OTASA DATA PROTECTION POLICY

1. INTRODUCTION AND PURPOSE

OTASA is committed to processing personal data in accordance with its responsibilities under the Protection of Personal Information Act (POPIA) and may be subject to similar information protection dispensations in other jurisdictions. These data protection laws impose strict guidelines to secure employees and members right to privacy with regard to their personal information.

The Organisation is committed to protecting and safeguarding all personal information in its possession or under its control and to take appropriate and reasonable measures (technological as well as organisational) to ensure the integrity and confidentiality thereof in respect of all its business activities in accordance with the law as well as ongoing risk assessments.

This Data Protection Policy is intended to:

- Ensure that OTASA complies with legal standards for the receipt, processing and storing of personal data of individuals and legal entities and to explain how this should be achieved
- Ensure that OTASA protects the rights of data subjects in respect of the privacy of personal information
- Ensure that OTASA provides a transparent system of personal information protection
- Protects OTASA against the risks and consequences of data breaches.

2. DEFINITIONS

Organisation	OTASA registered under number NPO 001-035
Information Officer	Prof Pat de Witt Deputy Information Officer: Tiana Ferreira
Data Subject	the person (individual or legal entity) to whom the data relates
Responsible party	the person/entity (either alone or jointly with others) who determines the purpose and manner in which personal information of a data subject is to be processed
Operator	a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
Personal information *	information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

*For the purpose of this policy, reference to 'personal information' shall include 'special personal information' as described hereunder	(a) 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; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) 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,
Special personal information	Means - (a) 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 (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Processing	Means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information.
De-identify	Means to delete any information that: identifies, or can be used/manipulated to identify, the data subject; or that can be linked to other information that identifies the data subject by a reasonably foreseeable method.

3. SCOPE

3.1. This policy applies to all personal information processed by the Organisation – whether by employees or by third-party Operators on its behalf. It will also apply to ancillary workers such as contractors, consultants, freelancers, etc. who may from time to time provide services to the Organisation and be exposed to personal information in its possession or under its control.

3.2. The Information Officer will be registered with the office of the Information Regulator and shall take responsibility for the Organisation's ongoing compliance with this policy.

3.3. This policy shall be reviewed at least annually.

4. THE RIGHTS OF DATA SUBJECTS

4.1. Data subjects have the right to know what personal information is held by the Organisation and for what purpose(s) it is processed.

4.2. The Organisation may in certain circumstances be legally obliged to disclose personal information to law enforcement or similar institutions, without the consent of the data subject. This will however only be done after verifying that the request is lawful and legitimate. Only the Information Officer will be authorised to furnish such information.

4.3. Data subjects may lodge a complaint with the Information Regulator it they are concerned about the security of their personal information or its processing by the Organisation. Data subjects are however encouraged to first contact the Deputy Information Officer to report their concerns to the organisation directly, to otofficefin@otoffice.co.za

5. LAWFUL, JUSTIFIED AND TRANSPARENT DATA PROCESSING

5.1. The organisation's legitimate business interests must always be balanced against the data subject's privacy rights. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal information. If an individual revokes their consent, this should be communicated to the Deputy Information Officer at otofficefin@otoffice.co.za

5.2. The lawful processing of personal information must also be done in accordance with five specific processing conditions:

- Accountability
  All employees (and Operators) shall continually be responsible for ensuring the safeguarding, protection and avoidance of any unauthorised disclosure or breach of personal information in the execution of employment duties and services to the Organisation, or otherwise in the course of rendering services or being associated with the Organisation.
  IT is responsible to ensure that all systems, services and equipment used for processing and/or storing data adhere to internationally acceptable standards of security and data safeguarding, and is regularly updated to continue to comply with such standards.

- Purpose Specification

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a legitimate function / activity of the Organisation and this purpose should generally be disclosed to the data subject.

- Further processing limitation

  Personal information that has been collected for a specific purpose, may not be processed further unless it is for a reason compatible to the original purpose, or if the data subject consent, or if specific circumstances exist that permit such further processing in terms of the law.

- Information quality

  The Organisation must take reasonable steps to ensure that the personal information processed by it is complete, accurate, not misleading and updated where necessary.

- Openness / Transparency

  Whenever the Organisation collects personal information (except if one or more of the exclusions in s18 of POPIA apply), it must take reasonable steps to notify the data subject of certain details relating to the processing of this information. The Organisation will also ensure that any third-party Operators that process personal information on its behalf, subscribe to and comply with the same level of security and that these obligations are set out in a mandatory written agreement with each Operator.

Account numbers

Failure by the organisation to appropriately protect account numbers of data subjects, could constitute a criminal offence if it ought to have known / foreseen risks in this regard, but failed to take reasonable steps to address those risks. Someone who knowingly or recklessly obtains, discloses or procures the disclosure of an account number in an unauthorised manner, or who sells such a number, may also be guilty of a criminal offence.

6. TRANSFERRING PERSONAL INFORMATION TO A COUNTRY OUTSIDE OF SOUTH AFRICA

The organisation will as far as possible ensure that the transfer of personal information to a recipient in a foreign country only takes place if there are adequate / similar levels of data protection in place – either by way of laws applicable to that country, or in terms of Binding Corporate Rules or a binding Transborder data processing agreement.

The data subject may however nevertheless consent to the cross-border transfer of their personal information; or such a transfer may take place if it is necessary in connection with a contract between the organisation and the data subject, or a contract concluded in the data subject's interest or to their benefit.

The cross-border transfer of special personal information or personal information relating to children, may however be subject to prior authorisation from the Information Regulator if the foreign country does not provide an adequate level of protection as required in terms of POPIA.

7. DATA BREACHES / SECURITY COMPROMISES

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Organisation must notify the Regulator; and the affected data subject(s) (unless the identity of such data subject cannot be established or it will impede a criminal investigation).

The Incident Response Plan includes a form that an employee or an Operator must complete whenever a security compromise is found or suspected, as well as specific reporting protocols. Operators may not make reports to data subjects or the Regulator directly, but must report to the Organisation as the responsible party. Employees, Operators and the like should not attempt to investigate such matters themselves, but should immediately contact the Information Officer or delegated person and preserve all evidence relating to the potential security compromise or data breach. The Information Officer is responsible to ensure that all relevant employees and Operators are made aware of the contents of the Incident Response Plan.

8. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

The organisation is committed to making data protection and privacy of data subjects a priority in all aspects of its business activities. To this end, the organisation's privacy strategy provides for continuous privacy- and data protection impact assessments as may be appropriate and for privacy considerations to form part of the development and implementation of all new projects, tools, programmes, equipment, etc.

9. IMPLEMENTATION OF POLICY IN RESPECT OF EMPLOYEES

This data protection policy governs every employee of the Organisation during the course of his/her services to it, and to the extent applicable, after termination of employment. It is the responsibility of every employee to familiarise him/herself with the content of this policy, and to remain up to date as to any changes to it issued by the Organisation.

To the extent that this policy sets out workplace rules and standards governing the employee in the course of his/her work and services to the company, these shall form part of the company's Disciplinary Code and Procedure and is hereby also incorporated into it.

A breach of any rule in relation to the protection of personal data set out in this policy that constitutes misconduct, shall be subject to disciplinary action and may lead to dismissal in appropriate circumstances.

The imposition of any disciplinary sanction or dismissal shall not preclude the Organisation from instituting civil proceedings against an employee who acted in breach of this policy where such breach has resulted in liability, loss, reputational damage and/or other damages to the Organisation in the course of pursuing its commercial operations.