HerEmpire Group
POPI Act Policy

Table of Contents

Protection of Personal Information Policy Version: 1
Publishing Date: 23 February 2024
Last Review Date:N/A
Frequency of Review: As Required
Next Review Date: As Required
Responsible Business Unit: Administration

This policy is crucial for the policy owner's business operations. All company members must comply with the policy's standards, methods, and procedures. Risk and control owners are responsible for supervising and enforcing control processes.

1. INTRODUCTION

The South African Constitution and POPIA both protect privacy as a fundamental human right. The company collects the personal information of clients, customers, employees, and other stakeholders while delivering quality goods and services. Privacy rights entail managing personal information without unwanted interference. The organisation is committed to complying with POPIA regulations to protect privacy.

2. DEFINITIONS

2.1. **Personal data** refers to any information that can be used to identify a living and natural person. It also applies to an identifiable, existing juristic person, such as a company. This can include details about a person's:

2.1.1. race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, and birth.

2.1.2. Additionally, it may include information about a person's education, medical history, financial history, criminal history, employment history, and any identifying numbers, symbols, email addresses, physical addresses, telephone numbers, location information, online identifiers, or biometric information.

2.1.3. It can also refer to a person's personal opinions, views, or preferences, as well as correspondence that is private or confidential, statements made about the person by others, and a person's name if it reveals any personal information.

2.2. **Data Subject:** The data subject is the individual or entity to whom personal information pertains, such as a client, customer, or company providing products to the organisation.

2.3. **Party Responsible** The accountable entity that requires personal information for a specific purpose is known as the responsible party and decides how to process it.

2.4. **Operator:** An operator handles personal data on behalf of a responsible entity through a contract or mandate without direct supervision. An indemnity agreement is necessary when working with an operator.

2.5. **Data Officer:** The Data Officer ensures POPIA compliance. If there's no Information Officer, the leader must carry out their duties. The Information Officer must register with the SA Information Regulator before commencing their duties, and they may appoint Deputy Information Officers.

2.6. **Processing:** Handling Processing information involves various activities related to personal data, such as collecting, storing, updating, sharing, and deleting data, among others.

2.7. **Record:** Record means documented information, in any format or storage method. It includes writing on any surface, data stored using devices like tape recorders or computers (hardware and software), or any material derived from such data. It also includes visual images in labels, markings, books, maps, photographs, films, or other devices that can be reproduced with or without additional equipment.

2.8. **Filing System:** A filing system is an organised collection of personal data that can be accessed based on certain criteria, regardless of whether it is centralised, decentralised, or dispersed based on function or location.

2.9. **Unique Identifier**: A Unique Identifier is an allocated identifier used by a responsible party to uniquely identify a data subject in regard to that party for operational purposes.

2.10. **Anonymize**: This refers to removing any data that can identify a data subject or can be used, either alone or in combination with other information, to identify the data subject.

2.11. **Re-Identify:** refers to the process of restoring any de-identified personal information that can be used to identify or alter data subjects.

2.12. **Consent:** Consent is a voluntary, precise, and informed statement of will that grants approval for the processing of personal information.

2.13. **Direct marketing:** involves contacting an individual, whether in person, by mail, or electronically, with the aim of promoting goods or services, or soliciting donations.

2.14. **Biometrics:** refers to a method of personal identification that relies on physical, physiological, or behavioural characteristics such as blood type, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

3. OBJECTIVE OF THE POLICY

The purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information, which include:

- **Violations of confidentiality.** Sharing personal data unlawfully can decrease revenue.
- **Lacking in providing options.** Data subjects should have control over their information.
- **Reputational harm.** A negative event, like a hacker erasing personal information, can harm the organisation's reputation and shareholder value.

This policy shows the organisation's dedication to safeguarding the privacy rights of data subjects by outlining expected behaviour and ensuring compliance with the regulations of POPIA and industry best practices.

- To protect personal information, an organisation should establish a culture that values privacy as a fundamental right.
- Implement internal controls and business processes to manage compliance risks related to safeguarding personal information.
- Delegate tasks to control owners such as Information Officers to safeguard the organisation's interests and rights of data subjects.
- Increase awareness through training and guidance for individuals handling personal information.

4. IMPLEMENTATION OF POLICY

This policy applies to everyone associated with the organisation, including the governing board, branches, employees, volunteers, contractors, affiliates and suppliers. It should be interpreted alongside POPIA and the organisation's PAIA Policy.

