PRIVACY POLICY

1. PURPOSE AND SCOPE

1.1. NTJ UAB, legal entity code 306169597, registered address at Konstitucijos ave. 7, LT-09308, Vilnius, Lithuania (hereinafter – the Company, we or us) is a Company duly incorporated under the laws of the Republic of Lithuania acting as the administrator of the Platform available at www.safe2transact.com, which enables access to the financial services provided by duly authorised third parties.

1.2. In any case, all personal data collected by us is processed in accordance with the EU General Data Protection Regulation No. 2016/679 (**GDPR**), Law on the Legal Protection of Personal Data of the Republic of Lithuania and other applicable legal acts.

1.3. In this Privacy Policy, we provide you with explanation on what kind of personal data we collect when providing you with access to the Platform, what the purposes of such processing are, and what rights you have in respect of your personal data.

1.4. When writing 'you', we mean you as – a potential, existing or former client, our client's employee or other parties, such as beneficial owners, authorised representatives, business partners, our merchant's clients, other associated parties or a person contacting us by e–mail or using other communication means.

2. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

2.1. We are responsible for ensuring security of your personal data made available to us, in particular to prevent unauthorized access to your data.

2.2. When processing personal data, we follow the principles of:

- legality, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality.

3. WHAT INFORMATION WE COLLECT, FOR WHAT PURPOSES AND ON WHAT LEGAL BASIS

3.1. Categories of personal data being processed

3.1.1. The personal data we collect can be grouped into the following categories:

Category	Personal data elements
1. Basic personal data	First, last, middle name, job title.
2. Identification information and other background verification data (your, or your representatives' and, ultimate	Name, surname, personal identity code, date of birth, any other unique sequence of symbols granted to you, intended for personal identification, country of birth, address, nationality (in the case of a stateless person – the state which issued the identity document), citizenship, gender, copy of passport or ID card and its details (e.g., type, number, place and date of issuance, expiry date, MRZ code, signature), evidence of beneficial ownership or the source of funds (funds for account opening or transactions, occupation/employment information), source of wealth

Category	Personal data elements
beneficiary owner's)	(information on how wealth was obtained), tax information (tax residence, tax identification number), number of shares held, voting rights or part of share capital, title, visually scanned or photographed image of your face or image that you provide through a mobile or desktop camera while using our identification application, video and audio recordings for identification.
3. Details of your activities on your account or mobile application	History of the actions performed on your account, mobile application, technical information, including the internet protocol (IP) address used to connect your computer to the internet, your log-in information (e.g., login time), browser type and version, time-zone setting, operating system and platform, type of device you use, unique device identifier.
4. Details of your activities on our website	History of the actions performed on our website, technical information, including the internet protocol (IP) address used to connect your computer to the internet, time zone setting, operating system and platform.
5. Information related to legal requirements	Data resulting from enquiries made by the authorities, data that enables us to perform anti-money laundering requirements and ensure the compliance with international sanctions, including the purpose of the business relationship and whether you are a politically exposed person and other data that is required to be processed by us in order to comply with the legal obligation to "know your client" (collected data will differ depending on the client's risk score)
6. Contact details	Phone number, e-mail, residential address
7. Special category data	Biometric data

3.2. Purposes and legal basis for personal data processing

Purpose	Legal basis	Categories of personal data
1. To identify you remotely	• Your consent	• Special category data (biometric data)
2. To prevent, limit and investigate any misuse or unlawful use or disturbance of the Services or to establish, exercising and defend legal claims	• Performance of the contract; • Legitimate interest – defend against legal claims and prevent fraud; • Legal obligations – Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania	• Basic personal data; • Identification and other background verification data; • Monetary operation details; • Details of your activities in your website account or mobile application; • Details of your activities in our website; • Details of your existing bank account/-s; • Information related to legal requirements; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing Services).

Purpose	Legal basis	Categories of personal data
3. To ensure adequate provisions of the Services, the safety of information within the Services, as well as to improve, develop and maintain applications, technical systems and IT-infrastructure or our legitimate business interests, such as enabling us to improve and deliver a better and more personalised service	• Legitimate interest - to improve and deliver a better and more personalised service.	• Basic personal data; • Contact details; • Details of your activities in your website account or mobile application; • Details of your activities in our website; • Other personal data needed (in order to evaluate the possibility of providing Services).
4. To provide an answer when you contact us via our website or other communication means	• Legitimate interest – to provide good customer service.	• Basic personal data; • Contact details; • Other personal data needed (in order to evaluate the possibility of providing Services).

