<u>**DATA PROCESSING AGREEMENT**</u>

THIS DATA PROCESSING AGREEMENT IS ENTERED INTO ON THE DATE SIGNED BY PROCESSOR

PARTIES:

1. **Company** and

2. **Processor**,

(each a **party**, together the **parties**).

INTRODUCTION:

A. The Processor may, from time to time, provide certain services to the Company which services may include the processing of Personal Data on behalf of the Company (the **Services**).

B. The parties wish to set out the terms governing the parties' processing of Personal Data in connection with the Agreement and their roles and responsibilities in respect of Personal Data (as defined below) processed under the Agreement.

C. This Data Processing Agreement has been pre-signed on behalf of the Company. To complete this Data Processing Agreement, Processor must: (i) complete the information in the signature box and sign; (ii) send the signed Data Processing Agreement to the Company by email to contracts@derivco.com. Upon receipt of the validly completed Data Processing Agreement by the Company at this email address, this Data Processing Agreement will become legally binding.

D. For the mutual promises exchanged herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereby agree the following.

AGREEMENT:

1. **Definitions and Interpretation**

1.1 For the purposes of this Data Processing Agreement the following terms have the following meanings:

Agreement means any means any agreement (including agreements entered into or purported to be entered into after the date of this Data Processing Agreement, unless explicitly agreed otherwise in writing, signed on behalf of the parties) governing the provision of the Services. Whereby no such agreement exists, the Agreement means this Data Processing Agreement.

Competent Regulator means the competent data protection regulator, which, by way of example, is the ICO in England and Wales or the Information Regulator in RSA;

Data Processing Agreement means this data processing agreement, including the Introduction;

Data Protection Legislation means all applicable data protection, privacy and electronic marketing legislation, including any national legislation implementing Directive 95/46/EC and Directive 2002/58/EC, GDPR (and any related national legislation), any replacement or repealing legislation, POPIA, and any codes of practice issued by the Competent Regulator relating to the same;

EEA means the European Economic Area;

GDPR means Regulation (EU) 2016/679;

ICO means the Information Commissioner's Office;

Personal Data means the personal data processed by Processor on behalf of the Company through the provision of the Services by the Processor and where POPIA applies includes Personal Information;

PER   BJO

Personal Information shall have the meaning attributed to the term in section 1 of POPIA;

POPIA means the Protection of Personal Information Act 4 of 2013;

RSA means Republic of South Africa;

Restricted Transfer means: (a) a transfer of Personal Data from Company to a processor; or (b) an onward transfer of Personal Data from Processor to a sub-processor. In each case, where such transfer would be prohibited by Data Protection Legislation in the absence of the SCCs. For clarity, the parties to this Data Processing Agreement intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Legislation of the UK or EU Data Protection Legislation in the absence of the SCCs. A Restricted Transfer does not include transfers of Personal Data authorised by Data Protection Legislation in the exporting country, for example in the case of transfers from within the European Union to a country with an adequacy decision (such as Switzerland);

SCCs means the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, which clauses are found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF;

Services means any services as may applicable applying between the parties which may include the processing of personal data ; and

sub-processor means any processor appointed by Processor to assist with Processor's processing of Personal Data.

1.2   For the purposes of this Data Processing Agreement the terms **controller**, **data subject**, **personal data**, **process**, **processing**, **processor** and **pseudonymisation** shall have the meanings attributed to them in Article 4 of GDPR and where POPIA applies a **data subject** includes a juristic person as far as is applicable, and their cognate terms shall be construed accordingly.

1.3   Use of the terms **include** or **including** shall be construed without limiting the generality of the words preceding those terms.

1.4   References to **Clauses** are to clauses of this Data Processing Agreement.

2.   <u>**Acknowledgement of Roles**</u>

2.1   The parties hereby acknowledge that the Company is the controller and Processor is the processor in respect of Personal Data processed through the provision of the Services.

2.2   Company instructs Processor (and authorises Processor to instruct each sub-processor) to:

2.2.1   process Personal Data; and

2.2.2   transfer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with any Agreement.

