



## ACQUIFIN PROPRIETARY LIMITED

### PROTECTION OF PERSONAL INFORMATION POLICY


Version	Version 1
Publishing Date	April 2024
Last Review Date	April 2024
Frequency of Review	Annually
Next Review Date	April 2025
Policy Owner	Deputy Information Officer (Karien Venter)
Responsible Business Unit	Legal & Compliance


## POLICY STATEMENT

- This policy forms part of the policy owner's internal business processes and procedures.
- Any reference to "The Organisation" shall be interpreted to include the "policy owner".
- The Organisation's governing body, its employees, volunteers, contractors, service providers and any other persons acting on behalf of The Organisation are required to familiarise themselves with the policy's requirements and undertake to comply with the stated processes and procedures.
- Risk owners and control owners are responsible for overseeing and maintaining control procedures and activities.
- The Organisation collects and uses Personal Information of employees, individuals and corporate entities with whom it works, in order to operate and carry out its business effectively.
- The Organisation regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between The Organisation and its stakeholders.
- The Organisation therefore fully endorses and adheres to the principles of POPIA.

## POLICY ADOPTION

By signing this document, I authorise the policy owner's approval and adoption of the processes and procedures outlined herein.

Name & Surname	Gerdouw Steyn
Capacity	Director
Signature	
Date	18 June 2024

Name & Surname	Frederick Nicolaas Van Loggerenberg
Capacity	Director
Signature	
Date	20 June 2024

## CONTROL MEASURES

- Establish a Regulatory Risk & Compliance Management Framework for The Organisation.
- Implement control measures (actions, activities, processes and/or procedures) that will provide reasonable assurance that The Organisation's compliance obligations are met and that non-compliances are prevented, detected and corrected.
- Control measures must be periodically evaluated and tested to ensure their continuing effectiveness.

Action / Activity / Process / Procedure	Control Owner
Annual Review	Deputy Information Officer
Information Officer	Gerdouw Steyn
Deputy Information Officer	Anton Gerber & Karien Venter
POPI Audit	Deputy Information Officer
POPI Awareness Training	Deputy Information Officer

## TABLE OF CONTENTS

1. INTRODUCTION TO ACQUIFIN.....	5
2. DEFINITIONS .....	5
3. POLICY PURPOSE .....	7
4. POLICY APPLICATION.....	7
5. RIGHTS OF DATA SUBJECTS.....	8
6. GENERAL GUIDING PRINCIPLES .....	9
7. PROCESSING PERSONAL INFORMATION.....	9
8. INFORMATION OFFICERS.....	14
9. SPECIFIC DUTIES AND RESPONSIBILITIES .....	14
10. TRAINING & DISSEMINATION OF INFORMATION .....	18
11. POPI AUDIT .....	19
12. DIRECT MARKETING .....	19
13. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE .....	20
14. POPI COMPLAINTS PROCEDURE .....	21
15. DISCIPLINARY ACTION .....	22
16. ANNEXURE A: PERSONAL INFORMATION REQUEST FORM .....	23
17. ANNEXURE B: POPI COMPLAINT FORM .....	24
18. ANNEXURE C: POPIA PRIVACY NOTICE .....	25
19. ANNEXURE D: ADDENDUM TO CONTRACT OF EMPLOYMENT .....	27
20. ANNEXURE E: POPIA POLICY ACKNOWLEDGEMENT .....	29
21. ANNEXURE F: SLA CONFIDENTIALITY CLAUSE .....	30
22. ANNEXURE G: (DEPUTY) INFORMATION OFFICER APPOINTMENT LETTER.....	31

## 1. INTRODUCTION TO ACQUIFIN

- 1.1. Acquifin Proprietary Limited ("The Organisation") is incorporated as a private company in terms of the laws of the Republic of South Africa. Acquifin is classified as a "private body" within the definition of Section 1 of the Act.
- 1.2. The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").
- 1.3. POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.
- 1.4. Through the provision of quality services, The Organisation is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.
- 1.5. A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions. Given the importance of privacy, The Organisation is committed to effectively managing personal information in accordance with POPIA's provisions.

## 2. DEFINITIONS

In this Policy, the following words and expressions bear the meanings ascribed to them:

- 2.1. **"Biometrics"** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
- 2.2. **"Consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
- 2.3. **"Data Subject"** this refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies The Organisation with products or other goods.
- 2.4. **"De-Identify"** means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.
- 2.5. **"Direct Marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
  - 2.5.1. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
  - 2.5.2. Requesting the data subject to make a donation of any kind for any reason.
- 2.6. **"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.
- 2.7. **"Information Officer"** is responsible for ensuring The Organisation's compliance with POPIA.
  - 2.7.1. Where no Information Officer is appointed, the head of The Organisation will be responsible for performing the Information Officer's duties.
  - 2.7.2. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
- 2.8. **"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. For example, a third-party service provider that has contracted with The Organisation to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

- 2.9. “Personal Information”** means any information that can be used to reveal a person’s identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning:
- 2.9.1.** 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 of a person;
  - 2.9.2.** information relating to the education or the medical, financial, criminal or employment history of the person;
  - 2.9.3.** any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
  - 2.9.4.** the biometric information of the person;
  - 2.9.5.** the personal opinions, views or preferences of the person;
  - 2.9.6.** 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;
  - 2.9.7.** the views or opinions of another individual about the person;
  - 2.9.8.** 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.
- 2.10. “Processing”** means the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:
- 2.10.1.** the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - 2.10.2.** dissemination by means of transmission, distribution or making available in any other form; or
  - 2.10.3.** merging, linking, as well as any restriction, degradation, erasure or destruction of information.
- 2.11. “Record”** means any recorded information, regardless of form or medium, including:
- 2.11.1.** Writing on any material;
  - 2.11.2.** 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;
  - 2.11.3.** Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  - 2.11.4.** Book, map, plan, graph or drawing;
  - 2.11.5.** 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.
- 2.12. “Re-Identify”** in relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject
- 2.13. “Responsible Party”** is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, The Organisation is the responsible party.

