
POPI: INFORMATION PROCESSING POLICY

FIRST IMPLEMENTATION DATE: 01/07/2021

LAST REVISION DATE: N/A

1. Introduction

The Protection of Personal Information Act (POPI) is South Africa's Privacy law and introduces requirements for the processing of Personal Information. The Protection of Personal Information Act (POPIA) gives effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations.

Section 2 of the Act lists the purposes of the Act. Amongst other the Act aims to protect important interests, including the free flow of information within the Republic and across international borders and to regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.

2. Scope and Application

The aim of the Information and record retention and disposal policy is to establish a framework and set out the guiding principles and the efforts of the Gradidge Mahura Group which includes:-

- Gradidge Mahura Investments (GMI)
- Gradidge Mahura Asset Protection (GMAP)
- Gradidge Mahura Asset Management (GMAM)
- Gradidge Mahura Fiduciary Services (GFS)

on the collection, storage, processing and destruction of Personal Information.

The policy is applicable to all employees of the Gradidge Mahura Group and staff members shall receive training with regards to the Protection of personal information policy. Failure to adhere to the policy will result in disciplinary action.

This Policy is aimed at documenting the Gradidge Mahura Group's position on the processing of Information related to any person as described under POPI. The Policy includes the Gradidge Mahura Group's position on:

- The collection of personal information
- The recording and storage of personal information
- The filing, collation, merging and organisation of personal information
- The updating or modification of personal information
- The transmission, distribution or other dissemination of information, and
- The restriction, degradation, erasure or destruction of information

The Policy applies to the processing of personal information entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.

This document should be read with the Gradidge Mahura Group's Information processing plan for detail on implementation of the policy objectives.

3. Definitions

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013	
Term	Definition
Consent	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
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 25 identifies the data subject, and “de-identified” has a corresponding meaning;
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;
Filing 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 subject;
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;
PAIA	Means the Promotion of Access to Information Act, 2 of 2000
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— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health,

	<p>well-being, disability, religion, conscience, belief, culture, language and birth of the person;</p> <p>(b) information relating to the education or the medical, financial, criminal or employment history of the person;</p> <p>(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;</p> <p>(d) the biometric information of the person;</p> <p>(e) the personal opinions, views or preferences of the person;</p> <p>(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;</p> <p>(g) the views or opinions of another individual about the person; and</p> <p>(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;</p>
Processing	<p>means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—</p> <p>(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;</p> <p>(b) dissemination by means of transmission, distribution or making available in any other form; or</p> <p>(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;</p>
Record	<p>means any recorded information—</p> <p>(a) regardless of form or medium, including any of the following:</p> <p>(i) Writing on any material;</p> <p>(ii) 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;</p> <p>(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;</p> <p>(iv) book, map, plan, graph or drawing;</p> <p>(v) 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;</p> <p>(b) in the possession or under the control of a responsible party;</p> <p>(c) whether or not it was created by a responsible party; and</p> <p>(d) regardless of when it came into existence;</p>

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 linked by a reasonably foreseeable method to other information that identifies the data subject, and “re-identified” has a corresponding meaning;
Restriction	means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;
Special Personal Information	means personal information as referred to in section 26 of the Act, which includes: <ul style="list-style-type: none"> ● 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 ● the criminal behaviour of a data subject to the extent that such information relates to— <ul style="list-style-type: none"> ○ the alleged commission by a data subject of any offence ○ any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Unique Identifier	means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

4. Guiding principles for the lawful processing of personal information

The Gradidge Mahura Group is committed to processing data in accordance with its responsibilities under the Protection of Personal Information Act.