2.3   Company warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in Clause 3.1.1. Company shall immediately inform Processor if, in its opinion, any instruction related to the processing of Personal Data infringes on any Data Protection Legislation.

2.4   **Error! Reference source not found.** to this Data Processing Agreement sets out certain information regarding the Processors' processing of Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Legislation). Company may make reasonable amendments to **Error! Reference source not found.** by written notice to Processor from time to time as Company reasonably considers necessary to meet those requirements.

PER   BJO

3. **Processor's Data Processing Obligations**

3.1   Processor shall:

3.1.1   only process Personal Data as is strictly necessary to fulfil any obligations to provide Services or in accordance with Company's express written instructions from time to time, and shall not process Personal Data for any other purposes save where it is required to process Personal Data pursuant to applicable laws and in such event, the Processor shall notify Company of that legal requirement before the relevant processing of that Personal Data;

3.1.2   be permitted to continue using those sub-processors already engaged by Processor as of the date of this Data Processing Agreement so long as the requirements set out in this Clause 3.1.2 are met. Processor shall give Company prior written notice of the appointment of any new sub-processor, including full details of the processing to be undertaken by the sub-processor. If, within ten (10) business days of receipt of that notice, Company notifies Processor in writing of its reasonable objections to the proposed appointment:

(a)   Processor shall work with Company in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed sub-processor or addresses such objections; or

(b)   where such a change cannot be made within thirty (30) business days from Processor's receipt of Company's notice, Company may immediately terminate the applicable Services order to the extent that it relates to the Services which require the use of the proposed Processor.

3.1.3   carry out adequate due diligence to ensure that any sub-processor is capable of providing the level of protection for Personal Data required by this Data Processing Agreement before the sub-processor first processes Personal Data and shall not appoint a sub-processor without the Company's consent and in the event that the Company does provide such consent Processor shall ensure that the sub-processor is bound by the terms of this Clause as it applies to Processor hereunder;

3.1.4   not transfer Personal Data outside the EEA or the RSA, whichever may be applicable, without the prior written consent of Company except as permitted and subject to Clause 3.4 below;

3.1.5   provide all reasonable assistance to Company to enable Company to comply with its obligations under Data Protection Legislation in respect of Personal Data, including assisting Company in complying with a data subject's right to access and to portability;

3.1.6   at the end of this Data Processing Agreement, promptly delete or return to Company (at Company's discretion) all Personal Data (including any Personal Data subcontracted to a sub-processor for processing) and provide written notice to Company to confirm that such deletion or return has been completed. This requirement will not apply to the extent that Processor is required by any applicable law or regulation to retain some or all of the Personal Data, in which event Processor will isolate and protect the Personal Data from any further processing except to the extent required by such law;

3.1.7   promptly comply with any request from Company requiring Processor to amend, transfer or delete Personal Data;

3.1.8   in the event that Processor receives any complaint, notice or communication (from either a Competent Regulator or a data subject) which relates directly or indirectly to the processing of Personal Data or to either party's compliance with Data Protection Legislation, Processor shall notify Company without undue delay and it shall provide Company and any Competent Regulator (if applicable) with full co-operation and assistance in relation to any such complaint, notice or communication. Processor shall not respond except on the documented instructions of Company or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by Data Protection Legislation inform Company of that legal requirement before Processor responds;

3.1.9   not disclose Personal Data to any data subject or to a third party other than at the request of Company;

PER   BJO

3.1.10   notify Company without undue delay upon becoming aware of any unauthorised or unlawful processing, loss of, damage to or destruction of any Personal Data. Processor shall co-operate with Company and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation in relation to Clause 3.1.10;

3.1.11   comply with any reasonable codes of practice or policies of the Company relating to Personal Data, as notified to Processor from time-to-time;

3.1.12   maintain all appropriate records of processing carried out in respect of Personal Data in accordance with GDPR and, where apposite, POPIA;

