on behalf of which payment is made, name, code, payment code), Banks's information: name, SWIFT code, Number of the account from which payment is made, Receiver's information (name, code, account number), Receiver bank's information (name, SWIFT code), Payment amount, Payer code / purpose of payment			
Providing APIs (Application Programming Interfaces) for payment services providers				
Clients	Name, Surname, address, account number (-s), balance (-s) of the account (-s), transaction information (amount, currency, description (purpose) of payment), token, Receiver's information (full name, account number, payment status	Article 6(1)(c) of GDPR (legal obligation) Article 31(1) (1,2) of Law on Payments of the Republic of Lithuania	Regulated and licenced payment service providers	3 years after the completion of the transaction
Sending reminders about late payments to the client				
Clients, representatives of the clients	Name, Surname, Email address, Company, position (of representative), Personal code, Address, Phone number, Account Number, Information on late payments	Article 6(1)(b) of GDPR (contract - in case the client is natural person), Article 6(1)(f) of GDPR (legitimate interest to perform contract with the client - in case the client is legal person)	No one	10 years after the end of contractual relationship
Restructuring of credit agreements, surety agreements (the purpose is to assess the solvency of the debtor / collateral provider / guarantor and the possibilities of debt repayment), only in restructuring cases of legal entities				
Owners / shareholders / managers of	Name, Surname, Personal Code, Address, Phone number, Email address,	Articles 6(1)(b) (contract), 6(1)(f)	Public authorities, courts, bailiffs	10 years after the end of

corporate debtors; Sureties; guarantors (including holders of promissory notes)	Transaction data, Property (movable and real)	(legitimate interest) of GDPR		contractual relationship
Monitoring of the fulfilment of obligations under concluded credit agreements				
Clients, representatives of the clients	Name, Surname, Email address, Phone number, Address, Correspondence, Other information related with the fulfilment of the obligations under the concluded credit agreements	Article 6(1)(c) of GDPR (legal obligation); Article 31(6) of Law on Financial Institutions of the Republic of Lithuania; EBA Guidelines on loan origination and monitoring	No one	10 years after the termination of agreement with the client
Debt records with the clients / suppliers				
Overdue clients, suppliers whose invoices are overdue	Name, surname, Email address, Personal code, Address, Telephone number, Account number, Overdue amounts	Article 6(1)(c) of GDPR (legal obligation) Law on Accounting of the Republic of Lithuania, Law on Value Added Tax of the Republic of Lithuania	No one	10 years from the date of the particular documents (from the end of the calendar year)
System testing (implementing the business continuity plan)				
Clients, authorized persons of the clients	Name, Surname, Unique customer number, Personal Code, Gender, Position, workplace, Marital Status, Date, place and country of birth, Nationality, Address, ID document type, number, and date of expiry, Telephone number, Email address, Transaction data, User ID, Activity logs, Property (movable and real), Account number, IBAN, Banks's information: name, SWIFT	Article 6(1)(c) of GDPR (legal obligation - Article 32 of GDPR, Clause 99 of the Resolution No. 03-174 of the Board of the Bank of Lithuania of 26 November 2020		The data shall be only processed during the test and after the test will not be stored or processed in any other way.

	code, Number of the account from which payment is made, Payment amount, other payment information, Product type.			
--	--	--	--	--

Direct marketing

Potential clients of the bank, representatives of potential clients of the bank	Name, Surname, Position, workplace, Telephone number, Email address, Linked in URL, location, IP address	Article 6(1)(a) of GDPR (consent)	No one	1 year after the receipt of the consent
---	--	-----------------------------------	--------	---

VI. PROCESSING IN THE COURSE OF ADMINISTRATION OF THE BANK BUSINESS

Whose personal data are processed?	What personal data are processed?	What is the legal basis for such processing?	Who receives the personal data (Data Controllers)?	How long do we keep the data?
------------------------------------	-----------------------------------	--	--	-------------------------------

Litigation

Debtors, representatives of the debtors, other persons potentially violating the rights of the Bank	Name, surname, Email address, Address, Telephone number, Personal Code, Financial information, Marital Status, Assets, Income	Article 6(1)(f) of GDPR (legitimate interest)	Courts, Attorneys	1 year from the date of the final decision of the court
---	---	---	-------------------	---

Handling inquiries, requests, claims submitted by customers or persons related to customers (representatives, etc.)

