European Merchant Bank UAB

Data Privacy Policy

Contents

I. OBJECTIVE AND SCOPE

1.1. This Data Privacy Policy addresses general principles and overall responsibilities regarding processing of personal data at the European Merchant Bank UAB (hereinafter referred to as the 'Bank', 'we' or 'us').

1.2. Definitions:

- Personal data means any data that allows directly or indirectly to identify natural person.
- Processing means any action carried out with personal data. For example, collecting, recording, storing, alteration, transfer, etc. regardless of whether it is done by automated means or not.
- Customer means any person who is using or expressed intent to use the Bank's services.
- Group company means any person directly or indirectly controlling the Bank, or a person directly or indirectly controlled by the Bank.

II. PRINCIPLES OF PERSONAL DATA PROTECTION

2.1. The Bank ensures to follow these principles when collecting, receiving and processing your personal data:

2.1.1. lawfulness, fairness and transparency principle: personal data are processed in a lawful, fair and transparent manner;

2.1.2. purpose limitation principle: personal data are collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

2.1.3. data reduction principle: personal data that Bank process is adequate, relevant and not excessive in relation to the purposes for which they are processed;

2.1.4. principle of retention limitation: personal data shall be kept in a form which permits identification of persons for no longer than is necessary for the purposes for which your personal data are processed and also in line with applicable legislation;

2.1.5. principle of accuracy: personal data are accurate and, where necessary, kept up to date;

2.1.6. principle of integrity and confidentiality: personal data is processed in such a way that appropriate technical or organizational measures are taken ensure adequate security of personal data, including protection against unauthorized processing or unlawful processing of data and against unintentional loss, destruction or damage.

III. PURPOSES OF THE PROCESSING OF PERSONAL DATA

3.1. The Bank process personal data for the below reasons:

3.1.1. To identify and verify your identity and implement the principle of "Know Your Customer";

3.1.2. To provide the Bank's services to the Customer (e.g. the Bank uses your personal data, to prepare and conclude an agreement with you);

3.1.3. To determine your creditworthiness;

3.1.4. To comply with a legal obligation to process your data, (e.g. bookkeeping laws; regulatory reporting requirements; statistical data required by competent authorities; other legal requirements);

3.1.5. To provide consultations and evaluate your needs;

3.1.6. To fulfill our contractual obligations;

3.1.7. To maintain relationships and communicate with you;

3.1.8. To ensure compliance with money laundering and terrorist financing prevention requirements and enforcement of international sanctions;

3.1.9. To ensure the quality of provided services and to protect violated rights of the Bank;

3.1.10. To protect rights and legitimate interests of the Bank;

3.1.11. To arrange and conduct the selection of employees and trainees;

3.1.12. To identify you in accordance with the requirements of the law when you are identified without physical presence (e.g., videos and / or photos and processing your image data);

3.1.13. To improve the quality of Bank's services (e.g., data analysis and research to help provide and improve our products, electronic platforms, content and services);

3.1.14. To provide personalized offers or to send direct marketing messages to you we use customer's representative name, surname and email address, which are sufficient to generate personalized offers. You may at any time optout of receiving such marketing messages;

3.1.15. To provide payment services related to the open banking;

3.1.16. In certain situations the Bank may rely on your consent to process personal data. Withdrawal of consent is possible at any time. However, withdrawal of consent might lead to a situation where the Bank might not be able to provide you with certain services or products;

3.1.17. To implement our legitimate interest as a business (e.g. recruitment processes, considering your suitability for employment, taking up references, and conducting appropriate checks; dealing with any legal disputes involving you or other prospective, current or former employees, workers or contractors; contacting former employers for work related or reference related reasons or using in articles, Bank press releases, Bank website and intranet, Facebook and in other our social network accounts, other communication channels of the Bank).

3.2. The Bank processes personal data with accountability, care and diligence. All personal data is processed in line with EU General Data Protection Regulation (GDPR) and on basis for data processing set thereof (e.g. your consent, legal obligation, to conclude and execute the contract concluded with you, legitimate interest).

