Data Protection Policy

1 Introduction

1.1 This Data Protection Policy is applicable to each entity (hereinafter the "**Company**") to which Standard Bank Offshore Trust Company Jersey Limited, Lumbro Corporate Services Limited and Cotillion Trust Company Limited render services (each, an "**Administrator**"), all of which are carrying on trust company business under the Financial Services (Jersey) Law 1998 (as amended), respectively as Affiliation Leader and Participating Members.

1.2 The Company has adopted this data protection policy (the "**Policy**") to ensure it meets its obligations under the Data Protection (Jersey) Law 2018 and the Data Protection Authority (Jersey) Law 2018 (as the same may be amended, varied or replaced) (the "**DPL**") and to the extent applicable, the EU data protection regime introduced by the General Data Protection Regulation (Regulation 2016/679, collectively with the DPL, hereinafter referred to as the "**Data Protection Legislation**").

1.3 References in this policy to the Board refer to the Board of Directors of the Company.

1.4 This Policy describes how Personal Data must be collected, handled, stored, disclosed and otherwise "processed" to meet the Company's data protection obligations and to comply with the Data Protection Legislation.

1.5 The purpose of this Policy is to ensure that everyone involved in the Processing of Personal Data at the Company is fully aware of, and complies with, the requirements of the Data Protection Legislation.

1.6 An External Privacy Notice has been approved by the Board to inform external individuals how their Personal Data is processed. An Internal Privacy Notice has also been approved. Both this Policy and these Privacy Notices are readily available to Data Subjects who are connected to the Company (including, but not limited to shareholders, settlors, founders, beneficiaries, protectors, enforcers, individual directors and any person, whether corporate or unincorporate, with an interest in the Company through any relevant agreement). These documents are available online at https://international.standardbank.com/international/personal/about-us/legal

1.7 In preparing the Policy, the Company has taken into account the nature, scale and complexity of its business and, in particular, the fact that it relies broadly on an outsourced model and the support of its delegates and affiliates for the performance of its functions. As the Company does not regularly and systematically monitor Data Subjects on a large scale, it has not appointed a data protection officer. The Board is ultimately responsible for ensuring that the Company meets its legal obligations and operates in full compliance with the Data Protection Legislation.

2 Definitions

2.1 "**Data Controller**" means any natural or legal person, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data (in this case, the Company).

2.2 "**Data Processor**" means a natural or legal person who processes Personal Data on behalf of the Data Controller such as an administrator, distributor and/or other delegates that receive Personal Data.

2.3 "**Data Subject**" means an identified or identifiable natural person who is the subject of Personal Data.

2.4 "**Personal Data**" means any personal information relating to a Data Subject, such as name, residential address, email address, contact details, corporate contact information, signature, nationality, place of birth, date of birth, tax identification, credit history, correspondence records, passport number, bank account details, source of funds details and details relating to a shareholder or investor's investment activity.

2.5 "**Privacy Notice**" means the data protection disclosure statement prepared in respect of the Company outlining the Company's data protection obligations and the data protection rights of Data Subjects investing in the Company, as required under the Data Protection Legislation.

2.6 "**Processing**" means performing any operation or set of operations on Personal Data, whether or not by automatic means, including collecting, recording, organising, storing, amending, using, retrieving, disclosing, erasing or destroying it.

2.7 **"Supervisory Authority"** means the Jersey Office of the Information Commissioner.

3 **The Company as Data Controller**

3.1 The Company is a Data Controller and shall comply with its obligations as such under the Data Protection Legislation.

3.2 When Processing Personal Data, there may also be times where other service providers to the Company (including the Administrator), to the extent they determine the purpose and the means of processing, may also be characterised as Data Controllers under the Data Protection Legislation. This, however, does not exonerate the Company from its responsibilities as a Controller. It is important that if there is any risk of the Company acting as a Controller jointly with a service provider, a review of the contractual arrangements as to the determination of the purpose and means of data processing and the attribution of responsibilities between the two, be comprehensively considered for governance and legal reasons.

3.3 The Company has authorised the Administrator to register the Company with the Jersey Office of the Information Commissioner and pay the requisite processing fee of £50.

4 **Service Providers to the Company**

4.1 The Company has appointed various service providers to the Company. In the main, they will act as Data Processors to the Company (save as set out at paragraph 3.2 above).

4.2 Where service providers or other third parties provide the Company with Personal Data concerning Data Subjects (e.g., tax advisers providing details about their clients), they must ensure that the

affected individuals are informed of the existence of this Policy and the relevant Privacy Notice. For example:

a) if you are an estate agent and you secure tenants for a property owned by the Company, you should draw the attention of the tenants to the External Privacy Notice;

b) if you are a tax advisor and you provide us with personal information about your clients or their beneficiaries, you must ensure that those individuals are made aware of the External Privacy Notice.

4.3 This Policy and the relevant Privacy Notices are readily available at https://international.standardbank.com/international/personal/about-us/legal

5 Data Protection Principles

5.1 The Data Protection Legislation sets out certain data protection principles with which the Company and its service providers must comply.

5.2 Personal Data shall be:

(a) Processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**).

(b) Collected only for specified, explicit and legitimate purposes (**Purpose Limitation**).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (**Data Minimisation**).

