APPROVED
by the decision of the Management Board of
SIA "Spirit Capital Investments"
of 20 December 2023
Decision No. 12-2024

SIA "Spirit Capital Investments"
PRIVACY POLICY

1. Purpose

1.1. The purpose of this Privacy Policy is to provide a natural person – the data subject – with information regarding the processing of personal data by the investment brokerage company (hereinafter – "IBS") SIA "Spirit Capital Investments," including the purposes of data processing, the legal basis, types (categories) of personal data, their retention period, the rights of the data subject, and personal data protection measures.

2. Data Controller

2.1. The data controller is SIA "Spirit Capital Investments," registration No. 40203160700, legal address: Avotu iela 34A, Rīga, LV-1009 (hereinafter – "the Company"), phone: +371 67885886, email: office@spiritcapital.eu.

2.2. The Company's email address for inquiries related to personal data processing: office@spiritcapital.eu.

3. General provisions

3.1. This Privacy Policy provides a general overview of how the Company processes and protects personal data.

3.2. When processing personal data, the Company complies with the Investment Brokerage Company Law, 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 (hereinafter – "General Data Protection Regulation"), the Personal Data Processing Law, and other applicable legal acts.

3.3. Within the framework of applicable legal acts, the Company ensures the confidentiality of personal data and implements appropriate technical and organizational measures to protect personal data against unlawful processing, including unauthorized access, disclosure, accidental loss, alteration, or destruction.

3.4. The Company may engage personal data processors for the processing of personal data. In such cases, the Company takes the necessary steps to ensure that such processors process personal data in accordance with the Company's instructions, the terms of the concluded agreements, and the applicable legal requirements, and require the implementation of appropriate security measures.

4. Categories of personal data, purpose of processing, and legal basis

4.1. The categories of personal data that the Company mainly, but not exclusively, processes include:

4.1.1. Data on potential/existing clients for service provision – to ensure proper service delivery and compliance with regulatory requirements, including assessing the suitability and appropriateness of a service for a client, providing customized services, determining client status, and managing risks*:*

a) Information specified in the client consultation form: identifying information of clients (investors) (first name, surname, represented company, address, contact details, nationality, date and place of birth, profession, tax identification number, relevant tax authority, etc.); identifying information of employees/agents (first name, surname, represented company, address, contact details, etc.); potential conflicts of interest; information about applicable fees; reason for the consultation; client's experience and knowledge in capital investments; financial status; main assets; family and professional status, including education; risk tolerance; investment goals; sustainability preferences; suitability statement/report, including the assigned client status and their attitude towards it; consultation proposal, etc.;

b) Data about potential/existing clients required for service contract conclusion and execution: client's identifying data (including name, surname, personal identification number, contact details), representative's identifying data (including name, surname, personal identification number, address, contact details, represented company, position/representation basis), service agreement, service fees, payment information, etc.

4.1.2. Data on potential/existing clients for the purposes of anti-money laundering, counter-terrorism and proliferation financing, and sanctions compliance – to fulfill the Company's obligations and exercise its official authority under applicable laws:

a) Information in client questionnaires – client details (for natural persons: name, surname, nationality, country of tax residence, address, personal ID number, date of birth, contact info; for legal entities: name, registration number, tax residence country, legal address, place of business activity, representative's name, surname, position or power of attorney basis, ID number, date of birth, contact info), beneficial owner (hereinafter "UBO") (name, surname, personal ID/date of birth, citizenship, country of permanent residence, ownership in share capital), politically exposed person (hereinafter "PEP") status (yes/no, name, surname, institution, position, country, relationship with client), client's activities, purpose and nature of the business relationship (planned services and scope), source of funds intended for investment, intended use of funds (e.g. financial instruments), client's bank/payment institution/broker, declarations, date, etc.;

b) Information obtained/prepared during client/issuer due diligence: details about the investigation (responsible person, date, type, rationale), service type (including planned investment/transaction amount), client type, identifying data (natural person: name, surname, nationality, country of tax residence, address, ID number, date of birth, passport number; legal person: name, registration number, registration country, legal and actual address, other registration details, representative's name, surname, representation basis, ID number, date of birth, passport number), identification info (type, performer, date), client's UBO (in case of enhanced due diligence – analysis/conclusions on data accuracy and reliability), PEP status (including conclusion if UBO is a PEP or related), client's personal/business activities, relationship with other