- 2.14. **“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.

### 3. POLICY PURPOSE

- 3.1. This purpose of this policy is to protect The Organisation from the compliance risks associated with the protection of personal information which includes:
- 3.1.1. Breaches of confidentiality. For instance, The Organisation could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
  - 3.1.2. Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose The Organisation uses information relating to them.
  - 3.1.3. Reputational damage. For instance, The Organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by The Organisation.
- 3.2. This policy demonstrates The Organisation’s commitment to protecting the privacy rights of data subjects in the following manner:
- 3.2.1. Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
  - 3.2.2. By cultivating an organisational culture that recognises privacy as a valuable human right.
  - 3.2.3. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
  - 3.2.4. By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of The Organisation.
  - 3.2.5. By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of The Organisation and data subjects.
  - 3.2.6. By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

### 4. POLICY APPLICATION

- 4.1. This policy and its guiding principles apply to:
- 4.1.1. The Organisation’s governing body
  - 4.1.2. All branches, business units and divisions of The Organisation
  - 4.1.3. All employees and volunteers
  - 4.1.4. All contractors, service providers and other persons acting on behalf of The Organisation.
- 4.2. The policy’s guiding principles find application in all situations and must be read in conjunction with POPIA as well as The Organisation’s PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).
- 4.3. The legal duty to comply with POPIA’s provisions is activated in any situation where there is:
- 4.3.1. A **processing** of
  - 4.3.2. **personal information**
  - 4.3.3. entered into a **record**

4.3.4. by or for a **responsible person**

4.3.5. who is **domiciled** in South Africa.

4.4. POPIA does not apply in situations where the processing of personal information:

4.4.1. is concluded in the course of purely personal or household activities, or

4.4.2. where the personal information has been de-identified.

## 5. RIGHTS OF DATA SUBJECTS

Where appropriate, The Organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The Organisation will ensure that it gives effect to the following seven rights.

### 5.1. The Right to Access Personal Information.

5.1.1. The Organisation recognises that a data subject has the right to establish whether The Organisation holds personal information related to him, her or it, including the right to request access to that personal information.

5.1.2. An example of a "Personal Information Request Form" can be found under "**Annexure A**". A request for access to a data subjects' information will only be considered if it is received from the data subject themselves or from a third party with a valid mandate to request the information.

### 5.2. The Right to have Personal Information Corrected or Deleted.

5.2.1. The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where The Organisation is no longer authorised to retain the personal information.

### 5.3. The Right to Object to the Processing of Personal Information.

5.3.1. The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.

5.3.2. In such circumstances, The Organisation will give due consideration to the request and the requirements of POPIA. The Organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

5.3.3. A data subject who wishes to object to the processing of personal information, must submit the objection to the responsible party on Form 1 of the Regulations to the Act. The responsible party, or a designated person, must render such reasonable assistance as is necessary, free of charge, to enable the data subject to make an objection on Form 1. A copy of Form 1 can be found on the Information Regulator's website.

### 5.4. The Right to Object to Direct Marketing.

5.4.1. The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

5.4.2. A responsible party who wishes to process personal information of a data subject for the purpose of direct marketing by electronic communication must obtain consent directly from the data subject or only approach data subjects who are customers of the responsible party due to a sale of product or service.

5.4.3. A responsible party may approach a data subject, who has not previously withheld such consent, only once in order to request the consent of that data subject.



## **5.5. The Right to Complain to the Information Regulator.**

- 5.5.1.** The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.
- 5.5.2.** An example of a “POPI Complaint Form” can be found under “**Annexure B**”.
- 5.5.3.** Any person who wishes to submit a complaint contemplated in section 74(1) of the Act must submit such a complaint to the Regulator on Part I of Form 5. A responsible party or a data subject who wishes to submit a complaint contemplated in section 74(2) of the Act must submit such a complaint to the Regulator on Part II of Form 5 of the Regulations to the Act. A copy of Form 5 can be found on the Information Regulator’s website.

## **5.6. The Right to be Informed.**

- 5.6.1.** The data subject has the right to be notified that his, her or its personal information is being collected by The Organisation.
- 5.6.2.** The data subject also has the right to be notified in any situation where The Organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

# **6. GENERAL GUIDING PRINCIPLES**

All employees and persons acting on behalf of The Organisation will at all times be subject to, and act in accordance with, the following guiding principles:

## **6.1. Accountability**

- 6.1.1.** Failing to comply with POPIA could potentially damage The Organisation’s reputation or expose The Organisation to a civil claim for damages. The protection of personal information is therefore everybody’s responsibility.
- 6.1.2.** The Organisation will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, The Organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.
- 6.1.3.** The Organisation shall remain liable for compliance with these conditions, even if it has outsourced its processing activities.