Personal information must be processed—

- lawfully
- in a reasonable manner that does not infringe the privacy of the data subject
- Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.
- Personal information may only be processed if
 - the data subject or a competent person where the data subject is a child consents to the processing
 - processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party
 - processing complies with an obligation imposed by law on the responsible party
 - processing protects a legitimate interest of the data subject
 - processing is necessary for the proper performance of a public law duty by a public body

- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

The conditions for the lawful processing of personal information by or for a responsible party are the following:

- "Accountability, as referred to in Section 8
- "Processing limitation", as referred to in sections 9 to 12
- "Purpose specification", as referred to in sections 13 and 14;
- "Further processing limitation", as referred to in section 15
- "Information quality" as referred to in section 16
- "Openness" as referred to in sections 17 and 18
- "Security safeguards" as referred to in sections 19 to 22
- "Data subject participation" as referred to in sections 23 to 25

The Gradidge Mahura Group and its employees will act in accordance with the following principles or conditions:

4.1. Accountability

The Gradidge Mahura Group is obligated to ensure compliance with the conditions for lawful processing of information, as provided for in terms of the POPI Act, and the measures that the Gradidge Mahura Group implement to give effect to the conditions throughout its engagement with its clients, employees and other stakeholders.

This policy shall set the principles for the personal information framework which shall include various measures, procedures and controls to ensure that all personal information processed by the Gradidge Mahura Group is protected. The Gradidge Mahura Group shall establish a function which shall be responsible for encouraging and ensuring compliance with the POPI Act and the Gradidge Mahura Group's personal information risk management and compliance framework.

The Gradidge Mahura Group has further implemented a Privacy Policy that speaks to the organisation.

4.2. Processing limitation

The Gradidge Mahura Group shall process personal information in a lawful and fair manner. The Gradidge Mahura Group shall process information for a specific reason and only adequate, relevant information which is limited to the purposes for which they are processed. Furthermore, information under the Gradidge Mahura Group's control shall only be processed with the informed consent of the data subject or for legitimate and justifiable reasons as provided for in the POPI Act.

The Gradidge Mahura Group shall inform its data subjects for the purpose or reasons for the collection of personal information and shall obtain written consent from the data subject. Information shall be obtained directly from the data subject unless the data subject has consented to the collection of personal information from another party or if the Gradidge Mahura Group can demonstrate a justifiable reason for collecting information from another source as provided for in the POPI Act.

The data subject has the right to withdraw consent or object to the processing of personal information and is required to do so in the prescribed manner.

The Gradidge Mahura Group shall further take special care to limit processing in respect of special information and shall in all such cases aim to comply with the conditions of Part B of the POPI Act.

4.3. Purpose specification

The Gradidge Mahura Group shall collect personal information for a specific, explicitly defined and lawful purpose which relates to the function or the activity of our organisation. The Gradidge Mahura Group shall endeavour to ensure that the data subject is aware of the purpose for the collection of information to enable the data subject to make an informed decision on whether or not to disclose the personal information to our organisation.

The Gradidge Mahura Group may not retain personal information any longer than necessary for achieving the purpose for which we have collected or processed the information unless:

- We are required by law to retain information for a longer period;
- Retention is required for lawful purposes related to our functions or activities;
- Retention is required in terms of a contract between the data subject and the Gradidge Mahura Group;
- In the case of a child's personal information, a competent person has consented to the retention of the records.

Once the personal information has been retained for the period of time mentioned above, the POPI Act requires that Gradidge Mahura Investments (Pty) Ltd:

- Destroy or delete the record; or
- De-identify personal data to such an extent that it cannot be reconstructed in a clear form.

In circumstances where the Gradidge Mahura Group is required to restrict the processing of personal data as prescribed by the POPI Act we shall only process information for the following purposes and before lifting the restriction inform the data subsequently:

- For storage purposes;
- For purposes of proof;
- With the consent of the data subject;
- For the protection of another person's rights; or
- If such processing is in the public interest.

4.4. Further processing limitation

If the Gradidge Mahura Group wants to process the personal information further or for additional purposes, it must be compatible or in line with the purpose for which it was collected.

To determine whether further processing is in accordance with the purpose for which it was initially collected the Gradidge Mahura Group shall consider the following:

- The relationship between the purpose for which it wants to further process the information and the purpose for which the information was collected;
- The nature of the information;
- What are the consequences of further processing of information for the data subject;
- The manner of how the information was collected; and
- Our contractual obligations.

Thus if the Gradidge Mahura Group wants to process the information it holds further and the purpose is not compatible with the original purpose, the Gradidge Mahura Group shall be required to obtain consent from the data subject or demonstrate a justifiable reason as provided for in the POPI Act for further processing personal information.