clients (including conclusion if any are high-risk), source of funds (including reliability conclusion), geographical/sanctions risks, additional risk factors, conclusions (including risk score result, risk level, recommendation to start/continue cooperation), etc.;

c) Risk assessment (scoring): risks related to the client's legal structure and UBO, transaction amount, PEP status, geographic risks, business/personal activity of the client and UBO, due diligence process, risk factors regarding existing clients, assessment result, etc.;

d) Internal reporting of potentially suspicious transactions or sanctions violations: information about the Company's employee who prepared the report (name, surname), client (ID, name, surname, ID number, date of birth), description of suspicious transaction/sanctions violation, risk specialist's analysis (name, surname, date, arguments and conclusions), management board member's decision (name, surname, decision, date), etc.

4.1.3. Data on engaged agents and related persons (agent assistants, responsible persons, agent managers) and candidates: identifying information of agents and related persons (name, surname, ID number, address, contact info, name of represented agent company, registration number, legal address, if agent is a legal entity), the EU/EEA country where the agent operates, information on compliance with qualification requirements and evaluation thereof (e.g. interviews, references, CV, education documents, training/exam results, certificates, work/professional experience, financial competence, reputation, legal violations, criminal records, evaluation conclusions, assessed level/status), cooperation agreement, compensation, payment details, bank account, registration as self-employed (if agent is a natural person), circumstances that may cause a conflict of interest (e.g. current job or occupations), photo, etc. – to ensure service provision and compliance with legal requirements.

4.1.4. HR data: about job applicants (education, qualifications, position, employer, contact info, CV) and Company employees (name, surname, position, ID number, CV, passport details, residential and declared address, contact info, employment contract, bank details, employee's account, education, training, language skills, vacations, certificates, documents, employment history, termination, work information, health data (e.g. temporary incapacity, mandatory health checks), photo, etc.) – to ensure human resource management, including staff selection, in line with legal requirements.

4.1.5. Accounting data: about employees (name, surname, position, date of birth, ID number, passport details, address, contact info, employment contract, employment history, bank account number, salary, changes in remuneration, bonuses, incentives, health insurance, vacation and vacation pay, data on temporary incapacity, mandatory medical checks, paid tax amounts, benefits, training, names of children, surnames, ID numbers, residential address), and about clients, service providers, suppliers, cooperation partners/their representatives (name, surname, position, contact info, contracts, payments, bank account), etc. – to ensure bookkeeping in accordance with legal requirements.

4.1.6. Administrative records data: name, surname, ID number, residential and declared address, position, contact info (phone number, email), correspondence, meeting minutes and decisions, contracts, visual and audio

recordings on online platforms used for meetings – to ensure administrative recordkeeping as required by law.

4.1.7. Data related to Company activity publicity, promotion, and service distribution: name, surname, position, occupation, contact info (phone, email), and image captured in photos or videos of Company event participants/attendees, employees, media representatives – to inform the public about the Company's activities and promote its services.

4.1.8. Other data voluntarily provided by the individual to the Company, or data the processing of which is necessary for the fulfillment of legal obligations, tasks in the public interest or the exercise of official authority legally granted to the Company, or for the conclusion and execution of contracts, or for the legitimate interests of the Company or third parties, or based on the individual's consent.

4.2. Personal data is primarily processed for the following purposes:

4.2.1. To ensure the provision of the Company's services, including the performance of duties and tasks assigned to the Company as a licensed IBS under applicable legal acts, such as client and representative identification, due diligence, risk management, establishment of business relationships, fulfillment of contractual obligations, payment administration, handling of objections or complaints, assessment of customer satisfaction, and improvement of service quality.

4.2.2. For human resource management – including personnel recruitment and preparation and administration of documentation related to employee work.

4.2.3. To ensure accounting and bookkeeping.

4.2.4. To ensure proper record-keeping.

4.2.5. To inform the public about the Company's activities and for marketing/distribution purposes.

4.2.6. To respect and protect the legitimate interests of the Company and third parties when necessary.

4.2.7. To ensure compliance with applicable legal requirements.

4.3. Legal Basis for Personal Data Processing:

4.3.1. Article 6(1)(a) of the General Data Protection Regulation (data subject's consent) – e.g., for marketing purposes (to offer/promote the Company's services to the client).