## **6.2. Processing Limitation**

- 6.2.1.** The Organisation will ensure that personal information under its control is processed:
  - in a fair, lawful and non-excessive manner, and
  - only for a specifically defined purpose.
- 6.2.2.** The processing of personal information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive. The Organisation may only process personal information if one of the following grounds of lawful processing exists:
  - The data subject consents to the processing;
  - Processing is necessary for the conclusion or performance of a contract with the data subject;
  - Processing complies with a legal responsibility imposed on The Organisation;

- Processing protects a legitimate interest of the Data Subject and
- Processing is necessary for pursuance of a legitimate interest of the Company, or a third party to whom the information is supplied.

**6.2.3.** The Organisation will inform the data subject of the reasons for collecting his, her or its personal information telephonically and obtain written consent from the data subjects for the processing of their personal information.

**6.2.4.** The Organisation will maintain a voice recording of the telephone call where the stated purpose for collecting the personal information is disclosed to the data subject.

**6.2.5.** The Organisation data subject's written consent is obtained through signature of the Acknowledgement of Debt and Credit Agreements that contain consent for processing personal information clauses.

**6.2.6.** The Organisation may only process Special Personal Information under the following circumstances:

- The data subject has consented to such processing;
- The Special Personal Information was deliberately made public by the data subject;
- Processing is necessary for the establishment of a right or defence in law;
- Processing is for historical, statistical, or research reasons; and
- If processing of race or ethnic origin is in order to comply with employment equity laws.

**6.2.7.** All data subjects have the right to refuse or withdraw their consent to the processing of their personal information, and a data subject may object, at any time, to the processing of their personal information on any of the above grounds, unless legislation provides for such processing. If the data subject withdraws consent or objects to processing then The Organisation shall forthwith refrain from processing the personal information.

**6.2.8.** Personal information must be collected directly from the data subject, unless:

- Personal information is contained in a public record;
- Personal information has been deliberately made public by the data subject;
- Personal information is collected from another source with the data subject's consent;
- Collection of personal information from another source would not prejudice the data subject;
- Collection of personal information from another source is necessary to maintain, comply with or exercise any law or legal right;
- Collection from the data subject would prejudice the lawful purpose of collection; and
- Collection from the data subject is not reasonably practicable.

**6.2.9.** An example of a "POPI Notice and Consent Form" can be found under "**Annexure C**" and a copy of this notice can be supplied upon request submitted by the data subject to the Deputy Information Officer.

### **6.3. Purpose Specification**

**6.3.1.** All of The Organisation's business units and operations must be informed by the principle of transparency.

**6.3.2.** The Organisation will process personal information only for specific, explicitly defined and legitimate reasons as outlined in 7.1.1 below.

### **6.4. Further Processing Limitation**

**6.4.1.** Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

- 6.4.2.** Therefore, where The Organisation seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, The Organisation will first obtain additional consent from the data subject.

## **6.5. Information Quality**

- 6.5.1.** The Organisation will take reasonable steps to ensure that all personal information collected is complete, accurate not misleading and updated.
- 6.5.2.** The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort The Organisation will put into ensuring its accuracy.
- 6.5.3.** Where personal information is collected or received from third parties, The Organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

## **6.6. Open Communication**

- 6.6.1.** The Organisation will take reasonable steps to ensure that data subjects are notified that their personal information is being collected including the purpose for which it is being collected and processed.
- 6.6.2.** The Organisation will ensure that it establishes and maintains a “contact us” facility, through a customer support service, for data subjects who want to:
- Enquire whether The Organisation holds related personal information, or
  - Request access to related personal information, or
  - Request The Organisation to update or correct related personal information, or
  - Make a complaint concerning the processing of personal information.

## **6.7. Security Safeguards**

- 6.7.1.** The Organisation will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.
- 6.7.2.** Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.
- 6.7.3.** The Organisation will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on The Organisation's IT network.
- 6.7.4.** All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which The Organisation is responsible.
- 6.7.5.** The Organisation's operators and third-party service providers will be required to enter into service level agreements with The Organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.
- 6.7.6.** An example of an “SLA Confidentiality Clause” for inclusion in The Organisation's service level agreements can be found under “**Annexure F**”.
- 6.7.7.** Any loss or theft of computers, laptops or other devices which may contain access to Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to safeguard the information, if possible.

## 6.8. Data Subject Participation

- 6.8.1.** A data subject has the right to request access to, amendment, or deletion of their personal information. All such requests must be submitted in writing to the Information Officer/ Deputy Information Officer in the prescribed form, Form 2. A copy of Form 2 can be found on the Information Regulator's website.
- 6.8.2.** Unless there are grounds for refusal as set out in paragraph 12.3, below, The Organisation shall disclose the requested personal information:
- On receipt of adequate proof of identity from the data subject, or requester;
  - Within a reasonable time;
  - On receipt of the prescribed fee, if any; and
  - In a reasonable format.
- 6.8.3.** The Organisation shall not disclose any personal information to any party unless the identity of the requester has been verified.
- 6.8.4.** The Organisation will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.
- 6.8.5.** Where applicable, The Organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

## 7. PROCESSING PERSONAL INFORMATION

### 7.1. Purpose of processing of personal information of data subjects

- 7.1.1.** The Organisation processes personal information of data subjects for the following purposes:
- Fulfilling its statutory obligations in terms of applicable legislation;
  - Verifying information provided to The Organisation;
  - Obtaining information necessary to provide contractual agreements;
  - Monitoring, maintaining and managing contractual obligations to customers, clients, suppliers, service providers, employees, directors and other third parties;
  - Marketing and advertising;
  - Resolving and tracking complaints;
  - Monitoring and securing the assets, employees and visitors to the premises of The Organisation;
  - Historical record keeping, research and recording statistics necessary for fulfilling The Organisations objectives.