4.5. Information quality

The Gradidge Mahura Group will take reasonably practicable steps to ensure that the personal information obtained from our data subjects or third parties is complete, accurate, not misleading and updated where necessary.

As an organisation, we understand that personal information is sensitive and we have implemented reasonable measures to ensure that personal data is not modified or misused by an unauthorized person.

4.6. Openness

The Gradidge Mahura Group is required to maintain documentation of all processing operations under its responsibility as referred to in terms of the Promotion of Access to Information Act.

The Gradidge Mahura Group will take reasonable steps to ensure that the data subject knows that personal information about him or her is being collected; the source from which this is collected; and the purpose for which information is collected before collecting information, including the information below:

- The name and address of the responsible party;
- Whether the information provided is mandatory or voluntary;
- Consequences of failure to provide the information;
- A law authorising or requiring the collection of information;
- If applicable, whether the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded;
- Recipients of the information;
- Nature and category of the information;
- The data subject's right of access and the right to rectify the information collected;
- The data subject's right to object to the processing of personal information;
- The right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.

4.7. Security safeguards

The Gradidge Mahura Group has the responsibility to secure the integrity and confidentiality of personal information in its possession or under its control and the Gradidge Mahura Group shall take reasonable and appropriate technical and organisational measures to prevent the loss, damage unauthorized destruction of personal information and unlawful access to or processing of personal information.

The Gradidge Mahura Group shall identify all reasonably foreseeable internal and external risk to personal data under its control and establish safeguards against those risks. The Gradidge Mahura Group will review its control measures and its effectiveness and update the safeguards in response to new risks of deficiencies in safeguards.

In the unfortunate event that the safeguards implemented were breached or in the event that the Gradidge Mahura Group has reasonable grounds to believe that the personal information has been accessed or acquired by an unauthorised person, the Gradidge Mahura Group will be required to notify the Information Regulator and the data subject as soon as reasonably possible after the discovery was made.

More detailed information in respect of Security safeguards are detailed in the Information Processing Plan.

4.8. Data subject participation

A data subject has the right to request from the Gradidge Mahura Group whether it holds personal information about the data subject and the Gradidge Mahura Group shall provide confirmation free of charge. A data subject may further request records of personal information. The Gradidge Mahura Group must first establish the identity of the data subject before disclosing the information and must respond to such a request within a reasonable time period and in a form that is generally understandable.

If there are grounds for refusal of access to records set out in PAIA, the Gradidge Mahura Group may refuse access to the information, but information that does not fall within the ambit of the exclusion in terms of PAIA must be disclosed. The Gradidge Mahura Group shall provide the data subject with reasons for refusing to provide access to information.

A data subject may request the Gradidge Mahura Group to correct or delete personal information under the control or in possession of the Gradidge Mahura Group if:

- The personal information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
- Delete a record or personal information about the data subject which the responsible party is no longer authorised to store or retain.

4.8.1. Data subject information requests

The Gradidge Mahura Group has implemented a POPI information request policy and procedure in terms of which a data subject may make a request for information from them. Such document is available on request.

4.8.2. Handling of data subject complaints

The Gradidge Mahura Group has implemented a Complaints resolution policy and procedure which is available on request.

5. Processing of Special Personal Information

The Gradidge Mahura Group shall not process personal information concerning—

- 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
- the criminal behavior of a data subject to the extent that such information relates to—
 - the alleged commission by a data subject of any offence
 - any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

unless the—

- processing is carried out with the consent of a data subject
- processing is necessary for the establishment, exercise or defence of a right or obligation in law
- processing is necessary to comply with an obligation of international public law
- processing is for historical, statistical or research purposes to the extent that—
- the purpose serves a public interest and the processing is necessary for the purpose concerned
- it appears to be impossible or would involve a disproportionate effort to ask for consent
- and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent
- information has deliberately been made public by the data subject

5.1. Authorisation concerning data subject's religious or philosophical beliefs

A data subjects religious or philosophical may not be processed unless the processing is carried out by:

- spiritual or religious organisations, or independent sections of those organisations if the information concerns data subjects belonging to those organisations or if it is necessary to achieve their aims and principles;
- institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or
- other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subjects unless they have indicated that they object to the processing.