4.3.2. Article 6(1)(b) GDPR (contract conclusion and performance) – e.g., to conclude and execute contracts with clients, employees, agents, other partners, and service providers.

4.3.3. Article 6(1)(c) GDPR (compliance with legal obligation) – to comply with legal obligations (e.g., obligations under the Investment Brokerage Company Law, including submitting required information to the Bank of Latvia; obligations under the Accounting Law; requirements related to employment under the Labor Law; and obligations under the Anti-Money Laundering and Counter-Terrorism and Proliferation Financing Law, including customer identification, due diligence, and risk assessment.

4.3.4. Article 6(1)(e) GDPR – for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company, such as preventing money laundering and terrorism/proliferation financing.

4.3.5. Article 6(1)(f) GDPR (legitimate interests) – the Company's legitimate interests include, for example, identity verification and due diligence, validating and

updating client-provided information, assessing prospective clients, managing business risks, improving service quality, public awareness of Company activities, marketing services, ensuring infrastructure and personnel security, and protecting legal interests, including interactions with public authorities or legal proceedings.

5. Special categories of personal data

5.1. Article 9(1) of the GDPR prohibits processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data (for unique identification), health data, or data concerning a person's sex life or sexual orientation.

5.2. Article 9(2) of the GDPR provides exceptions to the above prohibition, including where processing is necessary for the controller to comply with legal obligations. The Company processes special categories of personal data in a limited scope – for example, health data related to employees as required by law (e.g., information about temporary incapacity or mandatory medical examinations). Legal basis: Article 9(2)(b) and Article 6(1)(c) GDPR.

6. Personal data on criminal convictions and offenses

6.1. The Company processes data on criminal records and offenses in a limited scope – to comply with legal obligations concerning IBS officers, employees, agents, and AML/CTF/sanctions compliance, as well as for the protection of its or a third party's legitimate interests (e.g., verifying the reputation and reliability of data subjects to assess their suitability as clients, officers, employees, or agents and for possible termination of business relationships or employment, or for legal documentation purposes). Legal basis: Article 10 and either Article 6(1)(c) or 6(1)(f) GDPR.

7. Automated data processing

7.1. The Company may use profiling (this form of automated processing is one of several) – for example, to assess a data subject as a potential client, determine the suitability and appropriateness of services or financial instruments, provide personalized services, apply target market requirements, and determine a client's risk classification under AML/CTF and proliferation financing regulatory compliance.

8. Personal datu protection

8.1. The Company protects personal data by utilizing modern technological solutions, considering existing privacy risks and reasonably available organizational, financial, and technical resources, including the following security measures and solutions:

8.1.1. Data encryption during transmission (SSL encryption);

8.1.2. Firewall;

8.1.3. Intrusion detection and prevention systems;

8.1.4. Other protection measures in line with current technological developments.

9. Sources and recipients of personal data

9.1. Sources of data: The Company obtains personal data from data subjects themselves, as well as from external sources for verification and updating, such as competent authorities and their national registers and information systems, public and third-party registers, databases, search engines, media, etc.

9.2. Data recipients: Data may be transferred/made available to competent state and municipal institutions in accordance with legal provisions (e.g., the Bank of Latvia, the State Revenue Service, the Financial Intelligence Unit, law enforcement agencies, etc.), the Company's engaged agents and related persons, financial intermediaries, other service providers/data processors (e.g., IT service providers), consultants, auditors, and other authorized persons hired by the Company to provide services and/or perform specific tasks.

9.3. Data is not transferred to third countries. However, information published on the Company's website (https://spiritcapital.eu) and on the Company's Facebook, X, Instagram, YouTube, and LinkedIn pages may be accessible from abroad, including third countries outside the EU and EEA.

10. Personal data retention period

10.1. Personal data is processed for as long as necessary for the relevant purpose of data processing and in accordance with applicable legal requirements.

10.2. The retention period of personal data, or – if not determinable – the criteria used to define it, are as follows:

10.2.1. Personal data is stored for as long as necessary to achieve the purpose of processing, according to applicable legislation.