### 7.2. Categories of Data Subjects and their Personal Information

- 7.2.1.** The Organisation may process the personal information of the following categories of data subjects. This includes current, past and prospective data subjects:

Data subject	Personal Information Processed
Customers and employees, representatives, agents, contractors and service providers of such customers (Natural and Juristic Persons)	Names; contact details; physical and postal addresses; date of birth; ID number; nationality; race; age; disability, language; names of contact persons; name of legal entity; financial information; registration number; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; confidential correspondence.

Suppliers, service providers to and vendors of The Organisation and employees, representatives, agents, contractors and service providers of such suppliers and service providers;	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; confidential correspondence.
Directors, Employees and officers of The Organisation;	Names; contact details; physical and postal addresses; date of birth; ID number; nationality; race; age; disability, language; biometric information; financial information; tax related information; information relating to the education or the medical, financial, criminal or employment history; race; gender; marital status; national origin; confidential correspondence; the views of opinions of another individual about the data subject.
Shareholders	Names; contact details; physical and postal addresses; date of birth; ID number; financial information; confidential correspondence.
Job applicants	Names; contact details; physical and postal addresses; date of birth; ID number; nationality; race; age; disability, language; information relating to the education or the medical, financial, criminal or employment history; race; gender; marital status; national origin; confidential correspondence; the views of opinions of another individual about the data subject.
Visitors to any premises of The Organisation	Names; contact details; purpose for visitation.
Complaints, correspondents and enquiries from Natural and Juristic Persons	Names; contact details; date of birth; ID number; nationality; race; disability, language; names of contact persons; name of legal entity; registration number; confidential correspondence.

- 7.2.2.** The Company may possess Special Personal Information relating to staff members concerning their membership of trade unions, and medical information contained in medical assessment reports relating to Occupational Health and Safety and other medical information in the form of medical certificates from registered medical practitioners.

### **7.3. Categories of Recipients for Processing of Personal Information**

- 7.3.1.** The Organisation may supply the personal information to any party to whom The Organisation may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers, under the pretext of an official non-disclosure agreement signed by both parties, who render the following services:

- Capturing and organising of data;
- Storing of data;
- Conducting due diligence checks; and
- Accounting services.

- 7.3.2.** Furthermore, The Organisation may supply personal information to anybody enacted in terms of the laws of the republic of South Africa and in terms of which laws The Organisation is obligated to share such information, which may include but is not limited to The South African Revenue Service, The Department of Employment and Labour, the Unemployment Insurance Fund, the Bargaining Council and The Industries Benefit Administrator if any.

### **7.4. Actual or Planned Transborder Flows of Personal Information**

- 1.1.1.** The Organisation do not have any actual or planned transborder flow of any personal information of data subjects at this stage.

## 7.5. Retention of Personal Information Records

- 7.5.1. The Organisation may retain personal information records indefinitely, unless the data subject objects thereto. If the data subject objects to indefinite retention of its personal information, The Organisation shall retain the personal information records to the extent permitted or required by law as outlined in our Document Retention Policy.

## 7.6. General Description of Information Security Measures

- 7.6.1. The Organisation employs up to date technology to ensure the confidentiality, integrity and availability of the personal information under its care. Measures include:
- Firewalls;
  - Virus protection software and update protocols;
  - Logical and physical access control; and
  - Secure Company domain-based setup of hardware and software making up the IT infrastructure for overall remote management of systems.

# 8. INFORMATION OFFICERS

- 8.1. The Organisation will appoint an Information Officer and where necessary, Deputy Information Officers to assist the Information Officer.
- 8.2. The Organisation's Information Officer is responsible for ensuring compliance with POPIA.
- 8.3. The head of The Organisation will assume the role of the Information Officer. Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the re-appointment or replacement of any Deputy Information Officers.
- 8.4. Where the head of The Organisation has decided to authorise another employee of The Organisation to be the Information Officer, such authorisation will be in writing, according to the form and manner of "Annexure C" to the *Guidance Note on Information Officers and Deputy Information Officers* published by the Information Regulator. A copy of these Guidance Notes can be found on the Information Regulators website.
- 8.5. Once appointed, The Organisation will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties, in accordance with "Annexure A" to the *Guidance Note on Information Officers and Deputy Information Officers* published by the Information Regulator.
- 8.6. An example of a "Deputy Information Officer Appointment Letter" can be found under "**Annexure G**". This appointment letter will be used for the internal appointment of the Information Officer and / or Deputy Information Officers. The content of the appointment letter may also be incorporated into the designated employee's key performance areas as a measure to ensure accountability. As an additional requirement, The Organisation will appoint the Deputy Information Officer (if any) in the prescribed format in "**Annexure B**" to the *Guidance Note on Information Officers and Deputy Information Officers* published by the Information Regulator.

