

ANNEXURE D

PERSONAL INFORMATION PROCESSING ADDENDUM TO THE SERVICES AGREEMENT IN RESPECT OF THE PROVISION OF DAY-TO-DAY ELECTRICAL MAINTENANCE SERVICES – RFP

PREAMBLE

This Addendum –

- a. serves as the written agreement between the Service Provider as Operator and SARS as Responsible Party as contemplated in section 21 of POPIA;
- b. sets out the specific terms and conditions on which the Service Provider must process Personal Information relating to the Services Agreement; and
- c. is an integral part of and must be read with the Services Agreement.

1. INTERPRETATION AND DEFINITIONS

1.1 In this Addendum, unless clearly inconsistent with or otherwise indicated by the context:

1.1.1 “**Addendum**” means this Personal Information processing addendum;

1.1.2 “**Contractual Purposes**” means the exclusive purpose for which the Service Provider may lawfully process Personal Information furnished by SARS in terms of the Services Agreement, which is the execution by the Service Provider of the Services;

1.1.3 “**Services Agreement**” means the Services Agreement concluded between the Parties pursuant to SARS’ procurement process under reference RFP

1.1.4 “**Operator**” is as defined in POPIA, and in this Addendum, specifically refers to the Service Provider;

1.1.5 “**Personal Information Breaches**” means the accidental, unauthorised, or unlawful processing, access, copying, modification, reproduction, display or

distribution of Personal Information, including the accidental or unlawful loss, destruction, alteration, disclosure and damage of or to Personal Information;

1.1.6 **“Process”** and/or **“Processing”** is as defined and contemplated in POPIA; and

1.1.7 **“Responsible Party”** is as defined in POPIA, and in this Addendum, specifically refers to SARS.

1.2 Unless a definition is expressly amended herein, words and phrases defined in the Services Agreement shall bear the same meaning in this Addendum, and in the event of there being a conflict between the terms and conditions of the Services Agreement and those of this Addendum, the provisions of this Addendum shall prevail and take precedence, in so far as the conflict relates to matters which are the subject of this Addendum.

1.3 Terms / Wording defined in POPIA and used in this Addendum bear definitions contained in POPIA, except where otherwise defined or amplified herein.

1.4 The principles of interpretation stated in the Services Agreement apply to this Addendum.

2. SERVICE PROVIDER'S OBLIGATIONS IN RELATION TO PERSONAL INFORMATION

2.1 General Obligations

The Service Provider must –

2.1.1 process Personal Information only to the extent, and in such a manner, as is necessary for Contractual Purposes;

2.1.2 not process Personal Information for any other purpose or in a way that does not comply with this Addendum; the Services Agreement; POPIA or other Applicable Law;

2.1.3 where SARS issues an instruction to the Service Provider and the Service Provider is of the view that such instruction is inconsistent with POPIA or

other related Applicable Law, the Service Provider must immediately notify the Designated Representative, and await SARS' written response on the pertinent issue;

2.1.4 immediately comply with any written instructions by SARS to stop processing any Personal Information; and

2.1.5 where required, assist SARS at no additional cost, with meeting SARS' regulatory compliance obligations under POPIA in so far as such compliance relates to or is in connection with the Services or Personal Information provided to the Service Provider by SARS.

2.2 Obligations relating to the Service Provider's Personnel

2.2.1 The Service Provider must ensure that the Service Providers' Personnel –

- a) are informed of the confidential and sensitive nature of Personal Information;
- b) are bound by written confidentiality / information protection obligations, and have in place limitations of access or access restrictions in respect of Personal Information;
- c) have undertaken training on POPIA and understand how it relates to their handling of Personal Information and how it applies to their duties; and
- d) are aware of both the Service Provider's duties and obligations, and their personal duties and obligations under POPIA and the Services Agreement; and do in fact comply therewith.

2.2.2 The Service Provider must, as necessary, conduct background checks consistent with Applicable Law and take reasonable steps to ensure the reliability, integrity and trustworthiness of the Service Provider's Personnel with access to Personal Information.

2.3 Obligations relating to Information Security Measures

2.3.1 The Service Provider must –

2.3.1.1 implement security measures and maintain in place, for the duration of the Services Agreement, appropriate technical and

organisational measures as contemplated in section 19 of POPIA to secure the integrity and confidentiality of Personal Information and prevent Personal Information Breaches. Such measures must provide a level of security commensurate with corresponding risks, and may, as appropriate, include –

- a) the pseudonymisation and encryption of Personal Information;
- b) restricted access and complex passwords;
- c) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- d) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident; and
- e) processes for regularly testing, assessing and evaluating the effectiveness of the security measures.