3.3. We do not process special category data related to your health, ethnicity, or religious or political beliefs unless required by law or in specific circumstances where, for example, you reveal such data while using the Platform.

3.4. If you provide us personal data about other people (such as your spouse or family) or you ask us to share their personal data with third parties, you confirm that you have brought this Privacy Policy to their attention beforehand.

4. HOW WE COLLECT YOUR PERSONAL DATA

4.1. We collect information you provide directly to us when you:

4.1.1. fill out any forms on our website, platform and/or mobile application;

4.1.2. open an account to use any other Services provided by the entities registered in the Platform;

4.1.3. contact us via our website or by using other means of communication (e.g., via our social network accounts);

4.2. We may also receive your personal data from third parties. In particular:

4.2.1. we may receive personal data from third parties such as public or private registers and databases. This includes information to help us check your identity, if applicable;

4.2.2. occasionally we will use publicly available information about you from publicly available sources (e.g., media, online registers and directories) and websites for security searches and other purposes related to sanction risk management;

4.2.3. we may receive personal data from a third party which is connected to you or is dealing with us, for example, business partners, sub–contractors, service providers, merchants and etc.;

4.2.4. we may receive personal data from other entities which we collaborate with.

5. OUR IDENTIFICATION TOOLS

5.1. In order to perform your identity verification, we use the services provided by our partner GB Group Plc., The Foundation Herons Way, Chester Business Park, Chester, United Kingdom, CH4 9GB (hereinafter – "GBG"). The Service Provider takes the photo images or video recordings of your face and your ID document that you provide through a mobile application or a dedicated website using the camera. For more information on GBG please read their Privacy Policy here **https://www.gbgplc.com/en/legal-and-regulatory/products-services-privacy-policy/**

5.2. GBG's solution is used for comparing live photographic data or video record of you and your ID document, to comply with legal obligations (e.g., implementation of the obligations under the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other fraud and crime prevention purposes) and risk management obligations.

5.3. The result of the face similarity (match or mismatch) will be retained for as long as it is necessary to carry out verification and for a period no longer than six (6) months.

5.4. We ensure that your face similarity check is a process of comparing data acquired at the time of verification, i.e., this is a one-time user authorization by comparing person's live photo to their image on the document. Your facial template is not created, recorded or stored. It is not possible to regenerate the raw data from retained information.

5.5. Using GBG's services, personal data is collected and transferred to us to further identification and verification of the person in the identity document and the person captured in the photo. This process shall allow us to verify your identity more precisely and make the process quicker and easier to execute. If you do not feel comfortable with this identification method, you may contact us by e-mail at **support@safe2transact.com** for an alternative way to identify you.

6. DIRECT MARKETING

6.1. In case you are an existing client (i.e., you already use our Platform), we may use your e-mail address for direct marketing purposes, but only with regard to our products and/or Services that are similar or related to the Services you have obtained, and only if you do not object to such use of your e-mail address. You are also granted with a clear, free of charge and easily enforceable possibility to object or withdraw from such use of your contact details.

6.2. In other cases, we may use your personal data for the purpose of direct marketing, only if you give us your prior explicit consent regarding such use of the data.

6.3. Upon receiving your consent, we will process your email address for direct marketing purposes for a period of two (2) years from the date of consent.

6.4. We provide a clear, free-of-charge and easily enforceable possibility not to give your consent or, at any time, to withdraw your consent to receive our marketing messages. We shall state in each notification sent by e-mail that you are entitled to object to the processing of the personal data, and to refuse receiving messages from us and give you the ability to opt out. You shall be

able to refuse receiving our marketing messages by clicking on the respective link in each marketing e-mail received from us.

7. AUTOMATED DECISION MAKING

7.1. We do not use automated decision making.

8. HOW WE SHARE YOUR PERSONAL DATA

8.1. We may disclose your personal information to the recipients of the following categories:

8.1.1. public authorities, institutions, organisations, courts and other third parties, but only upon request and only when required by applicable laws, or in cases and under procedures provided for by applicable laws;

8.1.2. third parties providing services to us including providers of legal, financial, auditing, tax, business management, personnel administration, remote identification, accounting, advertising (including online advertising), direct marketing, communications, data centres, hosting, cloud and/or other services. In each case, we provide such third parties with only as much data as necessary to provide their services. Service providers engaged by us may process your personal data only in accordance with our instructions and may not use them for other purposes;

8.1.3. our affiliate companies – i.e., companies belonging to the same group;

8.1.4. other persons with your consent;

8.1.5. UAB STANHOPE FINANCIAL, a private limited liability company incorporated under the laws of the Republic of Lithuania, with company registration number 305574870, having its registered office at Konstitucijos pr. 7, Vilnius, Lithuania, data on the company being registered and kept in the Register of Legal Entities (hereinafter – “Stanhope Financial”);

8.1.6. Personal data may be disclosed to Stanhope Financial where such disclosure is necessary for the performance of a contract concluded with you, through the Platform, execution of transactions, client due diligence procedures, compliance with anti-money laundering and counter-terrorist financing (AML/CTF) requirements, fraud prevention, risk management, compliance with applicable legal and regulatory obligations, or for the establishment, exercise or defence of legal claims.