# 9. SPECIFIC DUTIES AND RESPONSIBILITIES

## 9.1. Governing Body

- 9.1.1. The Organisation's governing body cannot delegate its accountability and is ultimately answerable for ensuring that The Organisation meets its legal obligations in terms of POPIA.
- 9.1.2. The governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

**9.1.3.** The governing body is responsible for ensuring that:

- The Organisation appoints an Information Officer, and where necessary, Deputy Information Officers.
- All persons responsible for the processing of personal information on behalf of The Organisation:
  - are appropriately trained and supervised to do so,
  - understand that they are contractually obligated to protect the personal information they come into contact with, and
  - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which The Organisation collects, holds, uses, shares, discloses, destroys and processes personal information.

**9.2. Information Officer**

**9.2.1.** The Organisation's Information Officer is responsible for:

- Taking steps to ensure The Organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about The Organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with The Organisation's personal information processing procedures. This will include reviewing The Organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that The Organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to The Organisation. For instance, maintaining a "contact us" facility on The Organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by The Organisation. This will include overseeing the amendment of The Organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of The Organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about The Organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of The Organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by The Organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers and Deputy Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.
- Ensuring that a Compliance Framework is developed, implemented, monitored and maintained.

- Ensure that a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
- Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.
- Ensure that internal awareness is maintained regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- The Information Officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

**9.2.2.** The Deputy Information Officers will assist the Information Officer in performing his or her duties.

### **9.3. IT Manager**

**9.3.1.** The Organisation's IT Manager or the Senior Head of Network Engineering is responsible for:

- Ensuring that The Organisation's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Managing the external service provider SLA to ensure that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Managing the external service provider SLA to ensure that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Managing the external service providers SLA to ensure that they are performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on The Organisation's behalf. For instance, cloud computing services.

### **9.4. Marketing & Communication Manager**

**9.4.1.** The Organisation's Marketing & Communication Manager or the Person fulfilling the position/function is responsible for:

- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on The Organisation's website, including those attached to communications such as emails and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers in line with The Organisations PAIA Manual.
- Where necessary, working with persons acting on behalf of The Organisation to ensure that any outsourced marketing initiatives comply with POPIA.



## **9.5. Employees and other Persons acting on behalf of The Organisation**

- 9.5.1.** Employees and other persons acting on behalf of The Organisation will, during the course of the performance of their services, gain access, under a strict non-disclosure agreement, to and become acquainted with the personal information of certain clients, suppliers and other employees.
- 9.5.2.** Employees and other persons acting on behalf of The Organisation are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
- 9.5.3.** Employees and other persons acting on behalf of The Organisation may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within The Organisation or externally, any personal information, unless such information is already publicly known, or where the employee is legally obligated to disclose the personal information, or the disclosure is necessary in order for the employee or person to perform his or her duties.
- 9.5.4.** Employees and other persons acting on behalf of The Organisation must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
- 9.5.5.** Employees and other persons acting on behalf of The Organisation will only process personal information where:
- The data subject, or a competent person where the data subject is a minor, consents to the processing; or
  - The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
  - The processing complies with an obligation imposed by law on the responsible party; or
  - The processing protects a legitimate interest of the data subject; or
  - The processing is necessary for pursuing the legitimate interests of The Organisation or of a third party to whom the information is supplied.
- 9.5.6.** Furthermore, personal information will only be processed where the data subject:
- Clearly understands why and for what purpose his, her or its personal information is being collected as explained in the signed agreements; and
  - Has granted The Organisation with written or verbally recorded consent to process his, her or its personal information.
- 9.5.7.** Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form, for instance the agreements concluded with the data subject that contains a consent clause.
- 9.5.8.** Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
- the personal information has been made public, or
  - where valid consent has been given to a third party, or
  - the information is necessary for effective law enforcement.
- 9.5.9.** Employees and other persons acting on behalf of The Organisation will under no circumstances:
- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from The Organisation's central database or a dedicated server and secure internal domain systems.
- Share personal information informally. In particular, personal information should only be sent by email to individuals who possess the necessary mandates to receive said personal information.

**9.5.10.** Employees and other persons acting on behalf of The Organisation are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of The Organisation, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them and that those printed copies are destroyed when it is no longer of use.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time.

**9.5.11.** Where an employee, or a person acting on behalf of The Organisation, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

## **10. TRAINING & DISSEMINATION OF INFORMATION**

- 10.1.** This Policy has been put in place throughout The Organisation, training on the Policy and POPIA will take place with all affected employees.
- 10.2.** All existing employees will, after the required consultation process has been followed and probation period has elapsed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses. (**"Annexure D"**)
- 10.3.** All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPIA and be required to sign the POPIA Policy Acknowledgement (**"Annexure E"**)

- 10.4. Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

## 11. POPI AUDIT

- 11.1. The Organisation's Information Officer/ delegated employee will schedule periodic POPI Audits.
- 11.2. The purpose of a POPI audit is to:
- 11.2.1. Identify the processes used to collect, record, store, disseminate and destroy personal information.
  - 11.2.2. Determine the flow of personal information throughout The Organisation. For instance, The Organisation's various business units, divisions, branches and other associated organisations.
  - 11.2.3. Redefine the purpose for gathering and processing personal information.
  - 11.2.4. Ensure that the processing parameters are still adequately limited.
  - 11.2.5. Ensure that new data subjects are made aware of the processing of their personal information.
  - 11.2.6. Re-establish the rationale for any further processing where information is received via a third party.
  - 11.2.7. Verify the quality and security of personal information.
  - 11.2.8. Monitor the extend of compliance with POPIA and this policy.
  - 11.2.9. Monitor the effectiveness of internal controls established to manage The Organisation's POPI related compliance risk.
- 11.3. In performing the POPI Audit, Information Officers/ delegated employee will liaise with line managers in order to identify areas within in The Organisation's operation that are most vulnerable or susceptible to the unlawful processing of personal information.
- 11.4. Information Officers/ delegated employee will be permitted direct access to and have demonstrable support from line managers and The Organisation's governing body in performing their duties.