2.3.1.2 ensure, at all times, that the security measures are no less than what is prescribed by Applicable Law, and are, in addition, on par with applicable industry best practices for the security of information;

2.3.1.3 regularly conduct risk assessments and assess the sufficiency and adequacy of the measures envisaged above, and accordingly update the measures to ensure that any new risks or deficiencies identified are effectively addressed; and

2.3.1.4 regularly conduct verification processes to ensure that the measures envisaged above are indeed implemented and functional. The Service Provider must retain records of its verification processes and make such available to SARS on request.

2.3.2 The Service Provider must immediately, in writing, notify the Designated Representative at their provided email addresses, as well as the SARS Contracts Management office at the email address: Proc.OPE@sars.gov.za (Attention: Contracts Management), and the SARS Anti-Corruption Unit at

the email address: Anti-Corruption@sars.gov.za, where the Service Provider or the Service Provider's Personnel have reasonable grounds to believe or suspect that there has been a Personal Information Breach in respect of any Personal Information processed or held by the Service Provider pursuant to the Services Agreement.

- 2.3.3 Immediately following any Personal Information Breach, the Parties must meet to discuss the matter as necessary. The Service Provider must, at no additional cost, co-operate with and assist SARS in its further handling of the matter, including but not limited to:
- (a) assisting with any investigation;
 - (b) providing SARS with physical access to any systems, facilities and operations affected;
 - (c) facilitating interviews with the Service Provider's Personnel, including former employees and other parties involved in the matter;
 - (d) making available all relevant records, logs, files, Personal Information reporting and other material required to comply with POPIA or as otherwise reasonably required by SARS; and
 - (e) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Information Breaches, subject to **clause 13.1** of the Services Agreement.

2.4 SARS' Audit Rights

2.4.1 The Parties recognise that compliance with POPIA is material and critical to the successful implementation of the Services Agreement. SARS will, as part of honouring its legislative obligations as Responsible Party and as a POPIA compliance risk management strategy on its part, be entitled to monitor and audit the Service Provider's compliance with the Services Agreement, in general, and to conduct *ad hoc* audits of the Service Provider's compliance with this Addendum, to ensure that the Service Provider as Operator is fully compliant with the necessary POPIA, and contractual imperatives set out herein.

2.4.2 In addition to SARS' rights contemplated in the Services Agreement, SARS will be entitled to take any other reasonable monitoring measures to satisfy

itself that Personal Information, its employees, and stakeholders are not exposed to any risk of non-compliance with POPIA: Provided that any such measures will be implemented within the confines of Applicable Law, with prior notification to the Service Provider.

2.5 Data subject requests and third-party rights

- 2.5.1 The Service Provider must, at no additional cost to SARS, take such technical and organisational measures as may be appropriate, and promptly provide such information to SARS, as may reasonably be required, to enable SARS to comply with:
- (a) the rights of a data subject under POPIA; including, but not limited to, data subject access rights, the rights to rectify, port and erase Personal Information, object to the processing and automated processing of Personal Information, and restrict the processing of Personal Information; and
 - (b) any notice or request from a Regulatory Authority in relation to POPIA.
- 2.5.2 The Service Provider must promptly notify SARS in writing where it receives any complaint, notice or communication that relates directly or indirectly to the processing of Personal Information or to either Party's compliance with POPIA.
- 2.5.3 The Service Provider must notify SARS within twenty-four (24) hours where it receives a request from a data subject for access to their Personal Information or to exercise any of their other rights under POPIA.
- 2.5.4 The Service Provider must further provide, at no additional cost to SARS, its full co-operation and assistance in responding to any complaint, notice, communication or data subject request.

2.6 Indemnity

- 2.6.1 The Service Provider agrees to, at its own expense, indemnify, keep indemnified and defend SARS against all Losses incurred by SARS or for which SARS may become liable due to any failure by the Service Provider

or the Service Provider's Personnel, to comply with any of the Service Provider's obligations under this Addendum and/or POPIA.

- 2.6.2 Any limitation of liability set forth in the Services Agreement will not apply to this Addendum's indemnity or liability obligations.

DRAFT