Persons who submit an inquiry, request, or claim to the Bank	Name, Surname, Personal code, number, place and date of issuance of personal identity document, Telephone number, Email address, Customer's last financial transactions performed in each Customer's Account (date, amount, payer's / payee's names, trade / service company), Other data related to the particular inquiry, request, or claim	Article 6(1)(c) of GDPR (legal obligation) Rules for handling complaints received by financial market participants approved by the Bank of Lithuania	No one	10 years from the end of calendar year during which the particular inquiry, request, or claim was received
--	--	---	--------	--

Organising virtual events / seminars (promotion of the Bank)

Attendees to the events	Name, Surname, Company, Position, Email address, Information on attendance	Article 6(1)(a) of GDPR (consent)		10 working days after the end of the event
Accountability of internal risk management				
Clients of the Bank (specific clients of higher risk)	Name, Surname, Personal code, Internal client's code, Account number	Article 6(1)(c) of GDPR (legal obligation) Resolution No. 03-176 of the Bank of Lithuania on the Approval of the General Provisions on Internal Management of Banks		10 years
Archiving of paper files				
Counterparties, representatives of counterparties	Client files with various personal data	Articles 6(1)(c)(legal obligation, 6(1)(f) (legitimate interest) Rules on archiving		According to the approved documentation plan
Reports to the supervisory authority				
Clients of the EMBank	Name, Surname, Personal code, Client code, Account number	GDPR 6(1)(c) CIR Regulation 575/2013; Regulation 680/2014 - technical standards with regard to supervisory reporting of institutions	European Central Bank	10 years
Clients of the bank, beneficial owners of the clients	Name, Surname, Citizenship, Date of Birth, Personal code, Type and Number of Personal Identity Document, the country of issuance of such document, other information, provided in	GDPR 6(1)(c); Tax Administration Act Art. 55; STI director's order No. VA-61, description of XML scheme of	STI	The data is transferred and no longer stored for this purpose automatically as XML data file

	the STI director's order No VA-61.	MMR-SASK notifications		
Independent AML audit (provision of information to the external auditors)				
Clients of the Bank, persons related to the clients of the Bank (shareholders, members of management bodies), other representatives of the clients	Name, Surname, Personal Code, Client's code, Account number, other information collected for AML and KYC purposes	Articles 6(1)(c) (complying with AML obligations)), 6(1)(f) (legitimate interest to improve AML procedures of the bank)	Auditors	Information that has been submitted to an external audit is no longer stored. The information from which the data were extracted is stored for a further 10 years
Independent financial audit (provision of information to the external auditors)				
Clients involved in an ongoing internal investigation and / or operational risk event	Name and Surname, Information about banking services used by the client, Internal code of the client, Account number, Name and Surname, Personal Code, Internal client's code, Email address, Account number, Account balance, Telephone number	Article 6(1)(c) of GDPR (legal obligation) Article 39 of the Law on the Audits of the Financial Statement	Auditors	Information that has been submitted to an external audit is no longer stored. The information from which the data were extracted is stored for a further 10 years
Debt recovery (assessment of the possibilities of debt recovery)				
Persons whose payments are overdue	Name, Surname, Personal Code, Address, Phone number, Email address, Property (movable and real), Employer and income	Articles 6(1)(b) (contract), 6(1)(f) (legitimate interest) of GDPR	Public authorities, courts, bailiffs	10 years after the end of contractual relationship
Persons whose contracts with the Bank have been terminated with outstanding liabilities; persons against whom the debt collection	Name, Surname, Personal code, Address, Phone number, Email address, Marital status, Account number, Transaction data, Property (movable and real), Employer and income	Articles 6(1)(b) (contract), 6(1)(f) (legitimate interest) of GDPR		

