Privacy Policy

BLS Capital Fondsmæglerselskab A/S

December 2020

1. INTRODUCTION

1.1 The Board of Directors has adopted this Personal Data Protection Policy ("the Policy"), which sets forth the basic principles by which BLS Capital Fondsmæglerselskab A/S ("the Company") processes personal data of clients, co-investors, business partners, suppliers and employees. The Policy specifies the responsibilities of its business departments and employees while processing personal data.

1.2 The Policy applies to the Company's management (including the Board of Directors), employees and its data processors.

2. PURPOSE

2.1 When operating, the Company needs to gather and use certain information about individuals. These may include clients, co-investors (and their beneficial owners) of Kapitalforeningen BLS Invest ("BLS Invest"), business partners, suppliers, employees, and other persons the Company has a relationship with or may need to contact.

2.2 The Policy describes how Personal Data, cf. Section 4.1.1, must be collected, handled, and stored to meet the Company's data protection standards and to comply with European and Danish legislation, cf. Section 3.

3. LEGAL BASIS

3.1 When processing Personal Data, the Company must comply with The General Data Protection Regulation ("GDPR") and the Danish Data Protection Act.

4. DEFINITIONS

4.1 In this Policy the following words shall, unless the context otherwise requires, have the following meanings, and may be used in the singular or plural as appropriate:

4.2 "*Personal Data*": means any information relating to an identified or identifiable natural person ("Data Subject").

4.3 "*Identifiable Natural Person*": is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.4 "*Sensitive Personal Data*": means Personal Data, cf. Section 4.1.1, which are, by its nature, particularly sensitive in relation to union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4.5 "*Processing*": means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, cf. Section 4.1.1, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

4.6 "*Controller*": means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, cf. Section 4.1.1, where the purposes and means of such processing are determined by European or Danish legislation, the Controller or the specific criteria for its nomination may be provided for by European or Danish legislation.

4.7 "*Processor*": means a natural or legal person, public authority, agency, or other body which processes Personal Data, cf. Section 4.1.1, on behalf of the controller.

5. THE COMPANY AS CONTROLLER

5.1 In general, the Company processes Personal Data for its own purposes. Thus, the Company is a Controller, cf. Section 4.1.5, and decides the purposes and means of processing Personal Data. This responsibility extends to the activities of contractors, sub-contractors, vendors and other to whom the Company delegates some or all the processing activities which take place under its control (Processors, cf. Section 4.1.6).

5.2 The management of the Company's Processors are described in its internal business procedures e.g., a policy and business procedure for outsourcing activities.

5.3 The Company will on an annual basis make sure, that the Company's Processors provide sufficient guarantees to implement appropriate technical and organisational measures in a manner, by which processing will meet the requirements with Data Protection Law and the rights of any data subject.

6. BASIC PRINCIPLES

6.1 As its main principle related to personal data protection, the Company is accountable for its activities involving processing of Personal Data and holds a responsibility to safeguard the rights, freedoms, and safety of persons whose Personal Data are processed by the Company.

6.2 The Company only processes Personal Data when it has a legitimate ground. Any processing of Personal Data must be based on one of the following conditions:

- *Consent*: the Data Subject has given an unambiguous indication of its agreement for the Company to process their Personal Data. For a consent to be valid, it must be given on a basis of information sufficient to enable the Data Subject to understand clearly the purpose, nature, extent and effects of the processing., Furthermore, a consent to the Company is always given freely, which means the Data Subject are not exposed to negative consequences because of the refusal to give consent.
- *Contract*: the processing of Personal Data is necessary for the performance of a contract with the Data Subject or necessary to conclude a contract at the request of the Data Subject.
- *Legitimate interest*: the processing of Personal Data is necessary for purposes, which are in the Company's legitimate interest. However, processing of Personal Data in this situation can only take place where the interests or rights of the Data Subject do not override the Company's interest in the processing.
- *Legal obligation*: the processing of Personal Data is necessary for compliance with a legal obligation of the Company, such as communication information about its' employees' salaries to local tax authorities.

