

PRIVACY POLICY

Effective date: 25.10.2022

1. GENERAL PROVISIONS

- 1.1. UAB “Pervesk”, company code 304186270, with its registered office at Gedimino Ave. 5-3, LT-01103 Vilnius, the Republic of Lithuania (“**Pervesk**”, “**Company**”, “**we**” or “**us**”) is a licensed electronic money institution (electronic money institution license No. 17, Issuing and Supervisory Authority – Bank of Lithuania), which directly or through the intermediaries provides services which are allowed under our electronic money institution license and which are described on the website www.pervesk.lt (the “**Services**”). Services accessible via finrax.com, as well as special internet banking platform, accessible via domain ib.finrax.com, are provided by the Company which uses trademark “Finrax” and acts as a partner of Finrax only with regards to the provision of the Services. Services may also be available through our or our intermediaries’ internet banking systems (ib.pervesk.lt, ib.bankera.com or other), mobile apps or application programming interfaces (all of them or any of them hereinafter may be referred to as the “**Platform**”). The Services that Pervesk provides are subject to the relevant terms and conditions, which are presented in the respective Platform.
- 1.2. In order to provide Services, we may process personal data of our customers, their clients or representatives, other related persons, such as beneficial owners, transaction senders, etc. (all together referred to as “**Customer**” or “**you**”). Any personal data we gather, use or share about you is processed in accordance with the Regulation (EU) 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**”) and other applicable laws.
- 1.3. This Privacy Policy (“**Policy**”) applies to your use of the Platform and any of Services, available through it. The Policy explains how we process your personal data through any relationship we have, whether it would be use of the Services on the Platform, online support services or any other possible means. In case you provide information about other natural persons to the Company, you undertake to make this Policy known to them before the disclosure of such information to the Company.
- 1.4. By contacting us, using this Platform and / or our Services you confirm you have read, understood and agreed with this Policy.

2. PRINCIPLES OF PERSONAL DATA PROCESSING FOLLOWED BY THE COMPANY

- 2.1. The Company undertakes to ensure your personal data is:
 - 2.1.1. processed lawfully, fairly, and in a transparent manner in relation to you;

- 2.1.2. collected for specified, explicit and legitimate purposes (f. e. prevention of money laundering and terrorist financing, performance of Services, etc.), and not further processed in a manner that is incompatible with those purposes;
 - 2.1.3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - 2.1.4. accurate and, where necessary, kept up to date;
 - 2.1.5. kept in a form which permits your identification for no longer than is necessary for the purposes for which the personal data are processed;
 - 2.1.6. processed in a manner that ensures appropriate security of your personal data.
- 2.2. The Company follows the above indicated principles strictly during the processing of your personal data and requests the same from the data processors which it may use to process personal data on behalf of the Company.

3. LAWFULNESS OF PERSONAL DATA PROCESSING

- 3.1. Your personal data will be processed if:
- 3.1.1. you have given consent to the processing of your personal data for one or more specific purposes; and/or
 - 3.1.2. processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract; and/or
 - 3.1.3. processing is necessary for compliance with a legal obligation to which we are subject; and/or
 - 3.1.4. processing is necessary for the purposes of the legitimate interests pursued by us or the third party;
 - 3.1.5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.
- 3.2. If Services are allowed by us and available for the child under the age of 16, their personal data will be processed only with the consent of the holders of parental responsibility, and only to the extent that such consent or permit is given.
- 3.3. The Company may subject its Customers to decisions based solely on automated processing, including profiling, only if it is necessary for conclusion of a contract between you and the Company or due to provision of the Services under such contract, it is authorised by the law or you have expressed an explicit consent to such processing.

4. PURPOSES FOR THE COLLECTION AND USE OF YOUR PERSONAL DATA

- 4.1. Your personal data is being processed for the purposes of:
- 4.1.1. provision of the Services (account opening, transfers of funds, payment collection and other payment services);
 - 4.1.2. prevention of money laundering and terrorist financing (implementation of the principle "Know Your Customer");
 - 4.1.3. implementation of international sanctions;
 - 4.1.4. direct marketing;
 - 4.1.5. Services support;
 - 4.1.6. quality assurance;
 - 4.1.7. call recording;
 - 4.1.8. use of the Company's social networks accounts;
 - 4.1.9. proper and secure use of the Platform and of Customer's online account.
- 4.2. The processing of your personal data is necessary for the implementation of the above indicated purpose(s), therefore, if you fail to provide the requested data the Company may not be able to provide your requested Services.