(d) Accurate and where necessary kept up to date (**Accuracy**).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (**Storage Limitation**).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (**Security, Integrity and Confidentiality**).

(g) Not transferred to another country without appropriate safeguards being in place (**Transfer Limitation**).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (**Data Subjects' Rights and Requests**).

5.3 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (**Accountability**).

5.4 Fair and transparent Processing

Fairly obtained Personal Data generally requires that the Data Controller, either before or at the time the Personal Data is collected, makes the Data Subject aware of certain information.

The Company generally meets these requirements through the provision to Data Subjects of a Privacy Notice. We have produced two privacy notices. The first is an Internal Privacy Notice for directors, officers, employees and consultants of the Company. The second is an External Privacy Notice. The External Privacy Notice for shareholders of the Company and their advisors, officers and employees (if any), and any other relevant external stakeholders of the Company.

The Company will ensure that all information and communications relating to the Processing of Personal Data will be clear, concise, transparent, intelligible, easily accessible and easy to understand using clear and plain language. The Company will ensure that these transparency requirements are adhered to at all stages of the collection and Processing of Personal Data.

If any of the information described above changes after it has been provided to the Data Subject, the Data Subject shall be provided with an update to the information.

5.5 Security

In Processing Personal Data, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. In particular, the Company shall take all appropriate security, technical security and organisational measures to address the risks of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

Given that the Company utilises service providers for its systems, the Company will seek assurances from any service providers that act as Data Processors for the Company that they have implemented appropriate information security measures which comply with the relevant conditions of the Data Protection Legislation.

5.6 Transferring Personal Data to a country outside the EEA

The Company itself will not transfer Personal Data but anticipates that its Data Processors may transfer Personal Data to entities located outside of both Jersey and the EEA .

Data Processors may only transfer Personal Data outside of both Jersey and the EEA (a) with the written consent of the Company (which will only be provided subject to certain conditions being satisfied); (b) where required to do so by EU law or the law of an EU member state to which the relevant Data Processor is subject or (c) in certain limited circumstances, set out in the Data Protection Legislation e.g.: in pursuance of compliance with decisions of public authorities of the Island of Jersey based on an international agreement improving international obligations on the Island of Jersey.

Such transfers shall be subject to the provision by the Data Processor of appropriate safeguards in compliance with Data Protection Legislation, and to the availability of rights and effective legal remedies for Data Subjects, or shall otherwise comply with the requirements of the Data Protection Legislation.

6 **Data Subject Rights**

6.1 The Company has appointed the Administrator to manage the exercise of Data Subject rights.

7 **Keeping records of all Processing**

7.1 A record of the Company's Processing activities is maintained by the Administrator.

7.2 The Company will retain Personal Data for a period of up to 10 years following (1) the Data Subject's disinvestment from the Company, or (2) the termination of the Data Subject's relationship with the Company. Information may be retained for a longer period where this is necessary for compliance with a legal obligation or for the establishment, exercise or defence of a legal claim. The Company and its duly authorised delegates will refrain from collecting any further Personal Data and shall take appropriate steps to dispose of any records containing Personal Data, to the extent that this is operationally feasible and proportionate.

8 **Reporting of Personal Data breaches**

8.1 We have appointed the Administrator to assist in dealing with and reporting Personal Data breaches.

8.2 If the Company detects and records a Personal Data breach, it shall notify the Supervisory Authority without delay, and in any case not later than 72 hours, unless the breach is unlikely to result in a risk to the rights and freedoms of the Data Subject.

8.3 Each Data Processor shall notify the Company without undue delay after becoming aware of a Personal Data breach and shall include in any such notification the applicable information referred to in the Data Protection Legislation and shall provide all reasonable assistance to the Company in connection with any such Personal Data breach, including, in particular, facilitating the Company communicating details of any Personal Data breach to the relevant Data Subject, if required.

8.4 The Company shall document all Personal Data breaches, comprising the facts relating to the Personal Data breach, its effects and the remedial action taken.

8.5 Unless one of the conditions set out in sub-paragraphs (a) to (c) below are met, the Data Subject must also be notified without undue delay if the Personal Data breach is likely to result in a high risk to their rights and freedoms. The notification shall describe in clear and plain language the nature of the breach, the name of the contact point where more information can be obtained, the likely consequences and measures taken to mitigate or address the breach.

Notification to the Data Subject is not required in the following circumstances:

(a) where the relevant Personal Data is encrypted/protected in a manner making it unintelligible to unauthorised persons;

(b) where the Company has taken subsequent measures which ensure that the high risk to the Data Subject's rights and freedoms is no longer likely to materialise;

(c) where an individual notification would involve disproportionate effort (e.g. public communication or similar is sufficient).

9 Board Oversight and Updates to this Policy

9.1 This Policy is effective from 24 July 2025 and supersedes and replaces any previous Data Protection Policy applicable to a Company to which the Administrator renders services.

9.2 The Board will be responsible for the oversight of compliance with this Policy. It will review the appropriateness of this Policy annually and will ensure that it is operating as intended. It will also review this Policy to ensure that it continues to be compliant with applicable national and international regulations, principles and standards.

9.3 This Policy shall be reviewed and updated as necessary on at least an annual basis or as and when required or deemed necessary by the Company. Material changes to this Policy will be approved by the Board.