10.2.2. Personal data obtained during recruitment will be retained fully or partially for no longer than 6 months after receipt of the application, unless complaints regarding the recruitment process are received – in such cases, the data will be stored as long as necessary to resolve the specific dispute.

10.2.3. The following criteria are used to determine the data retention period – data is stored:

a) as long as there is a legal obligation to retain data (e.g., under the Accounting Law);

b) as long as the data is necessary to fulfill the Company's statutory obligations, tasks, or authority;

c) as long as the data is necessary to fulfill contractual obligations;

d) as long as the data is needed to enforce legitimate interests of the person or the Company (e.g., for audit, legal defense, dispute resolution – for instance, under the Civil Law general limitation period of 10 years – or until the legal interest is fully resolved);

e) as long as the data subject's consent remains valid, if there is no other legal basis for processing.

10.3. Once the retention period expires, personal data is deleted or destroyed, or transferred to the State Archives in accordance with applicable laws.

11. Cookies on the website

11.1. Information about the use of cookies is provided in the Company's Cookie Policy, available on the Company's website (https://spiritcapital.eu), under the "Cookie Policy" section".

12. Rights of the data subject

12.1. The data subject has the following rights regarding the protection of personal data:

12.1.1. Right to receive information about the processing of their data – the data subject may request information from the Company about how their personal data is processed.

12.1.2. Right of access to data – when exercising this right, the data subject must specify the time period and data they wish to obtain. The data subject may request details on which personal data is held, the purpose of processing, source and recipients of the data, retention period, and receive a copy of their personal data.

12.1.3. Right to rectification – if the data subject wishes to correct or update their personal data held by the Company, they must clearly indicate which data should be corrected and provide the accurate information. If the data was not obtained from the Company, a justification should be provided explaining why the correction is necessary to support a quicker and more appropriate assessment.

12.1.4. Right to erasure – to request deletion, the data subject must specify which personal data should be deleted and provide justification. Please note that deletion may not always be possible.

12.1.5. Right to restrict processing – if the data subject is unsure whether the Company is processing data lawfully, they may request restriction of certain data processing. The request must include the reason why the data subject believes restriction is necessary.

12.1.6. Right to object to processing – in specific cases, the data subject may object to processing due to individual circumstances. Such a request should include a description of the individual circumstances on which the objection is based.

12.1.7. Right to data portability – the data subject may request that the Company compile and transfer their data to another controller or provide it directly to them. The specific data to be transferred must be identified.

12.1.8. Right to withdraw consent – the data subject may withdraw their consent at any time, provided the processing is not based on another legal ground (e.g., statutory obligations binding on the Company). Withdrawal of consent does not affect the lawfulness of processing carried out before the withdrawal.

12.1.9. Right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects concerning them (or similarly significantly affects them).

12.2. Submitting and processing of data subject requests:

12.2.1. The data subject must submit their request in writing. The Company accepts documents in person, by post, or by email (with a secure electronic signature):

SIA “Spirit Capital Investments”,
Avotu iela 34A, Rīga, LV-1009,
office@spiritcapital.eu,
https://spiritcapital.eu,
+371 67885886.

12.2.2. The Company will assess the request without undue delay and will respond no later than 1 month from the date of receipt. If more time is needed, the Company

may extend the deadline by 2 additional months, and the data subject will be informed of the extension within 1 month.

12.2.3. The Company may refuse to fulfill the request if:

a) it is not clearly formulated;
b) the data subject cannot be identified;
c) a response to the same request has already been provided;
d) the scope of the request is excessive/disproportionate;
e) the request is manifestly unfounded (e.g., not relevant to the Company or no justification provided);
f) the law prohibits disclosure of such information or obliges the Company to retain specific data (e.g., when the request includes data deletion).

12.3. The data subject has the right to submit a complaint to the Data State Inspectorate if they believe that the processing of their personal data violates their rights and interests under applicable laws:

Data State Inspectorate,

Elijas iela 17, Rīga, LV-1050,

pasts@dvi.gov.lv,

www.dvi.gov.lv,

+371 67223131.

13. Final provisions

13.1. This Privacy Policy contains information required under Articles 12, 13, 14, and 15 of the General Data Protection Regulation.

13.2. The Company has the right to amend or supplement this Privacy Policy by publishing the latest version in the "Privacy Policy" section of its website.