5. METHODS OF PERSONAL DATA COLLECTION USED BY THE COMPANY

- 5.1. The Company collects your personal data directly from you or from the third parties when:
 - 5.1.1. you use or view the Platform;
 - 5.1.2. you register to the Platform;
 - 5.1.3. you request or use our Services;
 - 5.1.4. you request Services support;
 - 5.1.5. you call to us and consent to the call being recorded;
 - 5.1.6. we execute Customer's due diligence or ongoing due diligence;
 - 5.1.7. we monitor your transactions;
 - 5.1.8. we check whether you are not related to fraudulent activities;
 - 5.1.9. we receive requests, orders, decisions or etc. from the third parties regarding you;
 - 5.1.10. authorized third parties have provided your personal data.
- 5.2. In order to ensure smooth delivery of the requested Services or keep you updated about our news, the Company may also collect your personal data and renew personal data related to Customer's profile based on the up-to-date information received from the data controllers and / or the respectable third parties wherein you have already initiated or have an account, partners that process your contact details or public registers, sources.

6. CATEGORIES OF PERSONAL DATA THE COMPANY MAY PROCESS ABOUT YOU

- 6.1. The scope of the Customer's personal data indicated below which could be requested by the Company and further processed in order to provide the Services for the purposes indicated in article 3 of this Policy may vary depending on the type of Services chosen particularly by the Customer and Company's applied verification procedures to execute it, as well as, legal requirements applied for such provision of the Services in order to prevent possible risks and various crimes.
- 6.2. In order to provide the Services, we may process your personal data categories, such as (including but not limited):
 - 6.2.1. **General data:** name, surname, personal code, date of birth, citizenship(s), place of birth (city, country), country of residence for tax purpose, taxpayer identification number (TIN), address, city/town, postal code, phone number, e-mail, selfie with the identity document, video, data about Customer which may be provided in double-checking systems;
 - 6.2.2. **Other Customer's profile information:** profile type, unique character sequence assigned to the Customer for identification, executed Customer's assessment (evaluation) results, chosen means of identification, 2FA information, Customer's number, user ID, referral code, referral ID, session ID, login status, email confirmed status, phone confirmed status, compliance officer comments;
 - 6.2.3. **Social network data:** social network profile photo, name, surname, your comments, emotions and other actions expressed via our social network account, other your social network profile information provided by you;
 - 6.2.4. **Identity document data:** ID Type (Passport / Identity Card / Residence permit), its copy, MRZ, document number, date of issue, date of expiry;
 - 6.2.5. **Data obtained and/or created while performing legal obligation:** inquiries, requests, notifications, orders, courts decisions or other data related to the specific Customer(s) which may be received by or provided to the police, courts, investigative bodies, notaries, tax administrator, courts, bailiffs and other institutions;
 - 6.2.6. **Information about Customer's occupation and income sources:**
 - 6.2.6.1. Specific occupation: paid employee (position) / owner of legal entity (company name) / registered self-employee / unemployed / other;

- 6.2.6.2. Main sectors of customer's occupation, individual or business activity;
- 6.2.6.3. Information regarding countries in which customer is employed, carries out individual activity or business: countries, whereas activity or business is conducted or registered in preferential tax zone, percentage of turnover in cash for such activity or business;
- 6.2.7. Payment account opening information:**
 - 6.2.7.1. Purpose for account opening;
 - 6.2.7.2. Source of Customer's income and wealth;
 - 6.2.7.3. Services which the Customer plans to use
 - 6.2.7.4. Monthly planned account turnover in EUR;
 - 6.2.7.5. Number of transactions and countries from which the funds will be received or transferred;
 - 6.2.7.6. Account number;
- 6.2.8. Information about Politically Exposed Person ("PEP"):**
 - 6.2.8.1. Information whether the Customer is PEP itself or has an immediate relationship with PEP;
 - 6.2.8.2. General information regarding PEP: relation, name, surname, country, institution, PEP's position;
- 6.2.9. Information about Beneficial Owner ("UBO"):**
 - 6.2.9.1. Information whether the Customer is the UBO of the account and the funds in the account;
 - 6.2.9.2. General UBO's identification data: name, surname, ID copy, date of birth, personal code, citizenship, country of residence for tax purposes, tax identification number (TIN), place of birth (city, country), registered residential address, share of benefit;
- 6.2.10. Financial data:**
 - 6.2.10.1. related payment card (i.e. currency, card number, validity date, card owner's name and surname, CVV/CVV2);
 - 6.2.10.2. Customer's account information (e.g., services, transactions type, sender, recipient, amount, purpose, extracts, etc.)
 - 6.2.10.3. information about accounts in other financial institutions (i.e. name of institution, country, account number);
 - 6.2.10.4. Customer's creditworthiness information (i.e. creditors, type of debt and its amount, due dates, debtor's identification number, etc.).
- 6.2.11. Communication data:** date, time, correspondence, video and voice calls, chats, etc.
- 6.2.12. Information related to electronic devices:** IP address(es); time zone; log-in and log-out register; browser information; electronic device's operational system information; location data (country (code), city), internet service provider (ISP); selected language; information regarding Customer's actions within Platform;
- 6.2.13. History data:** Customer's experience using the Platform, the register of all Customer's actions performed on the Platform (i.e. operations, such as funds transactions, linking cards, log-in and log-out register, register of reset password),;
- 6.2.14. Call recording data:** the record of the call, including the representation of the agent and the caller, as well as, all information discussed during the call, data and time of the call, caller's telephone number, agent number;
- 6.2.15. Other data which may be requested or gathered by the Company or provided by the Customer herself/himself or any third party.**