POPIA regulations apply to personal information recorded for a responsible person in South Africa, but not to personal or household activities or de-identified information.

5. DATA SUBJECTS' RIGHTS

The company shall inform its clients and consumers of their rights as data subjects when necessary. The organisation will ensure that it upholds the following seven rights.

5.1. The Right to Access Personal Information

Individuals have the right to know if we have their personal information and can request access to it. See Annexure A for the "Personal Information Request Form".

5.2. The Right to Rectify or Erase Personal Information

The data subject can seek the correction or deletion of their personal information if the organisation is no longer permitted to keep it.

5.3. The Right to Object to Personal Information Processing

Individuals can object to their personal information being processed if they have reasonable grounds. The organisation will review the request and may stop using or sharing the data and delete it if possible.

5.4. The Right to Object to Direct Marketing

The individual has the right to oppose the use of their personal information for direct marketing through unsolicited electronic communications.

5.5. The Right to File a Complaint with the Information Regulator

To report a violation of POPIA rights, file a complaint with the Information Regulator and take legal action. See Annexure B for a "POPI Complaint Form" example.

5.6. The Right to Information

People have the right to know when their personal information is collected, and if it is accessed by an unauthorised person.

6. FUNDAMENTAL PRINCIPLES

All employees and representatives of the organisation must always adhere to the following guiding principles.

6.1. Accountability

Non-compliance with POPIA can harm reputations and lead to legal action. Protecting personal information is everyone's duty. We will ensure compliance and impose sanctions on violators.

6.2. Limitations in Processing

We will handle personal information fairly and lawfully, with the informed consent of the data subject, and only for specific purposes. We will obtain written consent before processing personal information and maintain an audio recording of the conversation when services or transactions are conducted over the phone or electronic video feed. We will not share personal information with anyone not involved in the original purpose of collecting the information.

6.3. Purpose Specification

The organisation's business units and operations must be transparent. Personal information will only be processed for specific lawful purposes, and data subjects will be notified before collection or recording.

6.4. Limitation on Subsequent Processing

Personal information can only be used for its intended purpose. If an organisation wants to use it for something else, they must obtain further consent from the individual.

6.5. Data Quality

We'll ensure that all personal information is accurate and complete. We'll verify it directly with the data subject or through independent sources.

6.6. Open Communication

Organisations must inform data subjects about the collection and processing of personal information, including its purpose.

Contact the organisation via email at info@herempire.group to request information or file a complaint.

6.7. Security Measures

The organisation will ensure the security of its filing system for personal information with security procedures to reduce the risk of loss, unauthorised access, disclosure, interference, alteration, or destruction. More stringent security measures will be used for highly sensitive personal information. The company will regularly assess its security controls to prevent cyber-attacks. Access to personal information will be restricted to authorised personnel only. New and current employees will sign contracts with confidentiality clauses to minimise unauthorised disclosures. Operators and third-party service providers must sign agreements to comply with POPIA.

6.8. Involvement of Data Subjects

Individuals can request correction or deletion of their data, and businesses must provide an opt-out option for electronic newsletters or marketing.

7. INFORMATION OFFICERS

An Information Officer and Deputy Information Officer may be designated by an organisation to ensure adherence to POPIA. While it is not a legal obligation, it is considered beneficial, especially in larger organisations. The appointed Information Officer is responsible for POPIA compliance, and the head of the organisation will take over in their absence. Annual reviews are conducted for the Information Officer and any Deputy Information Officers. The Information Officer must be registered with the South African Information Regulator once appointed, as mandated by POPIA.

8. SPECIFIC DUTIES AND RESPONSIBILITIES

8.1. Governing Body

The organisation's governing body is accountable for complying with POPIA. It can delegate tasks to management or other competent personnel.
The board must appoint an Information Officer and, if necessary, a Deputy Information Officer.

- Personnel handling personal data must be trained, supervised, and aware of the consequences of violating this policy.
- Data subjects are informed of the procedure they need to follow if they desire to inquire about their personal information.
- Schedule regular POPI audits to evaluate how personal information is handled.

8.2. Information Officer

The Information Officer is responsible for ensuring the organisation's compliance with POPIA.

