PROTECTION OF PERSONAL INFORMATION SUBSEQUENT ASSESSMENT AND DUE DILIGENCE FOLLOW-UP REPORT

ANDERS TJ INC.

Registration number: 1997/006026/21

COMPANY PROFILE – GENERAL INFORMATION

COUNTRY OF INCORPORATION:	SOUTH AFRICA
NATURE OF BUSINESS AND PRINCIPAL ACTIVITIES:	COLLECTIONS, LITIGATION AND TRANSFER OF DEEDS
INCORPORATORS:	KGALALELO JACOBELLA KOMANE STEFANUS PETRUS VAN DER WALT THEUNETHA JOHANNA VAN DER WALT
REGISTERED OFFICE:	132 GARSFONTEIN ROAD ALPHEN PARK PRETORIA
NUMBER OF OFFICES/BRANCHES:	1
LOCATION OF OTHER BRANCHES:	NOT APPLICABLE
COMPANY REGISTRATION NUMBER:	1997/006026/21

TABLE OF CONTENTS

1 DEFINITIONS AND INTERPRETATION

1.1 In this **Report** and for ease of reference, terms used shall bear the same meaning as provided in the paragraphs below, unless a definition to the contrary appears herein:

1.1.1 **"Act"** means the Protection of Personal Information Act (Act No. 4 of 2013).

1.1.2 **"Assets"** include both information assets and physical assets.

1.1.3 **"Biometrics"** means a technique of personal identification that is based on physical, physiological, or behavioural characterization, including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

1.1.4 **"Child"** means a natural person under the age of 18 years who is not legally competent to take any action or decision in respect of any matter concerning him or herself without the assistance of a competent person.

1.1.5 **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information.

1.1.6 **"CPA"** means the Consumer Protection Act (Act No. 68 of 2008).

1.1.7 **"Cybercrimes Act"** means the Cybercrimes Act (Act No. 19 of 2020).

1.1.8 **"Data Subject"** means the person to whom Personal Information relates, including a third party.

1.1.9 **"Direct marketing"** means to approach a Data Subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

1.1.9.1 promotion or offering to supply in the ordinary course of business, any goods or services to the Data Subject; or

1.1.9.2 requesting the Data Subject to make a donation of any kind for any reason.

1.1.10 **"Electronic communication"** means any text, voice, sound or image message sent over an electronic communications network and which is stored in the network or into the recipient's terminal equipment until it is collected by the recipient.

1.1.11 **"Electronic Communications Transactions Act"** means the Electronic Communications and Transactions Act (Act No. 25 of 2002).

1.1.12 **"Evidence"** refers to all the information used to establish a fact in issue, including information supplied by the Company and used by the assessor determining the compliance level of the Company. Evidence includes the information contained in the filing, information and electronic communication systems and other information relating to the Company's internal compliance

processes obtained through enquiries, questionnaires, inspection of records or documents or written confirmations, physical or virtual on-site inspections and analytical procedures.

1.1.13 **"Filing system"** means any structured set of Personal Information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

1.1.14 **"Information Officer"** of, or in relation to, a –

1.1.14.1 public body, means an Information Officer or Deputy Information Officer as contemplated in terms of section 1 or 17; or

1.1.14.2 private body, means the head of a private body as contemplated in Section 1 of PAIA.

1.1.15 **"Information Regulator"** or **"Regulator"** means the Information Regulator established in terms of Section 39 of the Act.

1.1.16 **"Information System"** means the process of and tools for storing, managing, using and gathering of data and communication in an organization.

1.1.17 **"Operator"** means a person who processes Personal Information for a Responsible Party in terms of a contract or mandate, without falling under the direct authority of that party.

1.1.18 **"PAIA"** means Promotion of Access to information Act (Act No. 2 of 2000).

1.1.19 **"Personal information"** means information relating to an identifiable, living, natural person and, where applicable, an identifiable, existing juristic person, including, but not limited to –

1.1.19.1 information relating to the race gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

1.1.19.2 information relating to the education or the medical, financial, criminal or employment history of the person;

1.1.19.3 any identification number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

1.1.19.4 the biometric information of the person;

1.1.19.5 the personal opinions, views or preferences of the person;

1.1.19.6 correspondence sent by the person which is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

1.1.19.7 the views or opinions of another individual about the person; and

1.1.19.8 the name of the person if it appears with other Personal Information relating to the person or if the disclosure of the name itself would reveal information about the person.

1.1.20 **"POPI"** or **"POPIA"** shall mean the Protection of Personal Information Act (Act No. 4 of 2013) or **"the Act"**.

1.1.21 **"Processing"** means any operational activity or any set of operations, whether or not by automatic means, concerning Personal Information, including –

1.1.21.1 the collection, receipt recording, updating or modification, retrieval; or

1.1.21.2 dissemination by means of transmission, distribution or disclosure in any other form; or

1.1.21.3 merging, linking as well as restriction, erasure or destruction of information.

1.1.22 **"Record"** means any recorded information, regardless of form or medium, including written, electronics information, label, marketing image, film, graph, drawing or tape which is in the possession or under the control of the company, irrespective of whether it was created by the Company and regardless of when it came into existence.