- *Vital interests (of the Data Subject)*: the processing of Personal Data is necessary to protect the Data Subject's life or physical safety or health.

6.3 The Company only process personal data in a way that can be reasonably expected by Data Subjects and in consideration of the Data Subjects' rights, freedoms, and safety.

6.4 The Company stands open about its activities involving the processing of Personal Data and document these processing thoroughly and in accordance with legal requirements. The Company seeks to communicate in a clear, concise, and transparent way with Data Subjects and relevant authorities regarding the Company's processing of Personal Data.

6.5 The Company solely obtains Personal Data for specific, explicit, and legitimate purposes. Personal Data can only be used for a specific processing purpose that the Data Subject has been made aware of.

6.6 The Company seeks to only use as much Personal Data as is required to successfully accomplish a legitimate task. This also means that Personal Data collected by the Company for one purpose cannot be repurposed without further consent.

6.7 The Company only process Personal Data that is accurate and kept up to date.

6.8 The Company will not store Personal Data longer than necessary for the purposes for which the Personal Data are processed. Personal Data that are no longer required will be removed.

6.9 The Company process Personal Data in a manner that ensures appropriate security of the Personal Data, including protection again unlawful processing or accidental loss, destruction, or damage.

7. RECORD OF PROCESSING ACTIVITIES

7.1 The Company maintains a record of its processing activities ("the Register").

7.2 The Period of retention and disposal of Personal Data in the Company are regulated in the Register, cf. Section 7.1.

8. DATA STORAGE

8.1 The only persons able to access data covered by the Policy are those who need it for their work.

8.2 When the Company store Personal Data electronically it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:

- Personal Data must be protected by strong passwords that are changed regularly and not shared between employees.
- Personal Data stored on removable media (e.g., a memory stick) must be kept locked away securely when not being used.
- Personal Data must be stored on the Company's designated internal drives and servers and should only be uploaded to approved cloud computing services.
- Personal Data must be backed up frequently. Those backups must be tested regularly in line with the Company's standard backup procedures.
- Personal Data shall never be saved directly to laptops or other mobile devices like tablets or smart phones.

8.3 When the Company store Personal Data on paper it must be kept in a secure place protected from unauthorized persons:

- Documents and printouts containing Personal Data must be kept in a locked drawer or filing cabinet.
- Documents and printouts containing Personal Data must be shredded and disposed of securely when no longer required.

9. PROCESSING GUIDELINES AND SECURITY MEASURES

9.1 The Company can only process Personal Data where a reason for doing so exists. Such reason exists if the:

- Processing of Personal Data is based on a consent;
- Processing of Personal Data is in the legitimate interests of the Company;
- Processing of Personal Data is required by law i.e., a legal obligation (e.g., anti-money laundering or tax regulation).
- Processing of Personal Data is required to fulfil contractual obligations.

9.2 The Company adopts technical and organisational measure with the aim of ensuring the appropriate security of Personal Data with respect to its processing activities, considering the specific risks to the Data Subjects' rights, freedoms and safety, technological possibilities, and cost-effectiveness.

9.3 The Company's security measures aim to sustain in a verifiable way the following objectives across systems and throughout the Personal Data lifecycle:

- *Confidentiality*: Personal Data is only accessible and disclosed to those who need it.
- *Integrity*: the Accuracy and completeness of Personal Data is preserved.
- *Availability*: Personal data can be accessed and used at all time by those authorized to do so.
- *Resilience*: the systems used for the processing of Personal Data are effective in protecting the Personal Data against actual threats, are regularly tested and recovery procedures minimising the impact of incidents on the systems are in place.

10. DATA ACCURACY

10.1 The Company takes all reasonable steps to ensure Personal Data is kept accurate and up to date in accordance with GDPR and other applicable legislation.

10.2 It is the responsibility of employees who process Personal Data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

10.3 Personal Data must be held in as few places as necessary. Employees shall not create any unnecessary additional data sets.

10.4 Employees shall take every opportunity to ensure data is updated e.g., by confirming a client's contact details when interacting.