- informing the governing body of the organisation's data protection duties as outlined in POPIA.
- If a security breach occurs, the Information Officer must notify and counsel the governing body about their responsibilities under POPIA.
- Consistently evaluating privacy regulations and ensuring they match the organisation's policies for processing personal information. This will involve evaluating the organisation's information protection practices and associated policies.
- Ensuring that POPI Audits are regularly scheduled and conducted.
- Ensuring the organisation facilitates easy access for anyone wishing to update their personal information or file grievances relating to POPI. For example, having a "Contact Us" feature on the organisation's website.
- Approving contracts that may affect the personal information kept by the organisation with operators, employees, and other third parties. This will involve supervising the revision of the organisation's employment contracts and other service level agreements.
- Encouraging adherence to the necessary conditions for the legal processing of personal data.
- Ensuring that employees and representatives of the organisation are well-informed on the risks related to handling personal information and are kept up to date on the organisation's security measures.
- Coordinating and supervising the awareness training for employees and other individuals handling personal information on behalf of the company.
- Responding to employees' inquiries regarding POPIA.

- handling all requests and complaints relating to POPIA filed by the organisation's data subjects.
- collaborating with the Information Regulator regarding any current investigations. The Information Officers will serve as the primary contact for the Information Regulator authorities for personal information processing and will seek advice from the Information Regulator as needed on other problems.
- The Deputy Information Officer will support the Information Officer in carrying out their responsibilities.

8.3. The IT Manager

The IT Manager oversees the organisation's IT operations.

- Ensuring that the organisation's IT infrastructure, filing systems, and any other equipment utilised for processing personal information adhere to accepted security requirements.
- Ensuring that all digital personal information is stored solely on specified discs and servers and sent exclusively to authorised cloud computing services. Placing servers with personal information in a secure place separate from the regular office environment.
- Ensuring that all digitally stored personal information is regularly backed up and tested.
- Ensuring that any backups containing personal information are safeguarded from unauthorised access, unintentional deletion, and harmful hacking efforts.
- Ensuring that personal information exchanged electronically is encrypted.
- Ensuring that all servers and computers storing personal data are safeguarded by a firewall and up-to-date security software. Conducting routine IT audits to verify the appropriate functioning of the organisation's hardware and software systems. Conducting routine IT audits to confirm if electronically stored personal data has been accessed or obtained by unauthorised individuals. Conducting a thorough due diligence evaluation before entering into contracts with operators or third-party service providers to handle personal information on behalf of the business. For example, cloud computing services.

8.4. Marketing & Communications Manager

The Marketing & Communication Manager of the organisation is in charge of:

- approving and ensuring the security of personal information statements and disclaimers on the organisation's website, as well as on communications like emails and electronic newsletters.
- Responding to inquiries regarding the protection of personal information from journalists or media sources like newspapers.
- Collaborating with individuals representing the organisation to ensure that any outsourced marketing efforts adhere to POPIA regulations.

8.5. Employees and other Persons acting on behalf of Organisation

Employees and representatives of the organisation may access personal information of clients, suppliers, and other workers as part of their job duties. Personal information is private and confidential, and sharing it is prohibited unless it is publicly available or necessary for job responsibilities. If there are any doubts or uncertainties, employees should seek assistance from their supervisor or the Information Officer.

Personal information will only be processed by employees and representatives of the organisation under the following circumstances:

- when the data subject or a competent individual (in the case of a child) gives consent;
- when processing is essential for fulfilling a contract involving the data subject;
- when processing is required by law;
- when processing serves a legitimate interest of the data subject; or when processing is necessary for pursuing the legitimate interests of the organisation or a third party receiving the information.

Additionally, personal data will only be handled if the individual:

- comprehends the reasons and objectives for collecting their personal information and
- has provided explicit written or verbal consent for the organisation to process it.

We obtain explicit and informed consent from data subjects before processing their personal information. Informed consent means that the data subject understands the purpose for which their personal information is required and with whom it will be shared. We accept written consent in any electronic medium that can be easily converted into printed form. When transactions are completed over the phone or through an electronic video feed, we retain a voice recording of the data subject's permission.

Direct consent from the data subject will be sought for processing their personal information, unless:

- the information is already public,
- consent has been given to a third party, or
- The information is required for law enforcement purposes.

