| Process Owner | Doc. Author | | | | Revision Data | |
|---|---|---|---|---|---|---|
| Group Financial Manager | J Leone | | | | **Effective Date** | 01/11/2018 |
| | | | | | **Revision Date** | - |
| **Document Title** | Protection of Personal Information Act 4 of 2013 Compliance Framework (POPI) | | | | | |
| **Document No** | WHL-SOP-POPI-1/2018 | **Controlled** | Y | | **Revision Number** | 01 |

## Amendment History

| Issue | Date | Amendment Details | Requested By |
|---|---|---|---|
| 01 | 01/11/2018 | New Document | J Leone |

## 1. OBJECTIVE

1.1. This Compliance Framework is aimed at setting out general guidelines for compliance with the Protection of Personal Information Act 4 of 2013 ("POPI"), which regulates the flow of information and the manner in which personal information in processed.

1.2. This Compliance Framework is merely a guideline and should be read in conjunction with any specific POPI policies formulated to regulate the flow of information in a specific business unit.

## 2. APPLICATION

2.1. This Compliance Framework shall apply to all subsidiaries and operating divisions of Workforce Holdings Ltd (hereinafter collectively referred to as "business units").

## 3. DEFINITIONS

For purposes of this Compliance Framework, the following definitions shall apply:

3.1. **"Data subject"** shall mean the person to whom personal information relates;

3.2. **"Personal Information"** shall mean information relating to an identifiable living natural person or where applicable an identifiable existing juristic person, of which the most pertinent for **our** purposes are: information relating to the education or the medical financial, criminal or employment history of the person, and any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assigned to the person;

3.3. **"Processing"** shall mean any operation or activity or set of operations, whether or not by automatic means, concerning personal information, including: collection, receipt recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution, or making available in any form; or merging, linking, restriction, degradation, erasure or destruction of information.

3.4. **"Record(s)"** shall mean any recorded information in any form or medium and shall include, but not be limited to: writing, tape recordings, labels, markings, books, maps, plans, graphs, drawings, photographs, films, and any form of visual images; irrespective of whether it was created by the business unit and regardless of when it came into existence.

3.5. **"Special Personal Information"** shall include information relating to: religious or philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health, sex life, biometric information, criminal behaviour.

## 4. MANAGEMENT RESPONSIBILITIES

4.1. The management structures established in all business units shall ensure compliance with this Compliance Framework and/or any specific POPI policies applicable to its business unit and shall monitor and manage such compliance or appoint a designated representative within its business unit to carry out this compliance function.

4.2. Business units may be required to submit to compliance audits from time to time, and/or report on its level of compliance from time to time.

4.3. Failure to comply with this Compliance Framework and/or any other POPI policies may be investigated and dealt with in terms of the Disciplinary Policy and Procedure applicable to business units.

## 5. LAWFUL PROCESSING

5.1. Personal Information shall at all times be lawfully processed in accordance with the provision of the POPI Act and relevant company policies.

5.2. Personal Information shall be processed in accordance with the following conditions:

5.2.1. Accountability:

- Business units shall ensure that all the conditions set out herein are complied with at the time of processing of the Personal Information.

5.2.2. Processing Limitation:

- Having regard to the purpose of processing the Personal Information, it shall only be processed if it is adequate, relevant and not excessive
- Personal Information shall only be processed if processing is necessary to carry out functions for the conclusion or performance of a contract to which the data subject is a party, processing protects a legitimate interest of the Data Subject, or Processing is necessary to pursuing a legitimate interest of the business unit to whom the information is supplied.
- Personal Information shall be collected directly from the Data Subject, unless the information can be obtained by means of public record, using another source will not prejudice a legitimate interest of the Data Subject, personal collection would prejudice a lawful purpose of the collection, or personal collection is not reasonably practicable.

5.2.3. Purpose Specification:

- Personal Information shall only be collected for a specific, defined and lawful purpose related to a function or activity of a business unit.
- Personal Information shall not be retained longer than necessary for achieving the purpose for which it was processed.

- Business Units shall destroy or delete all records of Personal Information or de-identify (as defined in the POPI Act) as soon as possible after the business unit is no longer entitled to retain such record. Reconstruction must be impossible.

5.2.4. Information Quality:

- Reasonable steps must be taken to ensure that Personal Information is accurate, updated and not misleading.

5.2.5. Openness:

- A Data Subject must be made aware of the following:
  - that information is collected or the source from which it is collected;
  - the name and address of the business unit collecting the information;
  - the purpose for the collection;
  - whether or not the supply of the information is voluntary or mandatory;
  - consequences of not providing the information;
  - any law requiring the information;
  - where applicable, that the information shall be transferred to a third party.

5.2.6. Security Safeguards:

- Business units shall secure the integrity and confidentiality of Personal Information by taking reasonable measures to prevent loss, damage or unauthorised destruction of Personal Information and unlawful access to- or processing of Personal Information.
- Where Personal Information is provided by a third party operator as defined in the POPI Act, business units shall ensure that a written agreement is entered into with such operator stipulating that the operator shall comply with the security requirements set out in the POPI Act.
- Should a business unit become aware of any possible unauthorised access or acquisition of Personal Information, it shall as soon as reasonably practicable report such unauthorised event to the Information Officer of Workforce Holdings, who shall be appointed by the Chief Executive Officer from time to time.

5.2.7. Data Subject Participation:

- Data Subjects have the right to request, free of charge, whether a Business Unit is in possession of its Personal Information, the nature of the Personal Information held and the identity of any third parties in possession of the Personal Information.

- Data Subjects further has the right to request the Business Unit correct or delete Personal Information held by the business unit which is inaccurate, irrelevant, excessive, incomplete, misleading or obtained unlawfully.
- Business units shall give effect to a Data Subject's requests as soon as possible and must notify the Data Subject that the request has been attended to.

## 6. SPECIAL PERSONAL INFORMATION

6.1. Special Personal Information shall in general not be processed except in the following instances:

- Consent from the Data Subject has been obtained;
- Processing is required for the establishment, exercise or defence of a right or obligation in law;
- Processing is necessary for historical, statistical or research purposes within the ambit of the POPI Act;
- Information has deliberately been made public by the Data Subject;

6.2. The specific exceptions to the processing of Special Personal Information set out in Sections 28 to 33 shall further apply where applicable.

## 7. DIRECT MARKETING

7.1. Personal Information used for purposes of electronic direct marketing shall only be permitted if:

- Consent is obtained
- Is an existing customer of the Business Unit

7.2. Data Subjects may only be approached once in order to request consent.

7.3. Where the Data Subject is an existing customer, their Personal Information may only be processed for Direct Marketing purposes if the information was obtained in the context of a sale of a product or service, and if the purpose of the processing is for Direct Marketing related to the business units *own* similar products or services.