3.1.13   notify Company in the event that Processor discovers (or reasonably suspects) that any instructions given by Company breach Data Protection Legislation;

3.1.14   upon request by Company, provide written evidence demonstrating its compliance with this Clause; and

3.1.15   take appropriate technical and organisational security measures (taking into account the risks associated with processing, including, inter alia, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the associated risk to the rights and freedoms of natural persons) against the unauthorised or unlawful processing of Personal Data, and against the accidental loss or destruction of, or damage to Personal Data, such measures may include (where appropriate):

(a)   the pseudonyimisation and encryption of Personal Data;

(b)   the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c)   ensuring that all individuals, parties, employees or other persons/entities with access to Personal Data are granted access on a "need to know" basis only and are bound by industry standard confidentiality obligations no less restrictive than those imposed by the Agreement which include keeping such Personal Data confidential;

(d)   the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(e)   a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.2   Processor shall keep at its normal place of business detailed, accurate and up-to-date records (whether in electronic form or hard copy) relating to the processing of Personal Data by Processor and to the measures taken by Processor under Clause 3.1.15 (**Records**).

3.3   Processor shall permit Company and its mutually agreed third-party representatives, on reasonable notice during normal business hours, but without notice in case of any reasonably suspected breach of Clauses 3.1.10 - 3.1.15, to:

3.3.1   gain access to, and take copies of, the Records and any other information held at Processor's premises or on Processor's computer systems; and

3.3.2   inspect all Records, documents and electronic data and Processor's computer systems, facilities and equipment,

as necessary for the sole purpose of auditing Processor's compliance with its obligations under this Data Processing Agreement. Company shall be responsible for the costs associated with such audit. Such audit rights may be exercised only once in any calendar year during the term of this Data Processing Agreement. Audit rights of Company only arise under this Clause to the extent that the Agreement does not otherwise give audit rights meeting the relevant requirements of Data Protection Legislation (including, where applicable, article 28(3)(h) of the GDPR).

3.4   For so long as the Processor or sub-processor is in a third country which does not ensure an adequate level of data protection pursuant to Article 45 of the GDPR and in respect of any Restricted Transfer from Company to Processor, the parties undertake to each other to comply with the SCCs, and such SCCs are incorporated by reference into this Data Processing Agreement. SCC's shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Legislation. The SCCs shall come into effect on the later of: (i) the data exporter becoming a party to them; (ii) the data importer becoming a party to them; and (iii) commencement of the relevant Restricted Transfer. To the extent there is any conflict between the provisions of this Data Processing Agreement and the provisions of the SCCs, the provisions of the SCCs shall prevail. Where the SCCs apply, Appendix 1 and Appendix 2 hereto shall apply. Processor warrants and represents that, before the commencement of any Restricted Transfer to a sub-processor, the SCC's will have been duly and effectively authorised by that sub-processor and will be binding on that sub-processor in accordance with their terms.

4.   **Indemnity**

Notwithstanding any other provisions of this Data Processing Agreement, any limitations on liability set out in any Agreement shall not apply to Processor's liability to Company for a breach of its obligations under this Data Processing Agreement. Processor agrees to indemnify Company and hold harmless Company at Processor's own expense from and against all loss, costs, harm, claims, fines, group actions, liabilities or damages or expenses (including reasonable legal fees) suffered or incurred by Company or for which Company may become liable due to any failure by Processor or its employees, agents, subcontractors or sub-processors to comply with any of its obligations under this Data Processing Agreement. Nothing in any other agreement between the parties shall limit Processor's liability under this indemnity.

5.   **Term and Termination**

This Data Processing Agreement shall take effect upon the commencement of the Services and shall remain in effect for so long as the Processor is providing Services.

6.   **Survival**

Clauses 3.1.6 - 3.1.10 (inclusive), 3.1.12 - 3.1.15 (inclusive), 3.2, 4 and 7 shall survive the termination or expiry of this Data Processing Agreement.