8.1.7. Stanhope Financial acts as independent data controller where it determines the purpose and means of processing of personal data in connection with the services it provides to you. In such cases, your personal data shall be processed in accordance with its respective privacy policy and applicable data protection legislation and can be found here https://sh.financial/privacy-policy/. Personal data shall be shared only to the extent necessary for the specified purposes and subject to appropriate technical and organisational safeguards in accordance with the GDPR.

8.2. Role of the Company and Financial Service Providers

8.2.1. The Company acts as an independent data controller with respect to personal data processed for the purposes of operating and administering the Platform, enabling user registration and access, ensuring technical functionality and security of the Platform, preventing misuse, and fulfilling its own legal and regulatory obligations.

8.2.2. STANHOPE FINANCIAL acts as independent data controller with respect to personal data processed for the purposes of providing regulated financial services to you, including but not limited to client onboarding, due diligence, transaction execution, compliance with anti-money laundering and counter-terrorist financing requirements, risk management, and regulatory reporting.

8.2.3. The Company may collect and transfer personal data to such financial service providers where such transfer is necessary to enable the provision of their services to you or to ensure compliance with applicable legal and contractual obligations. Each financial service provider shall process personal data in accordance with its own privacy policy and applicable data protection legislation.

8.2.4. The Company does not determine the purposes and means of processing carried out by the financial service providers in relation to the financial services they provide and therefore does not act as a joint controller with respect to such processing unless explicitly stated otherwise.

9. INTERNATIONAL TRANSFER OF PERSONAL DATA

9.1. In case your personal data is transferred outside the European Economic Area (EEA), we will take necessary steps to ensure that your data is treated securely and in accordance with this Privacy Policy and we will ensure that it is protected and transferred in a manner consistent with the legal requirements applicable to the personal data. This can be done in a number of different ways, for example:

9.1.1 the country to which we send the personal data, a territory or one or more specified sectors within that third country, or the international organization is approved by the European Commission as having an adequate level of protection;

9.1.2 the recipient has signed or contains in its terms of service (service agreement) standard contractual clauses adopted by the European Commission;

9.1.3 special permission has been obtained from a supervisory authority.

9.2. We may transfer personal data to a third country by taking other measures if it ensures appropriate safeguards as indicated in the GDPR or on the basis of derogations. To find out about the exact additional security measure used, please write to us at support@safe2transact.com.

10. HOW WE PROTECT YOUR PERSONAL DATA

10.1. Please note that, although no system of technology is completely secure, we have to implement appropriate security measures in order to minimize the risks of unauthorized access to or improper use of your personal information.

10.2. We and our third-party service providers that may be engaged in the processing of personal data on our behalf (for the purposes indicated above) are contractually obligated to respect the confidentiality of the personal data.

10.3. A variety of logical and physical security measures are used to keep your personal data safe and prevent unauthorized access, usage, or disclosure of it (the list indicated below is not exhaustive): we use antivirus software, access control policies, we review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems, we use data encryption, etc.

11. HOW LONG DO WE KEEP YOUR PERSONAL DATA

11.1. We will keep your personal data for as long as it is needed for the purposes for which your data was collected and processed, including for the purposes to comply with any legal, regulatory, tax, accounting or reporting obligations. This means that we store your data for as long as it is necessary for provision of the Services and as required by the retention requirements in laws and regulations. If the legislation of the Republic of Lithuania does not provide any applicable

data retention period, it shall be determined by us, taking into account the legitimate purpose of the data retention, the legal basis and the principles of lawful processing of personal data.

11.2. The terms of data retention of the personal data for the purposes of the processing of the personal data as specified in this Privacy Policy are as follows:

11.2.1. when data is processed based on your consent, we will process your data for as long as your consent remains in force, if there are no other legal requirements which shall be fulfilled with regard to the personal data processing;

11.2.2. the personal data submitted by you through our website or via e-mail is kept for an extent necessary for the fulfilment of your request and to maintain further cooperation, but no longer than 6 months after the last day of the communication, if there are no legal requirements to keep them longer.