7. DISCLOSURE OF PERSONAL DATA TO OTHER PARTIES

- 7.1. Your personal data indicated in article 6 of this Policy may be provided by the Company itself or upon respective request to the below indicated categories of personal data recipients:
 - 7.1.1. credit, financial, payment and (or) electronic money institutions, agencies, bureaus;
 - 7.1.2. payment services providers, as well as intermediary services providers;
 - 7.1.3. authorities (i.e. supervising institutions, law enforcement institutions, courts, bailiffs);
 - 7.1.4. auditors, legal and financial consultants;
 - 7.1.5. IT providers;
 - 7.1.6. marketing service providers;
 - 7.1.7. telecommunication and call recording service providers;
 - 7.1.8. fraud detection services providers;
 - 7.1.9. data processors;
 - 7.1.10. related business partners, agents;
 - 7.1.11. other service providers which services may include, or which are engaged in personal data processing executed by the Company.
- 7.2. Personal data may also be provided to other recipients if:
 - 7.2.1. the Company has to comply with a legal obligation to which it is a subject; or
 - 7.2.2. such requested personal data is necessary for the concrete data recipient to carry out a particular inquiry in the general interest, in accordance with the European Union or Member State law; or
 - 7.2.3. the data requesting party has a legitimate interest to request for such information;
 - 7.2.4. other grounds indicated in Article 6 of GDPR are applied.
- 7.3. The Company maintains strong cooperation with local and international authorities and institutions, therefore, upon request of such party substantiated under article 7.2. of this Policy, your personal data may be provided to the requested party without permission to notify you.
- 7.4. In general, the Company processes your personal data within the European Union ("EU") or the European Economic Area ("EEA"), however, there might be some cases when the Company cooperates with the recipients outside EU or EEA. In such cases the Company makes all reasonable efforts to ensure that at least one of the following GDPR requirements is complied:
 - 7.4.1. the recipient is located in the territory which is acknowledged by the European Commission as ensuring the adequate level of personal data protection;
 - 7.4.2. the Company and the recipient have concluded the Standard contractual clauses regarding personal data transferring which were approved by the European Commission;
 - 7.4.3. the Codes of Conduct or other measures indicated in Chapter V of GDPR have been complied.

8. PERSONAL DATA RETENTION PERIOD

- 8.1. The Company processes personal data so that it could achieve the purposes indicated in article 4 of this Policy.
- 8.2. In order to set the below indicated data retention periods the Company has referred to the legal acts and public recommendations applicable in the European Union and locally such as compliance with legit limitation periods, as well as current business practice.
- 8.3. Depending of the category of personal data and the purpose it is being processed your data retention period applied within the Company as it is required by the law or business practice to ensure smooth delivery of the Services is:
 - 8.3.1. for the purposes indicated in articles 4.1.1 – 4.1.3 of this Policy we process your personal data throughout the term of our contractual relationship and

store it after this relationship ends for as many years as it is required by law (for example, it may be required to store your personal data for 8 years, whilst the concluded service contract itself with the personal data therein may be necessary to store for 10 years after the contractual relationship ends). The personal data processing for such a period is based on necessity to execute Customer's due diligence, conduct ongoing monitoring, collect supporting evidence and records of transactions. In case the contractual relationship has not been established based on reasons not related with prevention of money laundering and terrorist financing (e.g., you decided not to finish application or verification procedure due to your own personal reasons) your personal data will be stored for 2 years since the last contact with you or action from your side;