## 12. DIRECT MARKETING

- 12.1. All Direct Marketing communications shall contain The Organisation name, and/or The Organisation's details, and an address or method for the customer to opt-out of receiving further marketing communication.
- 12.2. **Existing Customers.**
- 12.2.1. Direct Marketing by electronic means to existing customers is only permitted:
    - If the customer's details were obtained in the context of a sale or service; and
    - For the purpose of marketing the same or similar products.
  - 12.2.2. The customer must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.
- 12.3. **Consent**
- 12.3.1. The Organisation may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. The Organisation may approach a Data Subject for consent only once.
- 12.4. **Record Keeping**
- 12.4.1. The Organisation shall keep record of:
    - Date of consent;

- Wording of the consent;
- Who obtained the consent;
- Proof of opportunity to opt-out on each marketing contact; and
- Record of opt-outs.

## 13. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

### 13.1. Request Procedure

#### 13.1.1. Data subjects have the right to:

- Request what personal information The Organisation holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

**13.1.2.** Access to information requests can be made by email to the customer care service, addressed to the Information Officer/ Deputy Information Officers. The Information Officer/ Deputy Information Officers will provide the data subject with a “Personal Information Request Form” (Annexure A).

**13.1.3.** In addition to the aforementioned, where the data subject requests the correction, deletion or destruction of a record of personal information, the Information Officer/ Deputy Information Officers will provide the data subject with the necessary information as to where the **Form 2** to the Regulations of the Act can be obtained. The responsible party, or a designated person, must render such reasonable assistance, as is necessary free of charge, to enable a data subject to complete **Form 2**.

**13.1.4.** Once the completed form has been received, the Information Officer/ Deputy Information Officers will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against The Organisation's PAIA Policy.

**13.1.5.** The Information Officer/ Deputy Information Officers will process all requests within a reasonable time.

### 13.2. Remedies available if request for access to Personal Information is refused

#### 13.2.1. Internal Remedies

The Organisation does not have internal appeal procedures. As such, the decision made by the Information Officer/ Deputy Information Officers pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the Information Officer/ Deputy Information Officers.

#### 13.2.2. External Remedies

A requestor that is dissatisfied with the Information Officer's/ Deputy Information Officer's refusal to disclose information, may lodge a complaint with the Information Regulator in terms of Chapter 10 of POPIA.

### 13.3. Grounds for Refusal

**13.3.1.** The Organisation may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which The Organisation may refuse access include:

- Protecting personal information that The Organisation holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
- Protecting commercial information that The Organisation holds about a third party or The Organisation (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of The Organisation or the third party);

- If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
- If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- If disclosure of the record would prejudice or impair the protection of the safety of the public;
- The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
- Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of The Organisation;
- Disclosure of the record would put The Organisation at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- The record is a computer programme; and
- The record contains information about research being carried out or about to be carried out on behalf of a third party or The Organisation.

#### **13.4. Records that cannot be found or do not exist**

If The Organisation has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

## **14. POPI COMPLAINTS PROCEDURE**

- 14.1.** Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Organisation takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:
- 14.1.1.** POPI complaints must be submitted to The Organisation in writing. Where so required, the Information Officer/ Deputy Information Officers will provide the data subject with a "POPI Complaint Form".
  - 14.1.2.** Where the complaint has been received by any person other than the Information Officer/ Deputy Information Officers, that person will ensure that the full details of the complaint reach the Information Officer/ Deputy Information Officers within 7 business days.
  - 14.1.3.** The Information Officer/ Deputy Information Officers will provide the complainant with a written acknowledgement of receipt of the complaint within 2 business days.
  - 14.1.4.** The Information Officer/ Deputy Information Officers will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer/ Deputy Information Officers will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
  - 14.1.5.** The Information Officer/ Deputy Information Officers must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on The Organisation's data subjects.
  - 14.1.6.** Where the Information Officer/ Deputy Information Officers has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer/ Deputy Information Officers will consult with The Organisation's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

- 14.1.7.** The Information Officer/ Deputy Information Officers will revert to the complainant with a proposed solution with the option of escalating the complaint to The Organisation's governing body within 7 business days of receipt of the complaint. In all instances, The Organisation will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- 14.1.8.** The Information Officer's/ Deputy Information Officer's response to the data subject may comprise any of the following:
- A suggested remedy for the complaint,
  - A dismissal of the complaint and the reasons as to why it was dismissed,
  - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
- 14.1.9.** Where the data subject is not satisfied with the Information Officer's/ Deputy Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
- 14.1.10.** The Information Officer/ Deputy Information Officers will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

## **15. DISCIPLINARY ACTION**

- 15.1.** Where a POPI complaint or a POPI infringement investigation has been finalised, The Organisation may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
- 15.2.** In the case of ignorance or minor negligence, The Organisation will undertake to provide further awareness training to the employee.
- 15.3.** Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which The Organisation may lead to immediate dismissal of the employee in accordance with The Organisations Disciplinary Policy. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
- 15.4.** Examples of immediate actions that may be taken subsequent to an investigation include:
- 15.4.1.** A recommendation to commence with disciplinary action.
  - 15.4.2.** A referral to appropriate law enforcement agencies for criminal investigation.
  - 15.4.3.** Recovery of funds and assets in order to limit any prejudice or damages caused.

