PROTECTION OF PERSONAL INFORMATION

MANAGEMENT POLICY

of

ATOSSA FINANCIAL SERVICES (PTY) LTD

FSP 52305

Contents

1. INTRODUCTION

Data and personal information security laws mandate that organisations implement adequate safeguards to ensure the protection of company and personal information. As an authorised Financial Services Provider (FSP) and Accountable Institution (AI), data security is the biggest driver of Atossa Financial Services (Pty) Ltd IT processes. There are many regulations to consider such as Protection of Personal Information Act 2013 (POPI Act No.4 of 2013),Consumer Protection Act 68 of 2008 (CPA) and King IV, and each is considered in conjunction with each other to ensure adherence to the full set of obligations imposed on the FSP by these regulatory and governance guidelines.

The King IV Code requires that all governing bodies must ensure that their organisations are protecting the privacy of personal information. It requires disclosure of the status of lawful processing of personal information in the annual integrated reports.

The Protection of Personal Information Act ("**PoPIA**") regulates how companies handle, keep and secure personal information. With the appointment of the Information Regulator and the subsequent formalisation of the legislation, companies urgently need to enhance (or if necessary, upgrade) their information technology security systems.

The development of a standard operating procedure to ensure adequate protection of personal client information which becomes available to Atossa Financial Services (Pty) Ltd, and its personnel is of utmost importance for the effective operations and risk management practices of the company. Moreover, internal control mechanisms to constantly review and measure adherence to procedures and processes are important risk management tools and assist the company in treating its clients fairly. The absence of a personal information risk management plan will expose the company to unnecessary risk and create a burden in respect of financial and other regulatory requirements.

Atossa Financial Service (Pty) Ltd subscribes to the principles expressed in the Protection of Personal Information Act and the Constitution of South Africa in respect of:

- The lawful processing of client data by Atossa Financial Services (Pty) Ltd acting as a responsible corporate citizen; and
- The identification and allocation of accountability, where personal data is processed contrary to the prescripts of the Act.

Atossa Financial Service (Pty) Ltd has developed the following policies in response to its internal data governance responsibilities:

- This Personal Information Management Policy
- Cyber Security Policy
- Promotion of Access to Information Manual
- Incident Management Policy
- Record Keeping Policy & Procedure

2. OBJECTIVES

This personal information management policy ensures that Atossa Financial Services (Pty) Ltd:

- Complies with data protection regulation and follows good practice;
- Protects the rights of staff, customers as well as partners; ✞ Is open about how it stores and processes clients' data; ✞ Protects itself from the risks of data breaches.

3. SCOPE

This personal information management policy applies to all personal information held by the company relating to identifiable individuals, even if that information technically falls outside of the Protection of Information Act. This can include but not be limited to:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Remuneration;
- Race and Gender;
- Information external to the immediately knowledge of an employer; ✞ Any other information relating to individuals.

It is understood that personal information may also include sensitive personal information, and thus the compliance acknowledges the need for increased scrutiny of its safety, protection and security measures.

4. DEFINITIONS

*"***Act"** means **the Protection of Personal Information Act No.4 of 2013;**

"Data subject" means the person to whom personal information relates;

"consent" means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information;

"data subject" means the person to whom personal information relates;

"**de-identify",** in relation to personal information of a data subject, means to delete any information that –

(a) Identifies the data subject;
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject,

"direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

(a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
(b) Requesting the data subject to make a donation of any kind for any reason;

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

"enforcement notice" means any notice issued in terms of section 95 of the Protection of Personal Information Act No. 4 of 2013;

"filling system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subjects;

"information officer" of, or in relation to, a –

(a) Public body means an information office or deputy information officer as contemplated in terms of section 1 or 1; or
(b) Private body means the head of a private body as contemplated in section 1 of the Promotion of Access to information Act;

"Minister" means the Cabinet member responsible for the administration of justice;

"operator" means 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;

"person" means a natural person or a juristic person;

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

i. 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;

ii. Information relating to the education or the medical, financial, criminal or employment history of the person;
iii. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
iv. The biometric information of the person;
v. The personal opinions, views or preferences of the person;
vi. 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;
vii. The views or opinions of another individual about the person; and
viii. 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;

"prescribed" means prescribed by regulation or by a code of conduct;

"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;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information –

(a) Regardless of form or medium, including any of the following:
- Writing on any material;
- Information produced, recorded, or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- Label, marking or other writing that identifies or describes anything or to which it is attached by any means;
- Book, map, plan, graph, or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable , with or without the aid of some other equipment, of being reproduced;

(b) In the possession or under the control of a responsible party;
(c) Whether or not it was created by a responsible party; and

(d) Regardless of when it came into existence;

"Regulator" means Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that – (a) Identifies the data subject;
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) Can be liked by a reasonably foreseeable method to other information that identifies the date subject;

"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;

5. PERSONAL INFORMATION RISK MANAGEMENT ROLES AND RESPONSIBILITIES

Everyone who works for or with Atossa Financial Services (Pty) Ltd has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal information must ensure that it is handled processed in line this policy and data protection principles.

