

EFTSURE AFRICA PROPRIETARY LIMITED (“Eftsure Africa” or the “Company”)

DATA PROCESSING ADDENDUM (“DPA”)

1. INTRODUCTION

This Data Processing Addendum (“DPA”) to the terms relating to the collection, storage, processing and use of personal data and other information, supplements the Privacy Statement and Data Protection Policy (Annex 1 to the terms), to provide for the matters contemplated in section 21(1) read with section 19 of POPI.

2. DEFINITIONS

Capitalised terms used in this DPA and not expressly defined herein shall bear the same meaning ascribed to them in the terms to which this document is Annex 2, unless the context clearly indicates otherwise.

In addition, in this DPA, unless inconsistent with or otherwise indicated by the context, the definitions set out hereunder shall bear the following meanings ascribed to them –

“**Data Security Incident**” means any breach of security to the Company’s technical and organisational measures leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise Processed by the Company;

“**Payee**” means a supplier, service provider, employee or other person or entity to whom the Company’s Customer wishes to make payment and whose details it wishes to verify by means of the Services offered by the Company;

“**Personal Information**” means any information relating to an identified or identifiable Data Subject or as otherwise defined by applicable law;

“**POPI**” means the Protection of Personal Information Act, 4 of 2013, together with any regulations promulgated thereunder from time to time and any other data protection or privacy laws applicable to the Company or to the Services;

“**Process**” means any operation or set of operations that is performed upon Personal Information, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, return or destruction, and “**Processed**” and “**Processing**” shall be construed accordingly;

“**Services**” means any and all services and business management products provided by or on behalf of the Company pursuant to its agreement with its Customer in connection with any Personal Information, including, without limitation, making available the Company’s cloud-based payee verification platform; and

“**Sub-Operator**” means an entity engaged by the Operator (or any further Sub-Operator) to Process Personal Information on behalf and under the authority of the Responsible Party.

The terms “**Data Subject**”, “**Information Regulator**”, “**Operator**” and “**Responsible Party**” shall have the same meanings as defined in POPI.

3. EFFECTIVE DATE

This DPA shall be effective from the same date as referred to in the online terms of which this Annex 2 is a part.

4. PROCESSING OF PERSONAL INFORMATION

Compliance with POPI. The Company will comply with POPI in the Processing of Personal Information and will not Process Personal Information other than as set out in the online terms (including Annexes 1 and 2) or on the relevant instructions from the Company’s Customer or any Data Subject or as may otherwise be required by applicable law.

Subject matter and duration. The subject matter and duration of the Processing of the Personal Information are set out in the terms which include this DPA.

Nature and purpose. The nature and purpose of the Processing of Personal Information entails, *inter alia*, the onboarding, screening and verification of Payees for purposes of authorising payments by Customer and the processing of other business documents such as, without limitation, invoices and statements rendered by you to the Customer..

Types of Personal Information. The types of Personal Information to be Processed comprise identifying particulars of individuals, registration details of entities, contact and address information, bank account and branch numbers, VAT status and other related information pertaining to Payees and their representatives, invoices, statements and payment and receipt records.

Category of Data Subjects. The category of Data Subjects to whom the Personal Information relates is predominantly suppliers, employees, business partners and prospective business partners.

Obligations and rights of Customer. The obligations and rights of Customer are set out in the terms (including this DPA).

5. THE COMPANY'S OBLIGATIONS

Roles. With respect to the Services, the Company's Customer is the Responsible Party in connection with each Payee's Personal Information, and the Company is the Operator on behalf of Customer in connection with such Personal Information.

Processing. The Company processes the Personal Information strictly to the extent necessary to perform the Services as described in the Agreement which the Company has with its Customer, and in accordance with any other valid, documented instructions of Customer or any Data Subject.

Confidentiality. The Company will make every reasonable effort to maintain the confidentiality of all Personal Information and will take commercially reasonable steps to procure same from, and to ensure the reliability of, any employee, agent or contractor who may have access to the Personal Information, endeavouring to ensure, in each case, that access is limited to those individuals who need to access the relevant Personal Information strictly for the purposes necessary to perform the Services and that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

Technical and organisational measures. 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, the Company shall, in relation to Personal Information, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Information, including, as appropriate, the measures required by section 19 of POPI. The Company may implement adequate alternative security measures from time to time, provided the security level of the alternative measures is not materially decreased.

Sub-Operators. The Company may engage the services of Sub-Operators to perform the Services and may continue to use those Sub-Operators already engaged by the Company as at the date of your acceptance of the electronic terms. The Company will make reasonable efforts to ensure that such Sub-Operators are bound by written agreements that require them to provide at least the level of data protection required herein.