process has already been initiated				
Owners / shareholders / managers of corporate debtors; Sureties; guarantors (including holders of promissory notes)	Name, Surname, Personal code, Address, Telephone number, Email address, Transaction data, Property (movable and real)	Articles 6(1)(b) (contract), 6(1)(f) (legitimate interest) of GDPR		
Internal investigations and operational risk events (analysis)				
Clients involved in an ongoing internal investigation and / or operational risk event.	Name, Surname, Email Address, ID document data, Telephone number, Address, Account numbers / extracts, Services provided by the bank to the particular client, Internal code of the client	Articles 6(1)(f) (legitimate interest), 6(1)(c) (legal obligation) of GDPR Provisions on the Organization of Internal Control and Risk Assessment (Management) of the Board of the Bank of Lithuania (Resolution No. 149 of 25 September 2008). IX Operational risk management Rules for Providing Information on the Internal Management and Activities of Banks to the Bank of Lithuania	External auditors, the Bank of Lithuania	10 years
Fraud prevention				
Clients, authorised persons of the clients	Username of the customer, IP Address, Location, Device Information, Traffic log data, Event ID, channel, Action taken	Articles 6(1)(c) of GDPR (legal obligation); Resolution of the Bank of Lithuania on the adoption	Law Enforcement Authorities	15 months

		of a description of information and communication technology and security risk management requirements; BoL Fraud Prevention Guidelines		
--	--	---	--	--

Drafting the minutes of the meetings of Supervisory Board, Management Board and the committees of the Bank

Employees, third party service providers	Name, surname, position, voting, position on the discussed item, content of the discussions, voice, image.	Article 6(1)(f) of GDPR (legitimate interest)	No one	Until the minutes are drafted (not longer than 20 days after the respective meeting)
--	--	---	--------	--

Contacting designated persons in case of an employee emergency

Employees' designated emergency contacts (family members, relatives, friends, or other trusted persons)	Name, Surname, Relationship to employee, Telephone Number	Article 6(1)(f) of GDPR (legitimate interest)	No one	Retained for the duration of the individual's employment; Deleted immediately upon termination of employment or upon submission of updated emergency contact information
---	---	---	--------	--

VII. PROCESSING IN THE COURSE OF EMPLOYEE SELECTION (RECRUITMENT)

For the purpose of assessing the **non-executive candidates**, the Bank processes the personal data as provided in the table below:

What personal data are processed?	What is the legal basis for such processing?	Who receives the personal data?	How long do we keep the data?
Name, Surname, Personal Code, Identity document information (necessary), Address, Telephone Number,	Articles 6(1)(a) (consent), 6(1)(b) of GDPR (steps prior to entering a contract)	No one	If no employment contract is concluded with the candidate - 3 working days after the end of the selection

Citizenship, Information provided in CV (education, languages, qualifications, former employers)	
Information about qualifications and reputation, sufficient experience and skills to perform the job responsibilities, avoid conflicts of interest, publicly available information (LinkedIn account data, other information found by internet search)	Article 6(1)(f) of GDPR (legitimate interest)
Conviction data	Articles 6(1)(c) (legal obligation), 10 of GDPR, Law of Markets in Financial Instruments of the Republic of Lithuania, Article 34(10), 34(12) of Law of Banks, Articles 8.3, 8.7 of Internal Control and Risk Assessment (Management) Regulations of Bank of Lithuania
Disability data (certificate number)	Articles 6(1)(c) (legal obligation), 9(2)(b) of GDPR
Data obtained from former employer	Article 6(1)(f) of GDPR (legitimate interest of the Bank to evaluate the candidate's suitability for the job)

procedure with below exceptions:

(I) If employment contract is concluded with the candidate (candidate becomes an employee) - 10 years after the termination of an employment contract

(II) For Open Positions: When there is an open position and candidate applies to a specific position, the data will be stored until the end of the recruitment process without receiving consent form. The candidate shall be deemed to have voluntarily consented to the processing of such data by applying to the position. At the end of the recruitment process, candidates who have not been selected for this specific position, but whose experience, personal or other qualities would be appropriate for positions that may arise in the future will be provided with an e-mail request for storing their data in the Bank database for 2 years. The data of the candidates who provided their consent via e-mail will be stored for 2 years. In absence of consent, data will be deleted immediately.