11.3. In the cases when the terms of data keeping are indicated in the legislative regulations, the legislative regulations are applied.

11.4. We may retain your personal data for a longer period when:

11.4.1. it is necessary in order for us to defend ourselves against existing or threatened claims, or to exercise our rights, or for the proper resolution of dispute, complaint or claim;

11.4.2. there is a reasonable suspicion of illegal activity;

11.4.3. it is required by applicable laws.

11.5. Upon expiration of the retention period, we will delete and/or reliably and irrevocably depersonalize your data as soon as possible, within a reasonable time required to perform such action.

12. YOUR RIGHTS

12.1. **The right to be informed**. You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data.

12.2. **The right to access**. You have the right to request from us the copies of your personal data. Where your requests are excessive, in particular if they are being sent with a repetitive character, we may refuse to act on the request, or charge a reasonable fee taking into account the administrative costs for providing the information. The assessment of the excessiveness of the request will be made by us.

12.3. **The right to rectification**. You have the right to request us to correct or update your personal data at any time, in particular if your personal data is incomplete or incorrect.

12.4. **The right to data portability**. The personal data provided by you is portable. You have the right to request that we transfer the data that we have collected to another organization, or directly to you, under certain conditions.

12.5. **The right to be forgotten**. When there is no good reason for us to process your personal data anymore, you can ask us to delete your data. We will take reasonable steps to respond to your request. If your personal data is no longer needed and we are not required by law to retain it, we will delete it or destroy it.

12.6. **The right to restrict processing**. You have the right to restrict the processing of your personal data in certain situations (e. g. you want us to investigate whether it is accurate; we no longer

need your personal data, but you want us to continue holding it for you in connection with a legal claim).

12.7. **The right to object processing.** Under certain circumstances you have the right to object to certain types of processing (e. g. receiving notification emails). However, if you object to us using personal data which we need in order to provide our Services, we may need to close your payment account as we will not be able to provide the Services.

12.8. **The right to file a complaint with a supervisory authority.** You have the right to file a complaint directly the State Data Protection Inspectorate of Lithuania if you believe that the personal data is processed in a way that violates your rights and legitimate interests stipulated by applicable legislation. You may apply in accordance with the procedures for handling complaints that are established by the State Data Protection Inspectorate and which may be found by this link: https://vdai.lrv.lt/lt/veiklos-sritys-1/skundu-nagrinejimas.

12.9. **Rights related to automated decision-making (currently not applicable).** You have the right not to be subject to a decision which is based solely on automated processing and which produces legal or other significant effects. In particular, you have the right:

- to obtain human intervention;
- to express point of view;
- to obtain an explanation of the decision reached after an assessment; and
- to challenge such a decision.

12.10. **Right to withdraw your permission.** If you have given us consent for processing of your data, you can withdraw your consent at any time. It will have been lawful for us to use the personal data up to the point you withdrew your permission. You also have a right to withhold your consent without any adverse effect.

12.11. If you would like to exercise any of these rights, please contact us via e-mail: **support@safe2transact.com**. For security reasons, we will not be able to process your request if we are not sure of your identity, so we may ask for your ID as proof.

12.12. Your requests will be fulfilled, or fulfilment of your requests will be refused by specifying the reasons for such refusal, within 30 (thirty) calendar days from the date of submission of the request that complies with our internal rules and the GDPR. The afore-mentioned time frame may be extended by 60 (sixty) calendar days taking into account the complexity and number of the requests. The Company will inform you of any such extension within 30 (thirty) calendar days of receipt of the request, together with the reasons for the delay.

12.13. We may refuse to satisfy you request if the exception and/or limitation to the exercise of data subjects' right set out in the GDPR apply, and/or if your request is found to be manifestly unfounded or disproportionate. If we refuse to satisfy your request, we will give you our reason for such refusal in writing.

13. COOKIES POLICY

13.1. If you access our information or Services through our website, you should be aware that we use cookies.

13.2. For more information on how to control your cookie settings and browser settings or how to delete cookies from your device, please read the Cookie Policy available on our website here https://safe2transact.com

14. LINKS TO OTHER WEBSITES

14.1. Our website may contain links to other websites which are not operated by us. When you decide to click on these links and be led to such websites, we recommend familiarising yourself with their privacy policies or notices, cookie policies and/or other documents. We assume no responsibility for the content, policies or practices of such third-party websites or services.

15. CHANGES TO THIS PRIVACY POLICY

15.1. We regularly review this Privacy Policy and reserve the right to modify it at any time in accordance with applicable laws and regulations. We will inform you of any material changes in advance.

CONTACT US

You may contact us by e-mail to **support@safe2transact.com**.