7.   **General**

7.1   This Data Processing Agreement is an addendum to and forms part of the Agreement and the terms of such Agreement shall remain in full force and effect.   In the event of any conflict between the terms of this Data Processing Agreement and any Agreement, the provisions of this Data Processing Agreement shall take precedence. This Data Processing Agreement (i) shall not replace any comparable or additional rights relating to processing of the Company's data contained in the Agreement (including any existing data processing addendum to the Agreement); (ii) appends the provisions in the Agreement that relate expressly to the parties' use of personal data; and (iii) amends any other provisions in the Agreement that conflict with the terms of this Data Processing Agreement.

7.2   A person who is not a party to this Data Processing Agreement may not enforce any of its terms under the Contracts (Rights of Third parties) Act 1999.

7.3   Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the SCCs, this Data Processing Agreement is governed by and will be construed in accordance with laws of Company: if Company is registered in Europe, this Data Processing Agreement shall be governed by the laws of England and Wales; if Company is registered outside Europe, this Data Processing Agreement shall be governed by the laws of South Africa and the parties irrevocably will be subject to the exclusive jurisdiction and venue of the courts of the capital city of the state or country whose laws govern with respect to any disputes or claims howsoever arising under this Data Processing Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity without giving

effect to any principles that provide for the application of the law of another jurisdiction, in respect of all matters arising out of or relating to this Data Processing Agreement, its performance or subject matter.

7.4   This Data Processing Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

7.5   Should any provision of this Data Processing Agreement be invalid or unenforceable, then the remainder of this Data Processing Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS whereof the parties have by their duly authorised representatives executed this Data Processing Agreement as at the date first before written.

Signed on behalf of the Company		Signed on behalf of the Processor	
Company Name	Derivco (Pty) Ltd	**Company Name**	
Signature (duly authorised)		**Signature** (duly authorised)	
Signatory Name	Ben Oates	**Signatory Name**	
Position	CFO	**Position**	
Date	1 July 2021	**Date**	
Signed on behalf of the Company		Signed on behalf of the Processor	
Company Name	Derivco (Pty) Ltd	**Company Name**	
Signature (duly authorised)		**Signature** (duly authorised)	
Signatory Name	Princeton Reddy	**Signatory Name**	
Position	Financial Manager	**Position**	
Date	1 July 2021	**Date**	

Data exporter

The data exporter is the Company.

Data importer

The data importer is the Processor.

Data subjects

The personal data transferred concern data subjects (individuals) who are:

- The Company's employees, agents, personnel, consultants, service providers and customers and family membersof such individuals; and

- Job seekers and prospective employees

Categories of data

The personal data transferred concern the following categories of data:

- Data related to proof of identity including identity number, passport number, gender, full name, date of birth,marital status, next of kin, dependents, address, email address, telephone numbers;

- employment related data, including CVs, work history, proof of nationality and entitlement to work;

- financial related data including bank account details and national security number.

Special categories of data (if appropriate)

Race and ethnic origin, religion or beliefs and health data.

Processing operations

The Personal Data transferred will be subject to the following basic processing activities by the data importer(Processor):

- Processing Personal Data as necessary to perform the Services for Company pursuant to the Agreement.

- The Duration of the processing of Personal Data will be the duration of the Services to be provided under the Agreement.

PER   BJO

The data importer (the Processor) warrants that, for the duration of the Data Processing Agreement, it implements the following technical and organisational security measures:

Technical measures: The security of Personal Data processed by the Processor is paramount and to this end the Processor adopts IT systems and software to protect Personal Data, specifically: all communications to theProcessors systems are secured and actively monitored 24/7 to alert on any Personal Data query incidences. Access to the Processor's systems and entry to the Processor's buildings and to buildings where Personal Data is hosted, is restricted to Processor personnel and authorised persons only.

Organisational measures: All staff who handle Personal Data on behalf of the Processor are bound by confidentiality. Furthermore, the Processor trains all relevant staff regarding use of Personal Data and how to keep Personal Data secure, including having in place policies governing the protection and security of data including, without limitation, a data protection policy.

PER   BJO