IV. TYPES OF PERSONAL DATA PROCESSED BY THE BANK

4.1. Individual personal information (e.g. name, surname, date of birth, personal code).

4.2. Individual personal contact details (e.g. address, email address, landline, fax and mobile numbers).

4.3. Identity information (e.g. photo ID, passport, utility bill, national ID card and nationality, biometric data).

4.4. Market research (e.g. information and opinions voluntarily expressed when participating in market research).

4.5. User authentication login and subscription data (e.g. login credentials for online banking and mobile banking apps, and voice print).

4.6. Financial information (e.g. salary, financial liabilities, credit history etc.).

4.7. Information about the usage of Bank's service (e.g. channels used, payment history from and to your account, transaction information, ATM usage information, geographic information, software used and information concerning your complaints).

4.8. Login data while using the internet banking: email address and phone number.

4.9. Any information received from external authoritative registers required for regulatory and compliance purposes.

4.10. Information captured in customer documentation or data exchange such as application forms or advice documents or via telephone (e.g. records of advice).

4.11. Marketing and promotional information (e.g. details of the services and your preferences).

4.12. Cookies and similar technologies used to remember your preferences and tailor content.

4.13. Risk rating information (e.g. credit risk rating and transactional behavior).

4.14. Investigations data (e.g. due diligence checks, sanctions and anti-money laundering, counter terrorist financing, tax avoidance checks).
4.15. Information to fulfill regulatory obligations (e.g. transaction details, user activity).
4.16. Information from other entities (e.g. relevant transaction information).
4.17. Information from third parties providing information to identify and manage fraud.
4.18. Video surveillance in and around the Bank's facilities
4.19. Voice recorded for quality and security purposes through voice call enquiries made at the Bank's Call Center.
4.20. Other information about you that is voluntarily provided by filling in forms or by communicating with us, whether face-to-face or via other available channels (e.g. by phone, email, online, Skype).

V. PERSONAL DATA PROCESSING FOR RECRUITING PURPOSES AND RETENTION PRINCIPLES

5.1. In order to join the Bank's team you may give us personal data about you by filling in forms online, corresponding with us by phone, email, in person, or otherwise, or through a recruitment agency or other third party.
5.2. The Bank will process the data you provide to us as per below rules, so please comply with personal information protection requirements and do not send us excessive information (e.g., personal identification code, health or other special (sensitive) data, financial data, bank account number, family member data, car license plate number, real estate data etc.).
5.3. The Bank ensures to follow these principles when collecting, receiving and processing candidates' data for recruiting process:

- lawfulness, fairness and transparency principle: personal data are processed in a lawful, fair and transparent manner;
- purpose limitation principle: personal data are collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposesand legal requirements;
- data reduction principle: personal data that Bank process is adequate, relevant and not excessive in relation to the purposes for which they are processed under applicable laws;
- principle of retention limitation: personal data shall be kept in a form which permits identification of persons for no longer than is necessary for the purposes for which your personal data are processed and legal requirements;
- principle of accuracy: personal data are accurate and, where necessary, kept up to date;
- principle of integrity and confidentiality: personal data is processed in such a way that appropriate technical or organizational measures are taken ensure adequate security of personal data, including protection against unauthorized processing or unlawful processing of data and against unintentional loss, destruction or damage.

5.4. The Bank will process personal data you present for the purpose of personnel selection, based on your consent, expressed by submitting this data. Our Data Processing will be as follows:

- 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.

- Reference Process: In order to evaluate candidacy, the Bank, in accordance to it's legitimate interest, may contact the former employers which the candidate have indicated for recommendations and consented in advance, and ask them about candidate's qualifications, professional skills and business qualities When the candidate's references are called, it is explained who and how the information is obtained and how these information will be stored. For more detailed information, it is referred to the data privacy policy on the Bank's web site.
- 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.
- All other data obtained from potential candidates shall be deleted immediately.

5.5. Please observe at least the following minimum requirements for the protection of your personal information by sending data to us: do not indicate excessive or unnecessary personal data either in the subject line of the letter or query, in the attached CVs or in motivational letters. in other files: personal identification code, health or other special (sensitive) data, financial data, bank account number, family member data, car license plate number, real estate data, and indicate any other personal data only to the extent necessary for the purposes for which the message is sent.