However, these people have key areas of responsibility:

- **Top management** is ultimately responsible for ensuring that Atossa Financial Services (Pty) Ltd meets its legal obligations.

- **The information officer** is responsible for:
    - Keeping the board update about data protection responsibilities, risks, and issues; ○ Reviewing all personal information protection procedures and related policies, in line with an agreed schedule;
    - Arranging data protection training and advice for the parties covered in this framework;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Dealing with requests from individuals to see the data Atossa Financial Services (Pty) Ltd holds about them;
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- **The IT manager,** is responsible for:
    - Ensuring all systems, services and equipment used for storing personal information meet acceptable security standards;
    - Performing regular checks and scans to ensure security hardware and software is functioning properly;
    - Evaluating any third-party services the company is considering using to store or process personal information. For instance, cloud computing services;
    - Either performing or obtaining third party assessments to gauge the level of the company's security of personal information and identify and improve any areas of weakness.

- **The marketing manager**, is responsible for:
    - Approving any personal information protection statements attached to communications such as emails and letters;
    - Addressing any personal information protection queries from journalists or media outlets like newspapers;
    - Where necessary, working with other staff to ensure marketing initiatives abide by personal information protection principles.

- **All employees**, are responsible to:
    - Understand and comply with this policy.
    - Create a full and accurate record of activities, transactions and decisions carried out during the course of business activities.
    - Ensure confidential or sensitive information is protected from unauthorised access.

- Keep information on Atossa Financial Services (Pty) Ltd premises to avoid security and privacy breaches. ○ Follow the protection of personal information requirements at all time to ensure compliance with statute.
- Safeguard and protect personal information so it is retained for as long as it is needed for business, legal and accountability requirements.

6. PROTECTION OF PERSONAL INFORMATION

The Protection of Personal Information Act No.4 of 2013 describes how organisations including Atossa Financial Services (Pty) Ltd must collect, handle and store as well as discard personal information.

The rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with regulatory requirements, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

This policy is underpinned by eight important principles. The principles state that data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects or competent persons if the data subject is a child;
7. Be protected in appropriate ways;
8. Not be transferred outside the borders of South Africa unless that country or territory also ensures an adequate level of protection.

Atossa Financial Services (Pty) Ltd has adopted the **Data Classification methodology** outlined in **Annexure 1** of this Policy.

7. THE PERSONAL INFORMATION RISK MANAGEMENT PROCESS

7.1. Data Protection Risk Identification, Analysis, Assessment and Prioritisation

This policy helps to protect Atossa Financial Services (Pty) Ltd from data security risks. When assessing risk, both inherent and residual risk is considered. Inherent risk considers the "worst case scenario" whilst residual risk measures the current level of risk considering the adequacy and effectiveness of controls and measures already in place thus understanding any remaining risk to which the organisation may be exposed.

Assessment of inherent risk assists in:

- Understanding of exposure level in the event of a significant control failure;
- Identifying key controls and considering their effectiveness;
- Understanding the relationship between risks and their associated responses and controls;
- Developing effective key risk indicators and controls.

Residual risk is essential to determining the organisation's current levels of risk and shall always be used. Determining the residual risk requires, as a pre-requisite, considering existing measures and controls that have already been implemented and assessing/ estimating the adequacy and effectiveness thereof.

7.2. Data Protection Control Measures

- The only people able to access data covered by this policy shall be those who need it for their work in relation to and on behalf of the FSP as contracted to do so;
- Data shall not be shared informally. When access to confidential information is required, employees may request it from their line managers;
- Atossa Financial Services (Pty) Ltd will provide training to all employees to help them understand their responsibilities when handling data;
- Employees shall keep all data secure, by taking sensible precautions and following the guidelines below;

- In particular, strong passwords must be used and they shall never be shared. Password updates shall become routine in the organisation;

- Personal information shall not be disclosed to unauthorised people, either within the company or externally;
- Data shall be regularly reviewed and updated if it is found to be out of date. If no longer required, it shall be deleted and permanently disposed of; unless is it required in the confines of the law to be maintained for a fixed period of time, in which case the FSP shall store such information safely and restricted access rights align with lawful parameters;
- Employees shall request help from their line manager or the Information Officer if they are unsure about any aspect of data protection;
- In the event of a breach of security regarding data the Information Officer shall notify the Information Regulator and the affected data subjects (or competent person as the case may be) as soon as reasonably possible, by such means and media as are appropriate in the circumstances to enable them to take steps to protect their interests;
- Atossa Financial Services (Pty) Ltd shall ensure, when requested to transfer data across the borders of South Africa, that this is so done only with the consent of the data subject and

thereafter only to a jurisdiction which has rules on the protection of data substantially similar to those contained in this policy and the Protection of Personal Information Act.

- Information regarding a data subject in respect of the following shall not be processed unless the data subject has authorised such processing or unless otherwise required by law:
    - the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information;
    - the criminal behaviour of a data subject to the extent that such information relates to-
        - the alleged commission by a data subject of any offence; or
        - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- Atossa Financial Services (Pty) Ltd shall not process data regarding children unless authorised by such children's guardian or otherwise as required by law.

7.3. Data Use Code of Conduct

Personal data is of no value to Atossa Financial Services (Pty) Ltd unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees shall ensure the screens of their computers are always locked when left unattended;
- Personal data shall not be shared informally;
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts;
- Employees shall not save copies of personal data to their own computers. Always access and update the central copy of any data.

7.4. Data Accuracy

Atossa Financial Services (Pty) Ltd has the responsibility to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Atossa Financial Services (Pty) Ltd shall put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff shall not create any unnecessary additional data sets;

- Staff shall take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call;
- Atossa Financial Services (Pty) Ltd will make it easy for data subjects to update the information which the FSP holds about them. For instance, via the company website, or annual update through means of a personal contact details update form;
- Data shall be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it shall be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

7.5. Subject access requests

All individuals who are the subject of personal data held by Atossa Financial Services (Pty) Ltd are entitled to:

- Ask what information the company holds about them and why;
- Ask how to gain access to it;
- Be informed how to keep it up to date;
- Be informed how the company is meeting is data protection obligations.

If an individual contacts the company requesting this information, this is called "Data Subject Access Request".

Data Subject Access Requests from individuals shall be made by email, addressed to the data controller at data@atossacapital.com and **cc:** help@atossacapital.com. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will aim to provide the relevant data within (5 business) days.

The data controller will always verify the identity of anyone making a Data Subject Access Request before handing over any information.

7.6. Disclosing data for other reasons

In certain circumstances, the Protection of Personal Information Act and other legislation which Atossa Financial Services (Pty) Ltd is subject to allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Atossa Financial Services (Pty) Ltd will disclose requested data. However, the data controller will endure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

7.7. Providing information

Atossa Financial Services (Pty) Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used;
- How to exercise their rights.

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

7.8. Incident Management

Atossa Financial Services (Pty) Ltd aims to ensure no unauthorised use or access to the personal information of a data subject. However, in the event there is a breach or compromise the "responsible party" i.e. Atossa Financial Services (Pty) Ltd shall ensure the following:

- Notify the Information Regulator of the breach;
- Notify the data subjects who have been the subjects of the breach within 72 hours of the breach having occurred;
- Investigate the nature of the breach and the causal reasons as to why the breach has occurred;
- Determine the necessary action(s) that may be necessary to remedy the breach having occurred, and or internal processes and procedures that may have led to contributing to the breach having occurred;
- Capture the breach on the privacy risk register;
- Respond to complaints from data subjects who may be seeking compensation as a result of the unauthorise leaking of or access to their personal information;
- Restore the integrity of systems, processes and procedures through appropriate action to avoid a recurrence of a future breach or compromise of the personal information of data subjects.

8. REVIEW OF POLICY

The contents of the policy will be reviewed by top management together with the Information Officer on an annual basis. Compliance with this policy shall be reviewed annually and reported on by the Information Officer, to the Board.

9. OWNERSHIP AND ACCOUNTABILITY

This **Protection of Personal Information Management Policy** is owned by Atossa Financial Services (Pty) Ltd, a duly registered company under the Companies Act, 2010, authorised Financial Services Provider and Accountable Institution.

As a member of the organisation's top management, I confirm that this policy is hereby adopted and commit to its successful implementation.

Full Name of Director:

Signature: _____ Date: _____

Full Name of Director:

Signature: _____ Date: _____