DATA PROCESSING AGREEMENT ('DPA')

This is the standard Data Processing Agreement of Cartlidge Morland Limited/The Cartlidge Morland Partnership/Cartlidge Morland Wealth Management LLP *('Cartlidge Morland')* ('the Processor') upon which we intend to rely.

It sets out how the Processor intends to comply with the General Data Protection Regulation (EU/2016/679), ('the Regulations') and is designed to come into force upon receipt.

The Processor will assume that you ('the Controller') consent to this agreement unless we receive written confirmation from you to the contrary. The scope, nature, purposes and duration of the processing and the types of personal data and categories of data subject are set out below.

The lawful basis under which the firm processes all categories of personal data is legitimate interest. The Processor (and any company associated with the firm) treats all personal and special category data as confidential and will not process it other than for a legitimate purpose. The Processor has considered the changes to the wider definitions; all categories of personal data are treated with the utmost care to ensure compliance.

The purpose of the processing under to this Agreement is the provision of employment benefit services. All employee personal data provided by the data Controller to the Processor for the provision of employment benefit services is subject to this Agreement.

The Processor Shall

- only act on the written instructions of the Controller (unless required by law to act without such instructions)
- ensure that people processing the data are subject to a duty of confidence
- take appropriate measures to ensure the security of processing
- keep records of its processing activities in accordance with Article 30.2
- assist the data Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- assist the data Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments
- delete or return all personal data to the Controller as requested at the end of the contract
- provide the controller with all information necessary to demonstrate that all obligations arising from the agreement have been met, including the participation in audits by the Controller or an appointed third party
- inform the Controller immediately if it is asked to do something infringing the GDPR or other relevant legislation
- notify any personal data breaches to the Controller in accordance with Article 33
- co-operate with supervisory authorities (such as the ICO) in accordance with Article 31
- only engage a sub-processor with the prior consent of the data Controller and a written contract
- impose the same safety measures on sub-processors as those on which the Processor is itself held on the basis of this agreement
- accept liability if a subcontractor does not fulfil its obligations regarding securing of data

Duration of Processing

The requirements of this DPA shall continue to apply for so long as Processor continues to provide services to the data Controller under the Agreement and for as long as those services continue to include the processing of personal data.

If you, the Controller, wish to terminate the processing under the terms of this Agreement you should notify us in writing at our London address. From the date we receive notification of termination our ongoing responsibility, as Processor, shall cease. We shall complete any transactions already in progress on your behalf and shall remain entitled to receive our professional charges in respect of such transactions.

The Processor will not usually terminate our relationship with you, the data Controller, on less than 30 days' notice. We reserve the right to terminate our relationship with you immediately if we consider that trust and confidence between us has broken down irretrievably and our relationship with you has become unworkable. In these circumstances our charges and obligations shall be as specified above. Should the completion of any transaction require your reasonable cooperation and it is withheld, we shall accept no responsibility for the consequences of the failure of that transaction to proceed, or to complete.

The Rights of Data Subjects

Unless exemptions apply, data subjects have the right:

- to ask that their personal data is not processed for marketing purposes
- to access their personal data held about them and to obtain a copy of it;
- to prevent any processing of personal data that is causing or is likely to cause unwarranted and substantial damage or distress to them or another individual
- to request the rectification or completion of personal data which are inaccurate or incomplete
- to restrict or object to the processing of their personal data
- to request its erasure under certain circumstances
- if appropriate, to receive their personal data, which they have provided to the firm, in a machine-readable format
- if appropriate, the right to transmit or have transmitted that data to another data Controller where technically feasible
- to be informed about any use and impact of their personal data to make automated decisions about them
- to complain about the way in which their personal data is being used to the Information Commissioner's Office

The Processor will comply with the rights of data subjects and will assist the Controller to fulfil its obligation to respond to requests for exercising the data subject's rights.

The right to erasure is not an absolute right and details of circumstances where the right will not apply are provided at Article 17(3). This includes processing which is necessary for 'exercising the right of freedom of expression and information' as well as for reasons of public interest in the area of public health or for archiving purposes.

Through financial services regulation, the Processor is required by its regulator to maintain full client records clients, with the specified minimum time-frame for maintaining full records varying from 3-5 years to an indefinite period. The rules are set out in the Financial Conduct Authority's handbook **www.handbook.fca.org.uk/handbook/COBS/9/5**

Security

The Processor's systems and controls have been designed to protect the business and the rights of data subjects. The firm takes appropriate security measures (including physical, electronic and procedural measures) to help protect the confidentiality, integrity and availability of personal information from unauthorised access and disclosure.
The Processor has procedures in place to ensure that:

- unauthorized persons are unable to gain physical or remote access to data systems used for processing personal data
- persons entitled to access and use data processing systems gain access only to such data as they have access rights to
- during electronic transmission, transport or storage personal data cannot be read, copied, modified or deleted by unauthorized persons, and that compliance with this can be certified
- it is possible to verify whether personal data has been entered, altered or removed from data processing systems and if so, by whom
- personal data processed on behalf of others is processed only in accordance with the data Controller's instructions
- personal data is protected against accidental destruction or loss
- that data collected for different purposes can be processed separately

Data protection matters should be referred in the first instance to the Data Protection Officer on 020 7709 5560 or in writing at Cartlidge Morland, 83 - 85 Mansell Street, London, E1 8AN.

Cartlidge Morland
October 2018