VI. SOURCES FROM WHERE THE BANK RECEIVES YOUR PERSONAL DATA

6.1. From you (e.g. during the process of submitting application for credit a card, when using services or contacting the Bank).
6.2. From other financial institutions.
6.3. From external sources: the Bank of Lithuania, the Ministry of Finance, the Department of Statistics, Boards of the State Social Insurance Fund, SE Center of Registers, SE Regitra, other registers and state institutions;
6.4. From other persons (e.g. the Bank might receive personal data if you are a representative of the company, from a spouse, from a person for whom you issue a warranty and this warranty is submitted to the Bank etc.).
6.5. From natural or legal persons (e.g., real estate broker, appraisers, notaries, etc.) when they provide them in the performance of contractual or legal requirements of legal acts (property valuation reports, certificates, etc.);
6.6. From legal entities, when you are the representative, employee, contractor, founder, shareholder of these legal entities, participant, owner, etc.;
6.7. From Group companies.

VII. WITH WHOM YOUR PERSONAL DATA COULD BE SHARED

7.1. Shareholders if such sharing is required by law.
7.2. Group companies.

7.3. Third parties that help the Bank to provide services. The Bank only works with reputable service providers (e.g., correspondent banks with which we cooperate, service providers carrying out controls regarding identity verification, SaaS and PaaS providers of the core banking system and the service providers supervising them, IT analyst, IT help desk, cloud computing IaaS providers) who in turn process your data on behalf of the Bank in line with highest professional and technical standards.

7.4. State authorities and other institutions which have right to access your data granted by law.

7.5. Credit rating agencies when the Bank has legitimate interest to determine credit rating.

7.6. Legal advisers.

7.7. External auditors, regulators, authorities.

7.8. Debt collecting agencies.

7.9. Public registers.

7.10. Any entity/person that you gave permission for the Bank to provide with your personal data.

7.11. The Bank could decide to transfer your personal data outside the European Union and European Economic Area (EU/EEA) if third party that provides services to the Bank is outside EU/EEA. In case the Bank transfers personal data to countries outside the EU and the EEA, one of the following security measures applies:

- Obtained permission from the State Data Protection Inspectorate;
- The recipient of the personal data is located in a country recognized by a decision of the European Commission as applying adequate standards of personal data protection;
- The contract signed with the recipient of the personal data would be based on the Standard Contract Terms approved by the European Commission.

The Bank guaranties that your personal data transferred outside the EU/EEA will be protected at the same level as in EU.

VIII. DATA RETENTION

The Bank retains personal data in accordance with the GDPR and applicable legislation. Personal data shall be kept for no longer than is necessary for the purposes for which the personal data are processed. Personal data retention periods are stipulated by applicable laws. Obligation to retain certain documents containing personal data for a specific time period arises on the basis of applicable law.

IX. MANAGEMENT OF PERSONAL DATA BREACHES

9.1. The Bank manages personal data breaches in regard to GDPR, legislation of Republic of Lithuania and internal Personal Data Breach Management Procedure.

X. COOKIES

10.1. When you browse the Bank's website small text files are stored on your computer in order to improve user experience, maintain website's order, and help to increase security. No cookies used by the Bank contains personal data of the website visitor. Our cookies cannot be used for the identification purposes. In management of cookies, We strictly follow all applicable GDPR legislation. Our Cookies Policy is published in the Bank official website for further information and may be subject to change from time to time as per applicable GDPR legislation.

10.2. The folowing are the categoris of Cookies in our Bank's website : (a) Mandatory/ Necessary – CloudFlare cookies for DNS and DDOS protection and (b) Optional/ Non-necessary – Google Tag Manager, Google Ads or other cookies for Advertising and Marketing purposed and Analytics Cookies, Mandatory/Necessary Cookies s are necessary for a website to function normally. 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.

XI. YOUR RIGHTS AND EXERCISE OF THEM

11.1. You have the following rights:

11.1.1. Receive information if your personal data is being processed by the Bank and if so, receive additional information about the processing.

11.1.2. Require your personal data to be corrected if it is inadequate, incomplete or incorrect.

11.1.3. Object to the processing of your personal data (e.g., for direct marketing purposes and when personal data is processed in the legitimate interests of the Bank).