Data Subject rights. Taking into account the nature of the Processing, the Company usually agrees with its Customers to assist them by implementing appropriate technical and organisational measures, insofar as this is practicable, for the fulfilment of Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subjects' rights under POPI. The Company will notify its Customer if the Company receives a request from a Data Subject to have access to his or her Personal Information under POPI and shall cooperate with Customer in responding to such request. The Company will not respond to any Data Subject request unless required by applicable law.

Notification of Data Security Incident. To the extent that the Company experiences a Data Security Incident with respect to the Personal Information that the Company Processes as part of its performance of the Services, the Company will notify its Customer promptly and without undue delay upon becoming aware of such Data Security Incident, providing Customer, to the extent possible, with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Data Security Incident under POPI. The Company will mitigate, to the extent practicable, any harmful effect of such Data Security Incident.

Co-operation. The Company will provide reasonable assistance to its Customer with any data protection impact assessment and with any prior consultations to any supervisory authority, including the Information Regulator, to the extent required by applicable law, in each case solely in relation to Processing of Personal Information by the Company on behalf of its Customer and as such Processing relates to the Services.

Destruction of Personal Information. After the end of the provision of Services, the Company will, at the choice of its Customer, either:

- 5.9.1 return a complete copy of all Personal Information to its Customer by secure file transfer in such format as may be agreed by those Parties in writing; or
- 5.9.2 delete all copies of Customer-specific Personal Information Processed by the Company or any of its Sub-Operators, other than such information as has been aggregated into the Company's whitelist (comprising high-level bank account details, the underlying entity information and VAT information) or unless applicable law requires continued storage of such Personal Information.

Demonstrated compliance. Upon prior written notice by the Company's Customer, the Company will make available to its Customer all information reasonably necessary to demonstrate compliance with the terms set forth in this DPA, including verification of whether the procedures for the technical and organisational requirements of data protection and information security are appropriate. The Company will promptly notify its Customer if, in the Company's opinion, the Processing instructions are in violation of POPI.

Transfers of Personal Information.

- 5.11.1 Given the nature of the Services, Personal Information may be transferred to foreign countries that may not have the same data protection laws as the country of original collection. Such transfer of Personal Information to foreign countries is necessary for the performance of contractual services between Customer and its Payees. Thus, for the purposes of establishing the appropriate safeguards in accordance with POPI, the transfer of Personal Information is hereby legitimised on the basis that such transfer is necessary for the performance of a contract between Customer and the applicable Data Subjects.
- 5.11.2 To the extent (i) that appropriate safeguards set forth in paragraph 0 are not sufficient to legitimise the lawful transfer of Personal Information to foreign countries, (ii) required by applicable law with respect to the Services provided, or (iii) requested by the Company's Customer, the Company agrees to execute a data transfer agreement governing the transfer of Personal Information in a form mutually acceptable to those Parties. To the extent there exists a conflict between the signed data transfer agreement and this clause 0, the signed data transfer agreement shall prevail to the extent of the conflict.
- 5.11.3 To the extent applicable, it may be necessary for the Company, in fulfilment of the Services or its Customer's documented instructions, to transfer Personal Information to a third-party agency or authority, including, without limitation, various governmental and/or quasi-governmental agencies, customs officials, and similar entities ("**Governmental Agencies**"), which itself may be located outside of the Republic of South Africa. Insofar as the Governmental Agencies make independent decisions as to the

purposes for and means of Processing of Personal Information, the Governmental Agencies are acting in the capacity as an independent Responsible Party and not as a Sub-Operator to the Company. Thus, the Company shall not be liable for the Processing of Personal Information by the Governmental Agencies.

6. CUSTOMER RESPONSIBILITIES

In performing the Services to its Customer or documented instructions on behalf of its Customer, the Company is relying on the following information to be true and accurate:

- 6.1 Customer is the Responsible Party and the Company is the Operator acting on its Customer's behalf;
- 6.2 Its Customer instructs the Company to Process Personal Information in order to provide the Services, including, without limitation, to transfer such Personal Information to any country or territory as is reasonably necessary for such purposes, consistent with the Agreement;
- 6.3 The Company's Customer is required to comply with all applicable laws and regulations related to privacy, data protection and confidentiality, including, without limitation, POPI;
- 6.4 The Customer shall be responsible for notifying or otherwise obtaining the consent of the Data Subject (unless other lawful mechanisms for transfer apply) for the Processing of the Personal Information; and
- 6.5 to the extent applicable, the Company's Customer shall be responsible for notifying or otherwise gaining approval of any regulatory body, including the Information Regulator, to the data transfer arrangements anticipated in the Agreement.