10.5 Personal Data shall be updated as inaccuracies are discovered e.g., by removing a client's contact details if the client can no longer be reached using these.

10.6 If inaccurate Personal Data is detected the individual in questions has the right to obtain from the Company without undue delay the rectification of the inaccurate Personal Data.

11. SUBJECT ACCESS REQUEST

11.1 Data Subjects have a right to access Personal Data that is processed about them by the Company and obtain a copy of this Personal Data. In addition, when the Data Subject can provide necessary evidence to that effect, the Data Subject has a right to request the rectification of incorrect or incomplete data, cf. Section 10, or to request the deletion of data, cf. Section 12.

11.2 All individuals who are subject of Personal Data held by the Company are entitled to ask what information the Company holds about them and the reason for the processing.

11.3 A subject access request can be made free of charge by email to the Company at info@blscapital.dk.

11.4 The Company will aim to provide a subject access request, cf. Section 11.3, within 14 business days.

11.5 The Company will always verify the identity of anyone making a subject access request before handing over any information.

12. THE RIGHT TO DATAPORTABILITY

12.1 A Data Subject of the Company has a right to obtain and reuse Personal Data concerning that individual if the information has been provided by the Data Subject to the Company.

13. THE RIGHT TO BE FORGOTTEN

13.1 A Data Subject of the Company has a right to request and demand erasure of Personal Data concerning that individual.

14. DISCLOSURE TO THIRD PARTIES

14.1 When processing Personal Data, the Company is the data controller.

14.2 Whenever the Company uses a third-party supplier or business partner to process Personal Data on behalf of the Company, it must contractually require the supplier or business partner to provide an equivalent level of data protection. The supplier or business partner must only process Personal Data to carry out its services if this is done in compliance with Section 8 of the Policy.

14.3 The disclosure of Personal Data to a third-party must be based on either a consent from the Data Subject or other of the criteria listed in Section 9.1.

15. PERSONAL DATA BREACH

15.1 The Company endeavours to protect Personal Data on the best of its abilities. Despite best efforts, the Company's technical or organizational security could be breached by accident or intentional actions and as a result the confidentiality, integrity or availability of Personal Data may be compromised.

15.2 In case of a Personal Data Breach, the Company must without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the Danish Data Protection Agency about the Personal Data Breach, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of the individuals in question. Where the notification to the Danish Data Protection agency is not made within 72 hours, it shall be accompanied by reasons for the delay.

15.3 If the Personal Data Breach is likely to results in a high risk to the rights and freedoms of the individuals in question, the Company must communicate the Personal Data Breach to the individual without undue delay.

16. KEY ROLES AND RESPONSIBILITIES

16.1 *The Board of Directors*

16.1.1 The Board of Directors are responsible for ensuring that the Company meets its legal obligations under GDPR, including the definition of roles and allocation of responsibilities.

16.2 *The compliance function*

16.2.1 The compliance function is responsible for training existing and new staff within the Company on the obligations according to this Policy and the relevant legislation. The training will take place annually or when onboarding of new staff.

16.2.2 The purpose of the training is to make sure that every staff member is aware of the requirements of Data Protection Law and their individual responsibilities for ensuring compliance within The Company.

16.2.3 The compliance function is responsible for monitoring and keeping log of staff training.

16.3 *Employees*

16.3.1 Employees are responsible for ensuring that Personal Data is collected, stored, handled, and destroyed in line with the Policy and the principles it contains, as well as rules and procedures developed in the Company based on this Policy.

17. INTERNAL CONTROL

17.1 The compliance function continuously monitors and control that Personal Data processed by the Company is done in accordance with this Policy.

17.2 The compliance function shall at least once a year prepare a written report to the Company's Board of Directors and the CEO on the performed activities under this Policy, including an update of the Register, cf. Section 7.1.

18. REVIEW AND UPDATES

18.1 The Policy must be reviewed by the Board of Directors when deemed necessary and at least on an annual basis.

Adopted by the Board of Directors, December 2020