- 8.3.2. for the purpose indicated in article 4.1.4. we will process your personal data as long as you are registered to use the Services and / or have contractual relationship with us, except in cases when you have objected to such processing, terminated the contractual relationship, requested erasure of your personal data or other provisions for data erasure have been applied.
 - 8.3.3. for the purposes indicated in article 4.1.5 – 4.1.6 we process your personal data collected via correspondence with you throughout the term of our contractual relationship and store it after this relationship ends for as many years as it is required by law (for example, it may be required to store such data for additional 5 years). In case you have not established or has already terminated contractual relationship with Pervesk, your personal data will be processed for these purposes for a period of 2 years since our last actual contact with each other (e.g., our last email to you answering your request);
 - 8.3.4. the purpose indicated in article 4.1.7. your personal data will be processed for 6 months since the date the record of the call has been made;
 - 8.3.5. for the purpose indicated in article 4.1.8. we process your personal data until your social network account or Company's social network account is deleted – whichever comes first;
 - 8.3.6. for the purposes indicated in article 4.1.9. we process your personal data throughout the term we support the Platform.
- 8.4. Upon the end of the retention period, indicated above, your personal data is erased or anonymised (irreversibly).

9. DIRECT MARKETING

- 9.1. In order to provide you generic or personalized up-to-date news about our Services, inform about current proposals and / or ask your opinion about the Services, your email address and / or telephone number might be processed by the Company for direct marketing purposes.
- 9.2. We process your personal data for direct marketing purposes based on legitimate interest by complying with applicable laws and regulations. We may also send profiled direct marketing material based on legitimate interest and categorization of your profile information (such as customer's type, last login, last transaction time, Services being ordered / used, source used for accessing the Services, customer's verification status, residing country, transaction information (amount, number, etc.), use of referral code / link) in order to inform you about the news that may be mostly interesting and relevant to you and / or ask your opinion about the specific Services.
- 9.3. In order to send you the direct marketing material we may engage our agent(s) and / or use third party services and share your email address and / or telephone number with them.
- 9.4. Your contact details, indicated in article 9.1, will be processed for the period indicated in article 8.3.2 of this Policy.
- 9.5. You shall have a right to object at any time to processing of your personal data for the purpose of direct marketing, which includes profiling to the extent that is related to

such direct marketing, by changing the settings in your profile, clicking on the withdrawal link provided in the received newsletters or by sending us a request at the contacts provided in the Platform.

10. INFORMATION SECURITY

10.1. The Company takes various security ensuring technologies and procedures in order to protect your personal data against unauthorised or unlawful processing, accidental loss, misuse, unauthorized access, illegal usage, destruction, disclosure, damage, etc. This includes legal, organisational, technical, and physical security measures, such as latest security systems, two-factor authentication and passwords, ability to detect cyber security attacks and other threats to the integrity of the Platform, working only with trustworthy service providers, etc. However, no transmission of information via e-mail or other telecommunication channels or your access to the Platform or the Services through the internet could be fully secured. Therefore, you should take due care when you are accessing the Platform or using the Services via the internet or sharing confidential information via e-mail or other telecommunication channels.

11. COOKIES

11.1. Cookies are small information files found in the Platform you visit and stored in your computer or mobile device. In order to get to know more about cookies, please read Cookie Policy on the Platform.

12. YOUR RIGHTS REGARDING THE PROCESSING OF YOUR PERSONAL DATA

12.1. You have certain legal rights in relation to the processing of your personal data, including:

12.1.1. the right to obtain confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information regarding its processing;

12.1.2. the right to obtain from us without undue delay the rectification of inaccurate personal data concerning you and, taking into account the purpose of the processing, the right to have incomplete personal information completed;

12.1.3. the right to obtain from us the erasure of personal data concerning you without undue delay if one of the grounds set out in article 17 of the GDPR applies;

12.1.4. the right to obtain from us restriction of processing where one of the grounds set out in article 18 of the GDPR applies;

12.1.5. the right to data portability in accordance with article 20 of the GDPR;

12.1.6. the right to object at any time to processing of your personal data in accordance with article 21 of the GDPR;

12.1.7. the right not to be subject to automated individual decision-making, including profiling in accordance with article 22 of the GDPR.

12.2. The Customer should be aware that the above indicated rights may not be absolute – it depends on the particular Customer's request and the purpose and / or basis for his / her personal data processing. Also this Policy does not deprive you of any other legal rights you may enforce under the applicable law.