11.1.4. Require the Bank to erase your personal data when the Bank does not have the right or obligation to process your data.

11.1.5. Restrict the processing of personal data.

11.1.6. Receive your personal data that is being processed by the Bank in written or commonly used electronic format.

11.1.7. Withdraw your consent given to the Bank to process your personal data.

11.1.8. Submit your complaints regarding processing of personal data to the State Data Protection Inspectorate (more information - www.vdai.lrv.lt).

11.2. To exercise any of your rights listed above or to exercise other existing rights regarding your personal data, you may contact the Bank's DPO under the following contacts: email: dpo@em.bank, or the office - Gedimino ave. 35, Vilnius.

11.3. The Bank may not enable you to exercise the above rights, when in the cases provided for by the applicable legal acts it is necessary to ensure the prevention, investigation and detection of crimes, violations of official or professional ethics, as well as the protection of the rights and freedoms of others.

11.4. The Bank undertakes to examine your requests and provide information no later than within one month from the date of your request.

11.5. In case your requests are manifestly unfounded or disproportionate (for example, due to their repetitive content), the Bank is entitled to charge a reasonable fee, taking into account the cost of providing the information.

XII. DATA STORAGE AND SECURITY

12.1. Your personal data will be processed only for a period that is necessary for data processing purposes and whereas retention periods are stipulated by applicable laws. In some case personal data could be saved for different period due to legal requirements (e.g., preventing money laundering and terrorist financing, taxation, accounting or employment legislation). The Bank will store your personal data for 10 years after contractual relationship with you have ended.

12.2. The Bank uses organizational and technical security measures to protect your Personal Data such as policies preparation, observance, implementation and review on an annual basis, whereas policy on data protection reviews every 6 months; employees training on data protection; limiting access to your Personal

Data; secured networks; SSL encryption; web application firewall; protects against DDoS; and any other organizational and technical measures required by law. We ensure that your Personal Data is protected against unauthorized access, disclosure, or destruction by utilizing practices that are consistent with standards in the industry to protect your privacy.

12.3. Although the Bank takes the protection and storage of your Personal Data very seriously, and all reasonable steps to protect your Personal Data, there might occur data breaches outside of our reasonable control. In case there would be an event of data breach, we would follow all applicable laws, including taking reasonable measures to mitigate any harm as well as notifying you of such breaches as soon as possible but no later as it is required by law.

XIII. BANKS' OBLIGATIONS

13.1. The Bank undertakes to process your data under the following conditions:

13.1.1. Only for clearly defined and legitimate purposes;

13.1.2. Not to process your personal data for purposes other than those specified in this Policy, except as provided by law;

13.1.3. To process your personal data lawfully, accurately, transparently, fairly and in such a way as to ensure the accuracy, identity, security of personal data;

13.1.4. To ensure that redundant personal data are not processed;

13.1.5. To process your personal data for no longer than is necessary for the purposes for which the personal data are processed;

13.1.6. To be responsible for ensuring that the principles enshrined in this Policy are complied with and be able to demonstrate compliance;

13.1.7. To perform other duties provided for in legal acts.

XIV. CONTACT US

14.1. European Merchant Bank UAB, registered address Gedimino ave. 35, LT – 01119, Vilnius. Email: info@em.bank, phone 8 700 11 200. 14.2. Bank's website: https://em.bank

XV. FINAL PROVISIONS

15.1. This Privacy Policy is up to date and effective from 12 May 2021.

15.2. The Bank may update this Privacy policy on a regular basis. The Bank shall notify you 30 days in advance if any substantial changes are being implemented. Updates to this Privacy policy will come into power after it is posted on the Bank's website.

15.3. The Privacy policy is reviewed, updated and approved at least every 6 months. In the course of the review of the Privacy Policy, the self-risk assessment, internal and external audit reports shall be taken into account.

15.4. This Privacy Policy is published on the Bank's website https://em.bank, and this Privacy Policy is also available at the Bank's department.

15.5. After updating the Privacy Policy, we will inform you about it by publishing a notice on the Bank's website https://em.bank and by other means.