Employees and representatives of the organisation are not allowed to:

- process or access personal information unless it is necessary for their work responsibilities or duties.
- Save personal information straight to their personal PCs, laptops, tablets, or smartphones. All personal data should be retrieved and modified from the organisation's central database or a designated server.
- disclose intimate information casually. Avoid sending personal information due to its lack of security. Personal information can be obtained from the appropriate line manager or Information Officer.
- Export personal data from South Africa without explicit consent from the Information Officer.

Employees and representatives of the company must ensure:

- the security of all personal information they handle by taking appropriate steps and according to the principles in this policy.
- Ensuring that personal information is stored in the minimum number of locations required. Avoid creating any superfluous records, filing systems, or data sets.
- Ensuring that personal information is encrypted before transmitting or sharing it electronically. The IT Manager will help employees and allow representatives of the company to send or share personal information with authorised external parties as necessary.
- Make sure any computers, laptops, and devices storing sensitive information are password protected and never left unattended. Passwords must be updated frequently and should not be disclosed to unauthorised individuals.
- Make sure to power down or lock computer screens and other devices when not in use or when away from desks.
- Make sure to securely store personal information on removable storage devices like external drives, CDs, or DVDs by keeping them locked away when not in use.

- Ensuring that paper-based personal information is stored securely in a place inaccessible to unauthorised individuals. For example, within a secured compartment of a filing cabinet. Make sure that printed personal information is not left unattended where unauthorised individuals could access or duplicate it. For example, near the printer.
- Ensuring that personal information is accurate and up to date by taking appropriate measures. For example, verifying a data subject's contact information when the client or customer contacts you via phone or email. Prior approval from the appropriate line manager or Information Officer is required to update outdated information about a data subject.
- Ensuring that personal information is maintained for only as long as necessary based on the original purpose for collection. Prior authorization from the relevant line manager or Information Officer is necessary to delete or dispose of personal information when it is no longer needed.
- receiving periodic POPI awareness training.

If an employee or a representative of the organisation detects or suspects a security breach involving unauthorised access, interference, modification, destruction, or unauthorised disclosure of personal information, they must promptly report it to the Information Officer or Deputy Information Officer.

9. REQUEST FOR PERSONAL INFORMATION PROCEDURE

Data subjects may

- request what personal information the organisation keeps and why.
- request personal data.
- learn how to update personal information.

Email the Information Officer for information requests.

An Information Officer will give the data subject a “Personal Information Request Form”. Before providing personal information, the Information Officer will authenticate the data subject's identity after receiving the completed form. All inquiries will be reviewed against the company's Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) policy. The Information Officer will respond to requests promptly.

10. POPI COMPLAINTS PROCEDURE

Complaints may be filed via email to **info@herempire.group**

11. DISCIPLINE

After a POPI complaint or infringement investigation, the organisation may recommend administrative, legal, and/or disciplinary action against any employee reasonably suspected of

engaging in any non-compliant activity outlined in this policy. Employee awareness training will be provided if ignorance or minor negligence occurs. The company may fire an employee for extreme carelessness or intentional mismanagement of personal information. Evidence of excessive carelessness will trigger disciplinary proceedings.

- A recommendation to start disciplinary action is an urgent step after an investigation.
- a criminal inquiry referral to law enforcement.
- recovering money and assets to minimise harm.

12. ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please download, complete and email to: info@herempire.group

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address	

Please be aware that we may require you to provide proof of identification prior to processing your request. There may also be a reasonable charge for providing copies of the information requested.

A. Particulars of Data Subject:	
Name & Surname	
Identity No	
Postal Address	
Contact Number	
Email Address	
B. Request:	
I request the organisation to:	
☐ Inform me whether it holds any of my personal information	
☐ Provide me with a record or description of my personal information	
☐ Correct or update my personal information	
☐ Destroy or delete a record of my personal information	
C. Instructions	

Signature:_____ Date:_____

13. ANNEXURE B: POPI COMPLAINT FORM

Please download, complete and email to:info@herempire.group

The Protection of Personal Information Act binds us to uphold your privacy and the confidentiality of your personal information.

Please submit the completed form to the Information Officer:	
Name	
Contact Number	
Email Address	

If we are unable to resolve your complaint to your satisfaction, you have the right to complain to the information Regulator.

Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.
Email: enquiries@inforegulator.org.za
Website: https://inforegulator.org.za/

A. Particulars of Complainant	
Name & Surname	
Identity No	
Postal Address	
Contact Number	
Email Address	
B. Details of Complaint	
C. Desired Outcome	

Signature:_____ Date:_____