Spiritual or religious organisations may also process personal information concerning the religion or philosophy of life of family members of the data subjects if it maintains regular contact with those family members in connection with its aims and the family members have not objected.

Under no circumstances may personal information be supplied to a third party without the consent of the data subject.

5.2. Authorisation concerning data subject's race or ethnic origin

A responsible party may process information about a data subject's race or ethnic origin if the processing of the information is carried out to:

- To identify the data subject when it is essential for that purpose;
- Comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

5.3. Authorisation concerning data subject's trade union membership

It is not prohibited to process information of the data subject's trade union membership if the information processing is done by the trade union to which the data subject belongs or the trade union federation to which the trade union belongs and if the processing is necessary to achieve the aims of the trade union or trade union federation.

The trade union or trade union federation may not without the consent of the data subject supply personal information to third parties.

5.4. Authorisation concerning data subject's political persuasion

Processing of personal information by or for an institution founded on political principles are allowed of:

- its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or
- a data subject if such processing is necessary for the purposes of—
 - forming a political party;
 - participating in the activities of or engaging in the recruitment of members for or canvassing supporters or voters for, a political party with the view to National or municipal elections, referendum or campaigning for a political party or cause.

No personal information may be supplied to third parties without the consent of the data subject

5.5. Authorisation concerning data subject's health or sex life

In general personal information of a data subject, health or sex life may not be processed. However, Section 32 of the POPI Act provides authorisation for the following persons:

- **Medical professionals, healthcare institutions or facilities or social services:**
If such processing of personal information about a data subjects health or sex life is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned.
- **Insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations:**
If the processing of the personal information by the aforementioned bodies is necessary for:
 - assessing the insured risk by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;
 - the performance of an insurance or medical scheme agreement; or
 - the enforcement of any contractual rights and obligations;
- **Schools**
If such processing of personal information is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life.
- **Public or private body managing the care of a child**
If such processing is necessary for the performance of their lawful duties;
- **Public body**
If such processing is necessary in connection with the implementation of prison sentences or detention measures
- **Administrative bodies, pension funds, employers or institutions working for them,**
If such processing is necessary for the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject or the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

The responsible parties may only process the information subject to an obligation of confidentiality whether by virtue of office, employment, the profession of a legal provision or in terms of a written agreement, even if no such obligation exists the responsible party is nonetheless obliged to treat information as confidential unless required by law or in terms of its duties to communicate to other parties who are authorised to process such information.

Inherited characteristics of a data subject may not be processed unless it is for medical purposes or processing of the information is necessary for historical, statistical or research activity.

5.6. Authorisation concerning data subject's criminal behaviour or biometric information

Bodies which are charged by law with applying criminal law or responsible parties who have obtained information about the data subjects criminal behaviour or biometric information are permitted to process such information.

The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

6. Processing of personal information of children

The Gradidge Mahura Group may not process the personal information of a child unless so authorised in terms of Section 35 of the POPI Act.

A child “means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself”

A competent person “means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child”

A responsible party shall be authorised or able to process personal information of a child if:

- carried out with the prior consent of a competent person (for instance a guardian or parent);
- necessary for the establishment, exercise or defence of a right or obligation in law;
- necessary to comply with an obligation of international public law;
- for historical, statistical or research purposes to the extent that is in the public interest or if it appears to be impossible to ask for consent or involve disproportionate effort to do so and guarantees are provided to ensure that processing of this nature does not affect the individual privacy of the child to a disproportionate extent;
- personal information which has been made public by a competent person.

Authorisation by the Regulator:

The Regulator may, upon application by the Gradidge Mahura Group or by notice in the Gazette, authorise a responsible party to process personal information of children if:

- It is in the public interest;
- Appropriate safeguards have been established; and
- Subject to conditions imposed.

The last mentioned conditions that may be imposed by the Regulator are:

- The manner in which the responsible party must provide means for the competent person to review the personal information processed and may refuse its further processing.
- Provide notice regarding the nature of the personal information of children that is processed, how it is being processed and further processing practices;
- How to ensure that a child is not persuaded to provide more information than necessary;
- Establish procedures to ensure the integrity and confidentiality of the personal information from children.