(III) CV Sending Process: From any channel (via linkedin, via e-mail, etc.), when the candidate sends his/her CV, if there

is an open position the process will be same as with aforementioned open position process. If not, the Bank will inform the candidate on how it will process his/her data and ask for explicit consent via e-mail. In the request of the consent, the Bank will inform the potential candidate how the data will be processed and time period of storing such data. If the candidate provides his or her consent, then the data shall be stored in the Bank's database for 2 years. In absence of consent, data will be deleted immediately.

For the purpose of assessing the **executive candidates**, the Bank processes the personal data as provided in the table below:

What personal data are processed?	What is the legal basis for such processing?	Who receives the personal data?	How long do we keep the data?
Name, Surname, Personal Code, Identity document information (necessary), Address, Telephone Number, Citizenship, Information provided in CV (education, languages, qualifications, former employers)	Articles 6(1)(a) (consent), 6(1)(b) of GDPR (steps prior to entering a contract)	No one	If no employment contract is concluded with the candidate - 3 working days after the end of the selection procedure with below exceptions: (I) If employment contract is concluded with the candidate (candidate becomes an employee) - 10 years after the termination of an employment contract. (II) For Open Positions: When there is an open position and candidate applies to a specific position, the data will be stored until the end of the recruitment process
Financial obligations, Data about immediate relatives (degree of kinship, name, surname, year of birth, workplace, position), Information on private interests (name, surname, connection), Information of provision of services to other companies (if any),	Article 6(1)(c) of GDPR (legal obligation), Article 6(1)(f) of GDPR (legitimate interest of the bank to ensure compliance with legal requirements when no specific data necessary to fulfil a legal obligation is listed in legislation), Article 34(10), 34(12) of		

Publicly available information, Real estate, other information about an impeccable reputation, qualifications, and experience required to perform their duties properly, avoid conflicts of interest, ensure independence and be able to devote time to the performance of their duties"	Law of Banks, Articles 8.3, 8.7 of Internal Control and Risk Assessment (Management) Regulations of Bank of Lithuania
Conviction data	Articles 6(1)(c) (legal obligation), 10 of GDPR, Law of Markets in Financial Instruments of the Republic of Lithuania, Article 34(10), 34(12) of Law of Banks, Articles 8.3, 8.7 of Internal Control and Risk Assessment (Management) Regulations of Bank of Lithuania
Disability data (certificate number)	Articles 6(1)(c) (legal obligation), 9(2)(b) of GDPR
Data obtained from former employer	Article 6(1)(f) of GDPR (legitimate interest of the Bank to evaluate the candidate's suitability for the job)

without receiving consent form. The candidate shall be deemed to have voluntarily consented to the processing of such data by applying to the position. At the end of the recruitment process, candidates who have not been selected for this specific position, but whose experience, personal or other qualities would be appropriate for positions that may arise in the future will be provided with an e-mail request for storing their data in the Bank database for 2 years. The data of the candidates who provided their consent via e-mail will be stored for 2 years. In absence of consent, data will be deleted immediately.

(III) CV Sending Process: From any channel (via LinkedIn, via e-mail, etc.), when the candidate sends his/her CV, if there is an open position the process will be same as with aforementioned open position process. If not, the Bank will inform the candidate on how it will process his/her data and ask for explicit consent via e-mail. In the request of the consent, the Bank will inform the potential candidate how the data will be processed and period of storing such data. If the candidate provides his or her consent, then the data shall be stored in the

			Bank's database for 2 years. In absence of consent, data will be deleted immediately.
The manager's questionnaire and other information and documents relevant to the assessment and issuance of the permit by the Bank of Lithuania approved in accordance with the requirements of the Bank of Lithuania	Guidelines for the assessment of the members of the managing body and key function holder of financial market participants supervised by the Bank of Lithuania	Bank of Lithuania	

In the event you have granted your separate consents, the Bank may process your personal data after the selection procedure is over and/or contact your current employer in order to receive their feedback about you as a professional. Detailed information on the processing will be provided in the consent forms.

VIII. SOURCES OF DATA

In the course of its activities, the Bank may collect personal data from various sources other than directly from you. These sources include:

- **Publicly Accessible Sources:** Registers and databases available to the public, such as Population Register, the Register of Legal Persons, the Real Estate Register.
- **Third-Party Service Providers:** Entities that assist in delivering the Bank's services, including credit reference agencies, fraud prevention agencies, and analytics providers such as UAB Creditinfo Lietuva and UAB Scorify.
- **Business Partners:** Organizations the Bank collaborates with to offer products or services, who may share personal data with us in accordance with applicable data protection laws.
- **Other Financial Institutions:** Banks and financial organizations involved in transactions or services you have requested, which may provide us with necessary personal data.
- **Governmental and Regulatory Authorities:** Bodies that provide information necessary for compliance with legal obligations, such as anti-money laundering regulations.

The Bank may also obtain personal data from other natural or legal persons (who, for example, are our customers), judicial institutions, etc.

The Bank ensures that any personal data obtained from these sources is processed in accordance with GDPR requirements and only for purposes outlined in this Privacy Policy. This approach maintains transparency and upholds your rights under data protection laws.

IX. CONTACT US

There are several ways how you can contact Bank: by phone, e-mail, text messages through [Contact Us](#) form on the Website, via social media accounts. We personally accept, review and reply to all messages. If you contact us, we can process the following data belonging to you: name, surname, e-mail address, IP address, phone number, date, your nickname used in social media networks, and text of messages. In the event you contact us

via Contact Us form provided on the Website, you will also be asked to provide the name of the name and size of the company you represent, and your role in such company.

Such data will be processed in order to prepare for the performance of agreement or to answer your questions. If you do not provide your contact details, we will not be able to contact you.

Electronic messages will be stored for 1 (one) year as of the receipt of the last message of the particular conversation except for information that must be stored for other terms pursuant to the Privacy Policy or legal acts.

All personal data provided by you in the course of communication with us will be used only for the aforementioned purposes and to review messages and administer and manage the communication flows. We undertake not to use your personal data without your express consent in any publications in such a way that would allow identifying you.

Please note that we may have to contact you by post, e-mail or phone. Please notify us of any changes of your personal data.

X. SOCIAL MEDIA

Currently, we have the following accounts (hereinafter referred to as **Social Accounts**):

- [European Merchant Bank](https://www.facebook.com/privacy/explanation) account on social network Facebook, privacy notice of which is available at <https://www.facebook.com/privacy/explanation>;
- [European Merchant Bank](https://help.instagram.com/519522125107875) account on social network Instagram privacy notice of which is available at <https://help.instagram.com/519522125107875>;
- [European Merchant Bank](https://www.linkedin.com/legal/privacy-policy) account on social network LinkedIn, privacy notice of which is available at <https://www.linkedin.com/legal/privacy-policy>;
- [European Merchant Bank](https://twitter.com/en/privacy) account on social network Twitter, privacy notice of which is available at <https://twitter.com/en/privacy>;
- [European Merchant Bank](https://policies.google.com/privacy?hl=en-US) channel on social network YouTube, privacy notice of which is available at <https://policies.google.com/privacy?hl=en-US>.

The information you provide to us on social media (including messages, the use of the Like and Follow fields, and other communications) is controlled by the social network manager. We recommend reading the privacy statements of third parties and contact service providers directly if you have any questions about the ways they use your personal data.

Cookies on Social Accounts

When you visit the Social Accounts, the administrators of the social media platforms place cookies on your device, and these cookies collect your personal data. Cookies are placed on your device both in case you are a registered user of the respective social media platform and in case you do not have an account on the respective social media platform. We do not have access to the collected personal data and only receive statistical information about visits to the Social Accounts from the administrators of the social media platforms.

Social media icons plugins

Website uses Facebook, Instagram, LinkedIn, Twitter, and YouTube icon plugins, so by browsing the Website, you agree that we may use your data in our Facebook, Instagram, LinkedIn, Twitter, and YouTube accounts.

XI. PERFORMANCE OF BANK AGREEMENTS

ANK processes personal data of employees of its suppliers or service providers (legal persons) and data of suppliers or service providers (natural persons) in order to perform the agreement concluded between Bank and the aforementioned persons. In such case, Bank will process the following personal data of the aforementioned natural persons: name, surname, date of birth, phone, e-mail address, messaging content, date, and other data related to the performance of the agreement.

The basis for the processing of data of customers, employees of service providers or suppliers of Bank is the legitimate interest of Bank.

If you provide services or sell goods as a natural person, Bank will process your personal data on the basis of performance of the agreement.

Personal data indicated in this section will be processed as long as the agreement is in effect. If personal data are indicated in the agreement, they will be stored for 10 years as of the date of expiration of the agreement.

XII. COOKIES

A cookie is a small text file in alphanumeric format that we place with your consent on your browser or device. We use different cookies for different purposes. Cookies also help us to differentiate you from other users of the Website, thus providing a more pleasant experience of using the Website and allowing us to improve the Website.

A detailed list of the cookies we use, and information on their management is provided in our [Cookie Policy](#). General description of the cookies we use is provided below.

(a) Mandatory/ necessary cookies.

These cookies are necessary for our website to work. The basis of the data processed by such cookies is the proper execution of the contract when you visit the Website, and we ensure the quality and security of the visit. These can be cookies, which, for example, allow you to log in and access secure areas, use the shopping cart feature or e-account services, CloudFlare cookies for DNS and DDOS protection.

(b) Optional/ Non-necessary cookies.

Google Tag Manager, Google Ads or other cookies for Advertising and Marketing purposed and Analytics Cookies. You can change what cookies are stored via your browser, but please be aware that disabling some of the cookies may prevent you from accessing certain features of the website.

XIII. DISCLOSURE OF DATA

We can disclose information about you to our employees, service providers such as debt administration or recovery companies, persons or subcontractors providing marketing and IT services if it is reasonably required for the respective purposes, as indicated in this Privacy Policy.

We may disclose your personal data to third parties, including but not limited to judicial institutions, regulatory and supervisory authorities, governmental agencies, financial and credit institutions, INVEGA (UAB „Investicijų ir

verslo garantijos“), auditors, consultants, third-party service providers, insurance companies, business partners, affiliates, and debt collection agencies in order to comply with legal obligations or to protect our legitimate interests.

We can also disclose information about you:

- if we must do this under the law;
- in order to protect our rights or interests (including the provision of your data to third parties in order to recover your debts to us);
- in order to sell a part of Bank activities or assets, where we disclose your personal data to the potential buyer of the activities or a part thereof;
- having sold the activities of Bank or a substantial part thereof to third parties.

Your personal data may be transferred to data processors (IT infrastructure context) established in the third countries. Such transfer only takes place if (i) the data processor is established in a third country with and adequate level of protection (adequacy decision has been adopted by European Commission), or (ii) other appropriate safeguards, generally, Standard Contractual Clauses, are applied. You can obtain a copy of the document specifying such appropriate safeguards by contacting the DPO of the Bank via the email provided in this notice.

Except in cases provided in this Privacy Policy, we do not transfer your personal data to any third parties.

The list of recipients and categories of recipients provided in the Privacy Policy may change; therefore, if you wish to be notified of any changes to the recipients of your personal data, please inform us via e-mail provided in this Privacy Policy indicating in the e-mail as follows: “I wish to receive information on the changes to the recipients of my personal data, name, surname”.

XIV. SECURITY OF YOUR PERSONAL DATA

Your personal data will be processed pursuant to the requirements set out in the General Data Protection Regulation, the Republic of Lithuania Law on Legal Protection of Personal Data, and other legal acts. In the course of processing of your personal data, we implement organisational and technical measures which ensure the protection of personal data from accidental or unlawful destruction, alteration, disclosure and any other unlawful processing.

XV. YOUR RIGHTS

This section contains information about your rights related to the processing of your personal data carried out by us and cases where you can exercise these rights. If you would like to receive more information on your rights or to exercise them, please contact us via e-mail indicated in this Privacy Policy.

Bank will provide information on actions taken on a request with regard to implementation of your rights without undue delay and in any event within 1 (one) month of the receipt of the request. In consideration of the request complexity and the number of received requests, the aforementioned term may be extended for 2 (two) further months. In this case, we will notify you of such term extension and reasons for it within 1 (one) month as of the receipt of request. Bank will refuse to implement your rights only in cases provided for in the legal acts.

