Personal Data Protection Policy

BLS Capital Fondsmæglerselskab A/S

October 2023

1. INTRODUCTION 3

2. LEGAL BASIS 3

3. DEFINITIONS 3

4. THE COMPANY AS CONTROLLER 4

5. PROCESSING PRINCIPLES 4

6. RECORD OF PROCESSING ACTIVITIES 4

7. DATA STORAGE AND SECURITY MEASURES 4

8. PROCESSING GUIDELINES 5

9. RIGHTS OF DATA SUBJECTS 6

10. DISCLOSURE TO THIRD PARTIES 6

11. PERSONAL DATA BREACH 6

12. KEY ROLES AND RESPONSIBILITIES 7

13. INTERNAL CONTROL 7

14. REVIEW AND UPDATES 7

15. TRACK RECORD 7

1. INTRODUCTION

1.1 The Board of Directors has adopted this Personal Data Protection Policy (the "Policy"), which sets out the principles by which BLS Capital Fondsmæglerselskab A/S (the "Company") processes Personal Data.

1.2 The Policy applies to the Company, its data processors, and to all practices concerning Personal Data to ensure secure and appropriate processing in adherence with applicable legislation.

1.3 The Company's operations depend on data and information. This includes the collection and use of Personal Data of clients, co-investors, business partners, suppliers, employees, and other persons the Company has a relationship with or may need to contact.

2. LEGAL BASIS

2.1 The Policy is prepared in accordance with Regulation (EU) 2016/679 ("GDPR") and the Danish Data Protection Act (Act no. 502 of 23 May 2018).

3. DEFINITIONS

3.1 The following definitions apply to this Policy:

- **Personal Data**: Any information relating to an identified or identifiable natural person ("Data Subject").
- **Data Subject**: Any identified or identifiable individual/natural person who is the subject of Personal Data held and processed by the Company.
- **Sensitive Personal Data**: Personal Data, 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.
- **Processing**: Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, 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.
- **Controller**: A natural or legal person, public authority, agency, or other body which, alone or in concert with others, determines the purposes and means of the processing of Personal Data; 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.

- **Processor**: A natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the controller.

4. THE COMPANY AS CONTROLLER

4.1 In general, the Company processes Personal Data for its own purposes. In these cases, the Company acts as a Controller and decides the purposes and means of processing Personal Data. This responsibility extends to the activities of Processors to whom the Company delegates some or all the Processing which take place under its control.

4.2 When Personal Data is Processed by a Processor on behalf of the Company, a Data Processing Agreement is entered and the Processor is required to provide sufficient guarantees to implement appropriate technical and organizational measures to protect the rights of Data Subjects and meet legal requirements. The Company performs risk-based testing of the Processors' compliance with agreements and legal requirements.

5. PROCESSING PRINCIPLES

5.1 The Company supports and complies with the data protection principles and Personal Data must be:

- lawfully, fairly, and transparently processed,
- collected only for clear and lawful purposes,
- limited to what is necessary to achieve the purpose,
- accurate and up to date,
- deleted once the purpose of storage seizes to exist, and
- its integrity and confidentiality must be protected.

6. RECORD OF PROCESSING ACTIVITIES

6.1 The Company maintains a record of its processing activities and retention periods for Personal Data.

7. DATA STORAGE AND SECURITY MEASURES

7.1 Access to Personal Data is restricted to those who need it for legitimate purposes.

7.2 The Company's electronic storage of Personal Data must be protected from unauthorized access, accidental deletion, and malicious hacking attempts, and take place in accordance with the Company IT security policies and procedures, which amongst others entails that the Company must ensure that:

- Personal Data is 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, servers and approved cloud computing services.
- Personal Data must be backed up frequently and backups must be tested regularly.
- The Company's physical storage of Personal Data must be kept secure and protected from unauthorized persons, and:
- Documents containing Personal Data must be kept in a locked drawer or filing cabinet.
- Documents containing Personal Data must be shredded and disposed of securely when no longer required.

7.3 The Company adopts technical and organizational measures with the aim of ensuring 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.

8. PROCESSING GUIDELINES

8.1 The Company solely processes Personal Data where one or more of the below legitimate reasons exist:

- Processing of Personal Data is based on 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.
- Processing of Personal Data is required to protect vital interests of the Data Subject.

9. RIGHTS OF DATA SUBJECTS

9.1 Data Subjects have the right to be informed of the Company's Processing of Personal Data and certain additional information.

9.2 Data Subjects have a right to obtain a copy of Personal Data that the Company is Processing and information on the purpose of the Processing.

9.3 Data Subjects have a right to request rectification of incorrect or incomplete data, or to request the deletion of Personal Data under certain circumstances.

9.4 Requests can be made via email to the Company at info@blscapital.dk. The Company seeks to answer requests within 14 business days and ensures verification of the identity of the Data Subject prior to delivery of Personal Data.

10. DISCLOSURE TO THIRD PARTIES

10.1 The Company keeps Personal Data confidential and do not disclose Personal Data to third-parties unless this is based on consent from the Data Subject or another legitimate criteria as set out in Section 8.

11. PERSONAL DATA BREACH

11.1 The Company protects Personal Data diligently. 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.

11.2 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 Data Subjects 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.

11.3 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.

12. KEY ROLES AND RESPONSIBILITIES

The Board of Directors

12.1 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.

The compliance function

12.2 The compliance function is responsible for training of existing and new staff within the Company on the obligations set forth in this Policy and applicable legislation. Training must be conducted annually and in connection with onboarding of new staff.

12.3 The compliance function is responsible for monitoring and keeping a record of training activities.

Employees

12.4 Employees are responsible for ensuring that Personal Data is collected, stored, handled, and destroyed in line with the Policy and additional procedures based on this Policy.

13. INTERNAL CONTROL

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

13.2 The compliance function must annually report to the Company's Board of Directors and the CEO on the performed activities under this Policy, including an update of the register of processing activities.

14. REVIEW AND UPDATES

14.1 The Policy must be reviewed by the Board of Directors when deemed necessary and at least annually.

15. TRACK RECORD

Updated by: EN	**Approved by:** Board of Directors	**Version**: 5.0
Date: 29/09/2023	**Dato:** 26/10/2023	