12.3. The Customer may exercise his / her rights only after the Company has successfully identified him / her. If the Company is not sure about the identity of the person sending the data request, the Company may not provide the requested information to him / her, unless the Customer's identity is confirmed. Therefore, if you would like to address a request towards the company regarding execution of your rights, we suggest you do once you are logged in to your personal account on the Platform (so that we could identify you). In case you decide to use other communication channels, such as sending a request via email, kindly ask you to indicate in the e-mail your name, surname, your date of birth and the last four digits of your identity document number

which you used when entering into a contractual relationship with the us. In addition, the Company keeps the right to decide if the other or additional legitimate means of identification proof should be requested, such as a selfie with your ID document, certified copy of your ID document, video or voice call, or any other additional document or method which could let to determine your identity.

- 12.4. The Customer is provided with information related to the exercise of his / her rights free of charge. However, the Customer's request for the exercise of rights may be waived or may be subject to an appropriate fee if the request is manifestly unfounded or excessive, in particular because of their repetitive character.
- 12.5. The Company shall provide the Customer with information on the actions taken upon receipt of the Customer's request for the exercise of his rights or the reasons for the inaction no later than within 1 month from the receipt of the request. The period for submitting the requested information may be extended, if necessary, for 2 more months, depending on the complexity and number of requests. When the Customer submits the request by electronic means, the information shall also be provided by electronic means.
- 12.6. If the Customer considers that his / her personal data is being processed in violation of his / her rights and legitimate interests in accordance with applicable law, the Customer shall have the right to file a complaint against the processing of personal data to the State Data Protection Inspectorate of the Republic of Lithuania.

13. YOUR RESPONSIBILITIES

- 13.1. You confirm that you have provided correct data about yourself in every required form and that afterwards, when changing or adding any data at the Platform, you will enter only correct data. The Company will not tolerate invalid, false or otherwise incorrect data and will pursue actions in accordance with its legal obligations. You shall bear any losses that occur with regard to the submission of invalid, false or otherwise incorrect data.
- 13.2. You are responsible for maintaining adequate security and control of every identification number, password, and / or any other code that you use to access the Platform. If you have not complied with this obligation and / or could, but have not prevented it and / or performed it on purpose or due to own negligence, you assume the losses and undertake to reimburse the losses of other persons incurred as a result of your (in)action.
- 13.3. In the event of loss of any password by yourself or if the password(s) are disclosed not due to your or Company's fault, or in case of a real threat that has occurred or may occur to your account, you undertake to change the password(s) immediately or, if you do not have a possibility to do that, not later than within 1 calendar day notify the Company. The Company shall not be liable for consequences that have originated due to the notification failure or unauthorised access to your account not due to the fault of the Company.
- 13.4. After the Company receives the notification from you as indicated above, the Company shall immediately suspend access to your account and provision of the Company's Services until a new password is provided / created for you.
- 13.5. The Company draws your attention to the fact that your user ID, email address or any other contact information you have chosen to link to your account are used for your identification and communication. You undertake responsibility to protect these instruments and logins to them. You are responsible for password disclosure and for all operations performed after you use the password for a relevant account. We recommend memorizing your passwords and not to write them down or enter anywhere where they may be seen by other persons.

14. CONTACT DETAILS

- 14.1. If you have any questions regarding this Policy or your personal data protection or if you want to withdraw your consent, or execute your rights you may contact our Data

Protection Officer who monitors that your data processing executed by the Company complies with the applicable data protection laws. You can reach our Data Protection Officer via e-mail: dpo@pervesk.lt or mail via postal address: UAB "Pervesk", address Gedimino Ave. 5-3, LT-01103 Vilnius, the Republic of Lithuania, with a notice "Data Protection Officer".

15. FINAL PROVISIONS

- 15.1. This Policy shall be viewed and applied in accordance with the GDPR and other applicable laws.
- 15.2. The Company reserves the right to make changes to this Policy from time to time. An up-to-date version of the Policy is posted on the Platform, therefore, please do review it regularly. Your continued use of the Platform and Services following any such revisions to the Policy will constitute your acceptance of such changes. If you do not agree to any such of such changes, do not continue to use our Services.
- 15.3. The Company is not responsible for ensuring clients' privacy in third parties' websites, even in cases where the client has accessed third-party websites by using links provided on the Platform. The Company recommends that you familiarize yourself with the privacy policies of third-party websites" beforehand.