Right to Consent Withdrawal

If you have given us your explicit consent to the processing of your data, you can withdraw it at any time.

Right to Access Your Personal Data

We want you to fully understand how we use your personal data and not to experience any inconvenience because of that. You can contact us at any time and ask if we process any of your personal data. If we store or use your personal data in any way, you have the right to access them. If you wish to do this, please submit a written request to us at the address or e-mail address indicated in this Privacy Policy and confirm your identity. Please comply with the fairness and reasonableness principles when submitting such request.

Right to Request More Information

We hope that you will understand that it is very difficult to discuss all possible methods of collection and use of personal data. We try to provide as explicit and comprehensive information as possible and undertake to update this Privacy Policy if there are any changes to the personal data use process. Nevertheless, if you have any questions about the use of your personal data, we will be happy to answer them or will provide you with all additional information that we can disclose. If you have any specific questions or did not understand the provided information, please contact us.

Additional Rights

Below, you will find information about your additional rights that you can exercise in compliance with the following procedure.

- (a) You have the right to request us to rectify any inaccuracies of data held by us. In this case, we may ask you to confirm the rectified information.
- (b) You have the right to ask us to erase your personal data. This right will be implemented in cases provided in Article 17 of the General Data Protection Regulation (EU) 2016/679.
- (c) You have the right to ask us to restrict the processing of your personal data or to object to their processing:
 - during the period required for us to verify the accuracy of your personal data when you submit claims with regard to data accuracy;
 - in cases of unlawful collection, storage or use of your personal data where you decide not to request the erasure of data;
 - when we do not need your personal data anymore, but you need them for the establishment, exercise or defence of legal claims;
 - during the period required to determine if 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.
- (d) You have the right to the portability of data obtained by us under your consent or for the purpose of agreement conclusion. If you exercise this right, we will transfer a copy of the data provided by you.
- (e) You have the right to object to use of your personal data by us:
 - in cases where we use such data in order to implement our legitimate interests, but we do not have an overriding legal basis to continue using your personal data; or
 - at any time when we use your personal data to send newsletters or for direct marketing purposes. In such case, the data will not be used for these purposes anymore; however, they may be used for other legitimate purposes.

You can read more about your rights as a data subject and exercise them under “Data Subjects’ Rights Implementation Procedure”.

XVI. COMPLAINTS

If you believe that your rights of the data subject have been and/or may be violated, please promptly contact us via e-mail indicated in this Privacy Policy. We ensure that as soon as we receive your complaint, we will contact you within the reasonable period and inform you about the complaint handling process, and then about its result.

If the handling results are unsatisfactory to you, you will be able to submit a claim to the supervisory authority – the State Data Protection Inspectorate (www.ada.it).

XVII. LIABILITY

You are responsible for the confidentiality of your password and submitted data and for any actions (transfer of data, submitted orders, etc.) performed on our website after logging in with your login data. You may not disclose your password to third parties. If a third party who has logged in to the Website using your login data uses services provided on our website, we consider that you are the logged in person. If you lose your login data, you must promptly notify us by post, phone, or e-mail.

You are responsible for the accuracy, correctness and completeness of your data submitted to us. In case of any changes to the data submitted by you, you must promptly notify us about that by e-mail. We will in no way be responsible for the damage incurred by you due to the provision of inaccurate or incomplete personal data or failure to notify us about changes to them.

XVIII. AMENDMENTS TO THE PRIVACY POLICY

We may update or amend this Privacy Policy at any time (at most bi-annually). Such updated or amended Privacy Policy will come into effect as of its publication on our website. You should check it from time to time and make sure that you find the current version of Privacy Policy acceptable.

After making an update to the Privacy Policy, we will notify you about any changes that we consider material by publishing them on the Website. If you log in to the Website after the publication of such notice, you consent to the new requirements indicated in the update. 'Updated on' date indicated below shows the date of the latest update to the Privacy Policy.

The Privacy Policy is to be updated by DPO and approved by the Management Board at least once per 2 years and more frequently whenever changes occur in regulations.