1.1.23 **"Report"** means the initial Protection of Personal Information Assessment and Due Diligence Report, and "**Follow-up Report"** means the regular and annual follow-up reports thereafter.

1.1.24 **"Responsible Party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing Personal Information.

1.1.25 **"Special Personal Information"** means information relating to –

1.1.25.1 the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a Data Subject; or

1.1.25.2 the criminal behaviour of a Data Subject to the extent that such information relates to:

1.1.25.2.1 the alleged commission by a Data Subject of any offence; or

1.1.25.2.2 any proceedings in respect of any offence allegedly committed by a Data Subject, or the disposal of such proceedings.

1.1.26 **"System owner"** means the person who is the main contributor in developing system design specifications to ensure that the security and user operational needs are documented, tested and implemented.

1.1.27 **"The Company"** means **ANDERS TJ INC.** with registration number: 1997/006026/21;

1.1.28 **"The Responsible Party"** means the Company.

1.1.29 **"Third Party"** in relation to a request for access, means any person, excluding the Company or a personal requester.

2 INTRODUCTION

SERR Synergy has been engaged in 2021 to assess/audit and report on the Company's compliance and the risks associated with the processing of Personal Information of the Company. A Report based on the 2021 assessment presented to the Board of Directors of the Company. The Company is required by the Act (POPIA) to carry out an assessment/audit on a regular basis.

We will conduct our follow-up due diligence investigation/assessment/audit (these terms are mutually inclusive and used interchangeably in this Report) in accordance with accepted international auditing standards. Those standards require that we comply with various ethical requirements. As part of an audit in accordance with international best practices, we exercise independent and professional judgement throughout the initial as well as the follow-up audit.

This Follow-up Report is compiled in terms of section 19 of POPIA. The Company, as Responsible Party in terms of POPIA, is required to –

- identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Because of the inherent limitations of an audit, together with the inherent limitations of internal controls, there is an unavoidable risk that some material misstatements may not be detected, even though the initial audit as well as the follow-up audit are properly planned and performed in accordance with international best practices.

Due to the technical nature of the Company's information and technology (IT) and network systems, an initial and follow-up audits of these systems were not undertaken. However, should the Company at any time require a specific investigation for the purpose of providing affirmation with regard to the operation of any other aspect

of the Company's internal protection of Personal Information control structure, this could be undertaken at the Company's request.

3 STANDARDS OF ETHICAL CONDUCT AND REQUIREMENTS

In order to obtain and maintain confidence, the assessor has to be able to demonstrate that his/her decisions are based on objective evidence and that his/her decisions have not been improperly influenced by other interests or by other parties. Principles for inspiring confidence are contained in the initial Report and apply in all aspects to this Follow-up Report as well.

3.1 **Assessment Methodology**

3.1.1 Apart from technical IT systems and network operations, the assessor has verified, validated and evaluated all information concerning the processing of Personal Information of the Company provided to the assessor based on the principles set out in POPIA and PAIA, including all the conditions provided for the POPIA for the lawful processing of Personal Information. All assessments are to be based on information submitted by the Company to the assessor.

3.1.2 The assessor has inspected and, where reasonably possible, assessed the information provided in order to assess the level of POPIA compliance and risks associated with the Company.

3.2 **Due Diligence**

3.2.1 The assessor has performed an assessment with an attitude of recognising all information provided by the Company, on face value. An attitude of professional scepticism was not applied as the assessment was not a critical assessment of the validity of evidence provided.

3.2.2 The assessor compared the information presented by the Company to ensure that there are no inconsistencies in the various pieces of documents and information and, if any, that such inconsistencies are properly addressed.

4 RECOMMENDED REMEDIAL INTERVENTIONS

Based on the non-compliance or partial compliant activities and associated risks identified above, the following interventions as recommended:

4.1 **In respect of the processing of Personal Information in general**

4.1.1 To adopt a **Protection of Personal Information Policy (Privacy Policy)** to deal with all aspects of processing of Personal Information, such as restricting processing when accuracy is contested by Data Subject, when a Data Subject opposes the restriction and to provide for a process to inform the Information Regulator and compromised Data Subject of any breach of Personal Information data.

4.1.2 To ensure that the safeguards are continually updated in terms of section 19(2)(*d*) of POPIA in response to new risks by conducting an **annual assessment**.

4.2 **In respect of access to information**

4.2.1 To **update** the manual at least once a year.

4.3 **In respect of the processing of information of Employees and the role of Employees in protecting Personal Information of the Company and other Data Subjects such as Clients and Customers**:

4.3.1 To enroll on regular basis, but at least once a year, **training programmes** to upskill staff on the legal requirements to lawfully process Personal Information.

4.4 **In respect of Physical Environmental Security**

4.4.1 Obtain an assessment from security experts to ensure access control and safety measures of the business premises in general.

4.5 **In respect of Hardware Security and Hardcopies**

4.5.1 Consider installing tracker systems on all electronic devices, especially those taken off the business premises.

4.5.2 Obtain an assessment report from an IT expert on the technical safety measures in place and to be put in place in respect of data protection and network safeguards.

Follow-up Report compiled by Assessor: **Retha van Zyl, SERR Synergy (Pty) Ltd**

Date: 22 November 2022