## 16. ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

### PERSONAL INFORMATION REQUEST FORM

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 Number:	
Postal Address:	
Contact Number:	
Email Address:	

#### B. Request

I request The Organisation to:

(a) Inform me whether it holds any of my personal information

☐

(b) Provide me with a record or description of my personal information

☐

#### C. Instructions


#### D. Signature Page

Signature

Date

## 17. ANNEXURE B: POPI COMPLAINT FORM

### POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

**Please submit your complaint to the Information Officer:**

Name	
Contact Number	
Email Address:	

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

**The Information Regulator:** Adv Pansy Tlakula

**Physical Address:** JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001.

**Email:** complaints.IR@justice.gov.za

**Website:** <http://www.justice.gov.za/inforeg/index.html>

#### A. Particulars of Complainant

Name & Surname	
Identity Number:	
Postal Address:	
Contact Number:	
Email Address:	

#### B. Details of Complaint


#### C. Desired Outcome


#### D. Signature Page

Signature:	
Date	



## 18. ANNEXURE C: POPIA PRIVACY NOTICE

### POPIA PRIVACY NOTICE

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

#### Our Information Officer's Contact Details

Name	Gerdouw Steyn
Contact Number	082 562 7563
Email Address:	gerdouw@ifsaprivateequity.co.

#### Our details:

Acquifin Proprietary Limited

Operations office: Block 14, Boardwalk Office Park, 79 Eros Street, Faerie Glen, Pretoria

Tel: 087 285 0341

customercare@acquifin.co.za

#### The source of collection of your personal information:

We collect personal information in the following ways:

- Directly from you when we contact you to discuss our products/ services.
- Directly from you when you contact us to inquire about our products/services.
- Directly from other sources, such as public databases, and third parties, as well as other financial institutions, or
- Indirectly through your interactions with third parties from cookies on our website.

Personal information is collected directly from you through the completion of an application form that is completed by one of our call centre agents during telephonic consultation. These forms are completed electronically.

#### Law authorising or requiring collecting of the personal information:

We are obligated in terms of the list of legislation contained in our Access to Information Manual to collect your personal information insofar as it relates to the rendering of the relevant financial services to you:

#### Purpose for Processing your Information:

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Complying with the obligations contained in the contract concluded between yourself and the organisation/ third party.
- To verify your identity and to conduct credit reference searches.
- To notify you of new products or developments that may be of interest to you.
- To confirm, verify and update your details.
- To comply with any legal and regulatory requirements.

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, income, expenditure and your banking details.

### Third parties and your personal information

We may need to share your information to third parties provide advice, reports, analyses, products or services that you have requested. Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us.

These third parties may include:

- Your employer (where applicable);
- The Compliance Officer of the organisation (where applicable);
- Information Technology specialists assisting us with data storage, security, processing, analytics, etc;
- Auditors of the Organisation;
- Regulatory or governmental authorities;

### The Transfer of your personal information outside of the Republic of South Africa

Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

We confirm that we will ensure that the level of protection afforded to your personal information by that third country or international organisation is equal to the protection afforded by the POPI Act.

### Complaints and objections

As a data subject, you have the right to –

- Request that we confirm, free of charge, whether or not we hold personal information about you;
- Request that we provide you with a description of the personal information we hold about you, and to explain why and how it is being processed (please complete Annexure A);
- Request that we consider your objections to the processing of your personal information (please complete Annexure B);
- Lodge a complaint with the Information Regulator (please complete Annexure B).

### The Information Regulator

In the event that your personal information has not been processed in accordance with the POPI Act and the principles set out above, you have the right to lodge a complaint with the Information Regulator.

For further information regarding the complaints process, please visit the website of the Information Regulator, as indicated below.

Alternatively, you may contact the Information Regulator for further assistance:

The Information Regulator: Adv Pansy Tlakula

Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

Email: [complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za)

Website: <https://www.justice.gov.za/inforeg/index.html>

## 19. ANNEXURE D: ADDENDUM TO CONTRACT OF EMPLOYMENT

### ADDENDUM TO CONTRACT OF EMPLOYMENT

#### Protection of Personal Information Act Declaration

In terms of POPIA, a "Responsible Party" (in this case being Acquifin (Pty) Ltd, hereafter the "Employer") has a legal duty to process a "Data Subject's" Personal Information (in this case being the Employee's personal information and related details) in a lawful, legitimate and responsible manner. In order to discharge this duty, the Employer requires the Employee's express and informed permission to process his/her Personal Information.

**"Personal Information"** (PI) shall mean the 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 of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

**"POPIA"** shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

The Employer undertakes to process the PI of the Employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the Employer's relevant policy available to the Employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an Employer and within the framework of the Employment relationship and as required by South African law.

The Employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the Employer. The Employee therefore irrevocably and unconditionally agrees:

1. That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the Employer's discharge of its obligations and to perform its functions as an Employer.
2. That he/she consents and authorises the Employer to undertake the collection, processing and further processing of the Employee's PI by the Employer for the purposes of securing and further facilitating the Employee's employment with the Employer.
3. Without derogating from the generality of the afore stated, the Employee consents to the Employer's collection and processing of PI pursuant to any of the Employer's Internet, Email and Interception policies in place insofar as PI of the Employee is contained in relevant electronic communications.
4. To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
5. The Employee also understand and accept that it is his/her responsibility to keep this information up to date by notifying the nominated person responsible at the Employer whenever his/her personal information changes.
6. To absolve the Employer from any liability in terms of POPIA for failing to obtain the Employee's consent or to notify the Employee of the reason for the processing of any of the Employee's PI.
7. To the disclosure of his/her PI by the Employer to any third party, where the Employer has a legal or contractual duty to disclose such PI.
8. The Employee further agrees to the disclosure of his/her PI for any reason enabling the Employer to carry out or to comply with any business obligation the Employer may have or to pursue a legitimate interest of the Employer in order for the Employer to perform its business on a day to day basis.
9. The Employee authorises the Employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The Employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

The Employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The Employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the Employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within The Organisation or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the Employee or person to perform his or her duties on behalf of the Employer.

By signing this addendum, the Employee confirm that he/she understands his/her right to privacy and the right to have his/her personal information processed in accordance with the conditions for the lawful processing of personal information, and hereby give his/her consent to the Employer to all of the above activities.

Signed at \_\_\_\_\_ on this \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_

\_\_\_\_\_

Employee name

\_\_\_\_\_

Employee signature

## 20. ANNEXURE E: POPIA POLICY ACKNOWLEDGEMENT

### POPIA POLICY ACKNOWLEDGEMENT

By signing this document, I [insert employee's name] hereby:

1. Confirm that I have read the POPIA policy, that I have received awareness training on POPIA, and that I have been given the opportunity to refer any aspects that are unclear to me or questions I might have to the Information Officer.
2. Give consent that my personal information (PI) may be collected, processed and stored in line with the policy and my employment contract.
3. Acknowledge that the Employer endeavours to keep my PI up to date, and that it is my responsibility to keep the Employer informed of any changes to my PI and to provide the relevant details timeously. I understand that I have the right to check my PI retained by the Employer to ensure that it is correct, complete and current. All this information is supplied voluntarily, without undue influence from any party and not under any duress.
4. Accept that I have the right to:
  - 4.1 Know what information is being kept and how that information is being used;
  - 4.2 Access the information at any reasonable time to rectify and correct my PI details;
  - 4.3 Revoke my consent given to the Employer in terms of this form at any time. This revocation must be in writing and addressed to the Information Officer. Any such action would require the Employer to review the impact this may have on the employment relationship. Withdrawal of consent is not retroactive and will not affect use of my information already made.
  - 4.4 Lodge a complaint to the Information Officer or Information Regulator.
5. I agree to report any breach with regards to this policy to the Information Officer promptly and to comply with the policy and the procedures described therein.

Employee Name: \_\_\_\_\_

Employee Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Witness Name: \_\_\_\_\_

Witness Signature \_\_\_\_\_

Date: \_\_\_\_\_

Instruction: Please return the signed Policy Acknowledgment form by **[insert date]** to **[insert name]**.

## 21. ANNEXURE F: SLA CONFIDENTIALITY CLAUSE

### SLA CONFIDENTIALITY CLAUSE

- **“Personal Information”** (PI) shall mean the 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 of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; 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; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.
- **“POPIA”** shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.
- The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.
- The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.
- The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.
- Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

## 22. ANNEXURE G: DEPUTY INFORMATION OFFICER APPOINTMENT LETTER

### DEPUTY INFORMATION OFFICER APPOINTMENT LETTER

I herewith and with immediate effect appoint you as the Deputy Information Officer as required by the Protection of Personal Information Act (Act 4 of 2013). This appointment may at any time be withdrawn or amended in writing.

You are entrusted with the following responsibilities:

- Taking steps to ensure the organisation's reasonable compliance with the provision of POPIA.
- Keeping the governing body updated about the organisation's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with the organisation's personal information processing procedures. This will include reviewing the organisation's information protection procedures and related policies.
- Ensuring that POPI Audits are scheduled and conducted on a regular basis.
- Ensuring that the organisation makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the organisation, to do so. For instance, maintaining a "contact us" facility on the organisation's website.
- Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by the organisation. This will include overseeing the amendment of the organisation's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that employees and other persons acting on behalf of the organisation are fully aware of the risks associated with the processing of personal information and that they remain informed about the organisation's security controls.
- Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the organisation.
- Addressing employees' POPIA related questions.
- Addressing all POPIA related requests and complaints made by the organisation's data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Deputy Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.
- Ensuring that a compliance framework is developed, implemented, monitored and maintained.
- Ensuring that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- Ensure that a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
- Ensure that internal measures are developed together with adequate systems to process requests for information or access thereto.
- Ensure that internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time.

**I hereby accept the appointment as Deputy Information Officer**

Name & Surname

Signature:

Date: