TRADE AVAIL 260 CC T/A CORPORATE INSURANCE CONSULTANTS CC

REGISTRATION NUMBER 2000/062348/23

PROTECTION OF PERSONAL INFORMATION AND ACCESS TO INFORMATION MANUAL

PUBLISHED IN TERMS OF THE PROMOTION OF ACCESS TO INFORMATION ACT (2 OF 2000) ("PAIA") AND THE PROTECTION OF PERSONAL INFORMATION ACT (4 OF 2013) ("POPIA")

JANUARY 2025 ISSUE

INDEX

1. INTRODUCTION

PAIA and POPIA give effect to the constitutional right of privacy and access to information held by private or public bodies.

Through the provision of services we collect, use, retain and disclose certain aspects of the personal information of clients, employees and other stakeholders.

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, we are committed to the effective management of personal information in accordance with POPIA's provisions. This Policy sets out the manner in which we deal with personal information collected, how it is stored and the purpose for which said information is used.

This manual further provides for the submission of requests for access to these records and details how to object to the processing, correction and deletion of personal information by CIC.

A copy of this policy is available on request to the Information Officer of CIC, whose details are contained in this document

The Policy is also published on CIC's website: https://cicassess.co.za/

Guides to PAIA and POPIA can be obtained and queries addressed the Information Regulator at www.justice.gov.za/inforeg/index.html / inforeg@justice.gov.za / complaints.IR@justice.gov.za

2. DEFINITIONS

"Personal Information" is 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: 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; 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.

"Data Subject" refers to the natural or juristic person to whom personal information relates, such as an individual client or a company.

"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.

"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 with whom documents are shared that contains personal information.

"Information Officer" is responsible for ensuring compliance with POPIA.. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties.

"Processing" the act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes: the collection, receipt, recording, organising, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as any restriction, degradation, erasure or destruction of information.

"Record" means any recorded information, regardless of form or medium, including: writing on any material; Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; book, map, plan, graph or drawing; photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

"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.

"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.

"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.

"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.

"PAIA" refers to The Promotion of Access to Information Act, 2 of 2000.

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

"Direct Marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or Requesting the data subject to make a donation of any kind for any reason.

"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.

3. POLICY OBJECTIVES

The objective of this policy is to ensure effective governance through the development and promotion of privacy and accountability whilst allowing for the access required to exercise and protect rights subject to the justifiable limitations set out in the Constitution of South Africa (108 of 1996).

4. POLICY APPLICATION

This policy and its guiding principles apply to our employees and management in all business units, branches and divisions as well as all contractors, suppliers and persons acting with or on behalf of CIC in the rendering of any services.

This policy should be read together with the PAIA Policy as required by the **Promotion of Access to Information Act, 2 of 2000**. The legal duty to comply with POPIA's provisions is initiated in any situation where there is: ***A processing of personal information, entered into a record by or for a responsible person who is domiciled in South Africa***.

POPI does not apply in situations where the processing of personal information -

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

We will ensure that our clients are made aware of the rights conferred upon them as data subjects and that we give effect to the following rights:

THE RIGHT TO ACCESS PERSONAL INFORMATION

A data subject has the right to establish whether CIC holds personal information related to him/her or it includes the right to request access to that personal information.

*The **Personal Information Request Form** is attached hereto and marked as **ANNEXURE A***

THE RIGHT TO HAVE PERSONAL INFORMATION CORRECTED OR DELETED

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

THE RIGHT TO OBJECT TO THE PROCESSING OF PERSONAL INFORMATION

The data subject has the right, on reasonable grounds, to object to the processing of his/her or its personal information. In such situations, we will give due consideration to the request and the requirements of POPIA. We 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.

THE RIGHT TO OBJECT TO DIRECT MARKETING

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.

THE RIGHT TO COMPLAIN TO THE INFORMATION REGULATOR

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 POPI and to institute civil proceedings regarding the alleged non-compliance with the protection of his/her or its personal information.

*The **POPI Complaint Form** is attached hereto and marked as **ANNEXURE B***

THE RIGHT TO BE INFORMED

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

6. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

We are committed to processing personal information lawfully and to comply with the following conditions:

CONDITION 1: ACCOUNTABILITY (Section 8)

We maintain an approach of transparency of operational procedures that controls the collection and processing of personal information. We will ensure that the provisions of POPIA and the principles outlined herein are complied with. We will also 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. Failing to comply with POPIA could potentially damage our reputation or expose us to a civil claim for damages.

CONDITIONS 2 & 3: PROCESSING LIMITATION (Sections 9 – 12) & FURTHER PROCESSING LIMITATION (Section 15)

We undertake to collect personal information in a legal and reasonable way and to process the personal information obtained from data subjects only for the purpose for which it was obtained in the first place. Processing of personal information obtained will not be undertaken in an insensitive or wrongful way that can intrude on privacy. Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose and additional consent is obtained.

We will inform the data subject of the reasons for collecting his/her or its personal information and **obtain written consent prior to processing personal information**. Alternatively, where services or transactions are concluded over the telephone or electronically, we will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent. Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other areas of our business and be provided with the reasons for doing so.

*A **POPI Notice and Consent Form** is attached hereto and marked as **ANNEXURE C***

CONDITION 4: PURPOSE SPECIFICATION (Sections 13 – 14)

Personal information will only be collected for a specific, explicitly defined and lawful purpose and related to the business of CIC. We are compelled to keep effective record of personal information and undertakes not to retain information for a period longer than prescribed by legislation. All personal information will be disposed of at the end of the retention period in such a way that it cannot be reconstructed. We will inform data subjects of these requirements prior to collecting or recording the data subject's personal information.

CONDITION 5: INFORMATION QUALITY (Section 16)

We will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. We 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, where the personal information is collected or received from third parties.

CONDITION 6: OPENNESS (Sections 17 - 18)

We 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. We will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through an electronic helpdesk, for data subjects who want to: ***enquire whether the we hold related personal information, request access to related personal information, request CIC to update or correct related personal information or make a complaint concerning the processing of personal information***

CONDITION 7: SECURITY SAFEGUARDS (Sections 19 – 22)

We 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. 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 reports, the greater the security required. We will continuously review our security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on our IT network. We will furthermore ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

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 we are responsible. All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment contracts containing the relevant consent and confidentiality clauses.

Our operators and third-party service providers will be required to enter into service level agreements with us where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement an also to contain a confidentiality clause.

CONDITION 8: DATA SUBJECT PARTICIPATION (Sections 23 – 25)

We will ensure that it provides a capability for data subjects who want to request the correction of or deletion of their personal information. We will also provide an option to data subjects to "unsubscribe" from any of its electronic newsletters or marketing material.

7. USAGE OF PERSONAL INFORMATION

The Personal Information of each data subject will only be used for the purpose for which it was collected and as agreed.

This may include, but not limited to:

- *Providing products or services to clients and to carry out the transactions requested;*
- *For underwriting purposes;*
- *Assessing and processing claims;*
- *Conducting credit reference searches and/or- verification;*
- *Confirming, verifying and updating client details;*
- *For purposes of claims history;*
- *For the detection and prevention of fraud, crime, money laundering or other malpractices;*
- *Conducting market or customer satisfaction research;*

- *For audit and record keeping purposes;*
- *In connection with legal proceedings;*
- *Providing communication in respect of the business of CIC and any related regulatory matter/s that may affect the client directly and or indirectly; and*
- *In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.*

According to section 10 of POPIA, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the processing of Personal Information:

i. The client's consents to the processing: consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;
ii. The necessity of processing: in order to conduct an accurate analysis of the client's needs for purposes of amongst other credit limits, insurance requirements, etc.
iii. Processing complies with an obligation imposed by law on CIC;
iv. Processing protects a legitimate interest of the client;
v. Processing is necessary for pursuing the legitimate interests of CIC or of a third party to whom information is supplied.

8. DISCLOSURE AND SAFEGUARDING OF PERSONAL INFORMATION

We may disclose a client's personal information to any of CIC's group of companies or subsidiaries, joint venture companies and/or approved product or third-party product suppliers or service providers whose services or products clients elect to use. We will ensure that we have agreements in place to comply with confidentiality and privacy conditions.

We may also share clients' personal information with, and obtain information about clients from third parties for the reasons already discussed herein above. We may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the rights of CIC. It is a requirement in terms of the POPIA to adequately protect personal information. We will continuously review our security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to safeguard the personal information of both Employees and Clients of CIC:

- ✓ Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- ✓ All existing employees, will be required to sign an Addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- ✓ Any archived client information stored at the offices of CIC is also governed by POPI. Access to these documents is limited to authorised staff members only and the Information Officer has a list of names of these staff members and periodic control checks are performed to ensure compliance.
- ✓ Product suppliers and all other third-party service providers will be required to sign a Service Level Agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.
- ✓ All electronic files or data are to be backed up on a regular basis.
- ✓ Consent to process client information is obtained from each individual client (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and needs analysis stage of the relationship.

9. INFORMATION OFFICER

Our Information Officer is responsible for ensuring compliance with POPIA. We will appoint a POPIA Information Officer and if needed, a Deputy Information Officer to assist the Information Officer in the execution of his/her duties. On an annual basis, we will review the appointment, re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.

Once appointed, we will register the Information Officer with the South African Information Regulator established under POPI prior to performing his or her duties. An **Information Officer Appointment Letter** is attached hereto and marked as **ANNEXURE D**.

10. ROLES AND RESPONSIBILITIES OF KEY ROLEPLAYERS WITHIN CIC

SENIOR MANAGEMENT

Our senor management cannot delegate its accountability and is ultimately responsible for ensuring that CIC meets its legal obligations in terms of POPIA. Senior management may delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

Senior management is responsible for ensuring that:

- ✓ We appoints an Information Officer, and where necessary, a Deputy Information Officer;
- ✓ All persons responsible for the processing of personal information on behalf of CIC 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.
- ✓ A periodic POPIA Audit is scheduled in order to accurately assess and review the ways in which CIC collects, holds, uses, shares, discloses, destroys and processes personal information.

INFORMATION OFFICER

Our Information Officer is responsible for:

- ✓ Taking steps to ensure CIC's reasonable compliance with the provisions of POPIA.
- ✓ Keeping senior management updated about CIC's information protection responsibilities under POPIA.
- ✓ Reviewing CIC's information protection procedures and related policies.
- ✓ Ensuring that POPIA audits are scheduled and conducted on a regular basis.
- ✓ Ensuring that CIC makes it convenient for data subjects who want to update their personal information or submit changes to their personal information.
- ✓ Managing all POPIA related complaints.
- ✓ Ensuring the maintenance of a "contact us" facility on CIC'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 CIC. This will include overseeing the amendment of CIC'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 CIC are fully aware of the risks associated with the processing of personal information and that they remain informed about CIC's security controls.
- ✓ Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of CIC.
- ✓ Addressing employees' POPIA related questions.
- ✓ Addressing all POPIA related requests and complaints made by CIC's data subjects.
- ✓ Working with the Information Regulator in relation to any ongoing investigations.

IT MANAGER/SERVICE PROVIDER

CIC's Manager/Service Provider is responsible for:

- ✓ Ensuring that CIC'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.
- ✓ Ensuring 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.
- ✓ Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion.
- ✓ Ensuring that personal information being transferred electronically is encrypted.
- ✓ Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security protection software.
- ✓ Performing regular IT audits to ensure that the security of CIC's hardware and software systems are functioning properly.

- ✓ 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 CIC's behalf.

MARKETING & COMMUNICATION MANAGER (where applicable)

CIC's Marketing & Communication Manager is responsible for:

- ✓ Approving and maintaining the protection of personal information statements and disclaimers that are displayed on CIC's website, including those attached to communications such as emails and electronic newsletters.
- ✓ Addressing any personal information protection queries received from the media and or newspapers.
- ✓ Working with any persons appointed by CIC to handle outsourced marketing initiatives to ensure that all such information comply with POPIA.

EMPLOYEES AND OTHER PERSONS ACTING ON BEHALF OF CIC

Employees and other persons acting on behalf of CIC are responsible for:

- ✓ Keeping all personal information 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 or password protected prior to sending or sharing the information electronically. The IT Manager/Service Provider will assist employees and where required, other persons acting on behalf CIC, 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 must be changed regularly and 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 is stored on removable storage media such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- ✓ Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- ✓ 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, for instance, close to the printer.
- ✓ 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. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- ✓ 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 POPIA Awareness training from time to time.
- ✓ Where an employee, or a person acting on behalf of CIC, 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.

11. POPI COMPLIANCE AUDITS

CIC's Information Officer will schedule periodic POPIA compliance audits.

The purpose of a POPI compliance audit is to:

- ✓ Identify the processes used to collect, record, store, disseminate and destroy personal information.
- ✓ Determine the flow of personal information throughout CIC. For instance, CIC's various business units, divisions, branches.
- ✓ Redefine the purpose for gathering and processing personal information.
- ✓ Ensure that the processing parameters are still adequately limited.

- ✓ Ensure that new data subjects are made aware of the processing of their personal information.
- ✓ Re-establish the rationale for any further processing where information is received via a third party.
- ✓ Verify the quality and security of personal information.
- ✓ Monitor the extent of compliance with POPIA and this policy.
- ✓ Monitor the effectiveness of internal controls established to manage CIC's POPIA related compliance risk.

12. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

Data subjects have the right to:

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

Access to information requests can be made by e-mail, addressed to the Information Officer. The Information Officer will provide the data subject with a **Personal Information Request Form**. Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests made for personal information will be processed and considered against CIC's PAIA Policy. The Information Officer will process all requests within a reasonable time.

13. RETENTION PERIODS OF CERTAIN DOCUMENT TYPES IN TERMS OF DIFFERENT LEGISLATION

Documents need to be retained in order to prove the existence of facts and to exercise rights CIC may have. It is also needed to exercise effective control over the retention of documents and electronic transactions

- as prescribed by legislation; and
- as dictated by business practice.

Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of CIC and to minimise reputational risks, to ensure that CIC's interests are protected and that the clients' rights to privacy and confidentiality are not breached.

We have identified the following legislation to be most applicable to CIC and the type of business we run and have highlighted the document retention requirements as required and need to take these into account in our data management processes:

COMPANIES ACT, NO 71 OF 2008, COMPANIES AMENDMENT ACT 3 OF 2011
CONSUMER PROTECTION ACT, (CPA) NO 68 OF 2008
FINANCIAL INTELLIGENCE CENTRE ACT (FICA) NO 38 OF 2001
EMPLOYMENT EQUITY ACT, NO 55 OF 1998
LABOUR RELATIONS ACT, NO 66 OF 1995
UNEMPLOYMENT INSURANCE ACT, NO 63 OF 2002
TAX ADMINISTRATION ACT, NO 28 OF 2011
INCOME TAX ACT, NO 58 OF 1962
CLOSE CORPORATION ACT, NO 69 OF 1984

14. ELECTRONIC STORAGE

The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with the IT department who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

SCANNED DOCUMENTS

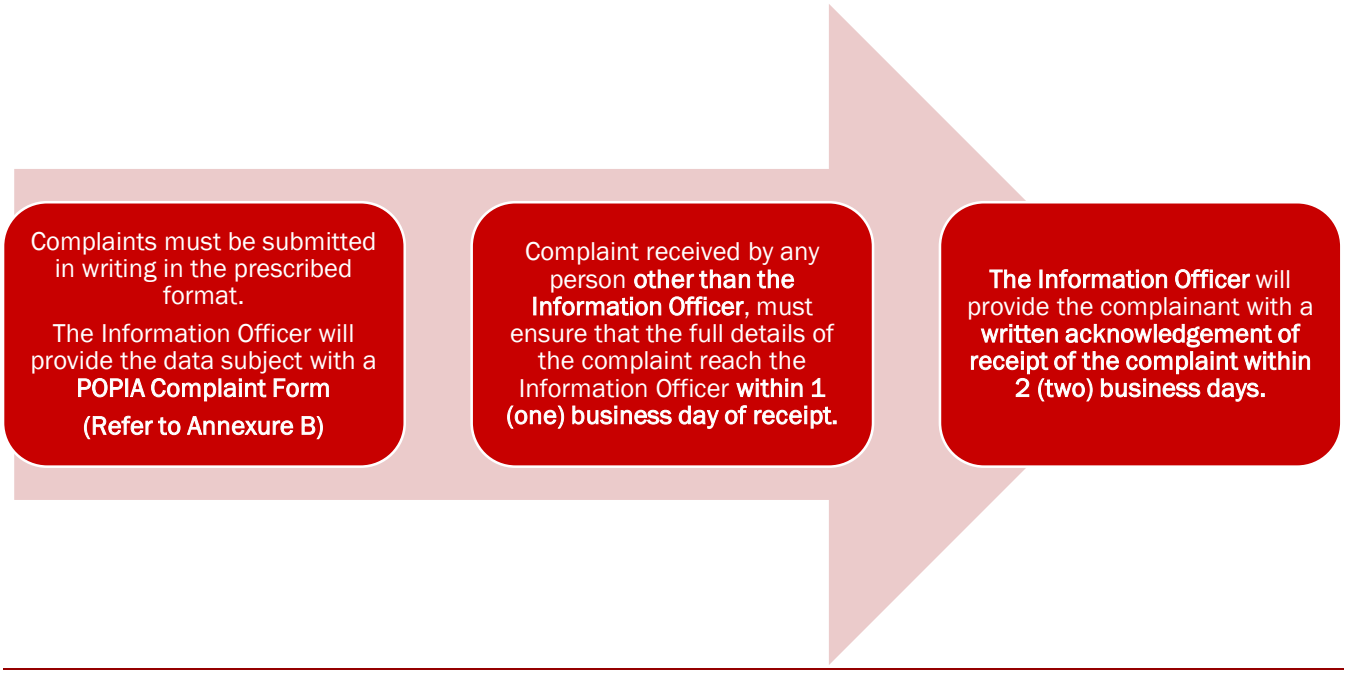
If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

SECTION 51 OF THE ELECTRONIC COMMUNICATIONS ACT (ECTA) NO 25 OF 2005

The ECTA requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

15. POPI COMPLAINTS PROCEDURE

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. All POPIA related complaints will be handled in accordance with the following process:



The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable, fair manner and in accordance with the principles outlined in POPIA.

1. The Information Officer should determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on CIC's data subjects.

2. Where the Information Officer has reason to believe that the personal information of data subjects have been accessed or acquired by an unauthorised person, the Information Officer will consult with CIC's senior management and thereafter the affected data subjects and the Information Regulator will be informed of this breach.

3. The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to CIC's senior management **within 7 (seven) working days of receipt of the complaint**. In all instances, CIC will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

The 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.*

Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator

The Information Officer 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 POPIA related complaints.

16. DISCIPLINARY ACTION

Where a POPIA complaint or a POPIA infringement investigation has been finalised, CIC 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.

In the case of ignorance or minor negligence, CIC will undertake to provide further awareness training to the employee. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which CIC may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.

Actions to be taken after an investigation include:

- ✓ A recommendation to commence with disciplinary action.
- ✓ A referral to appropriate law enforcement agencies for criminal investigation.
- ✓ Recovery of funds and assets in order to limit any prejudice or damages caused.

17. PENALTIES FOR NON-COMPLIANCE

There are essentially two legal penalties or consequences for serious breaches of POPIA for the responsible party:

I. A fine of between R1 million and R10 million and/or imprisonment of one to ten years; or
II. Paying compensation to data subjects for the damage they have suffered.

The other penalties include:

- *Reputational damage*
- *Losing customers (and employees)*
- *Failing to attract new customers.*

18. AVAILABILITY AND REVISION

This policy is made available on CIC's website and/or by request from the Information Officer. This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Information Officer

NAME & SURNAME:	
CONTACT NUMBER:	
E-MAIL ADDRESS:	

NOTE! 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 CIC to: **(please tick the appropriate action)**

(a) Inform me whether it holds any of my personal information	
(b) Provide me with a record or description of my personal information	
(c) Correct or update my personal information	
(d) Destroy or delete a record of my personal information	

C. INSTRUCTIONS

D. SIGNATURE

_____
SIGNATURE
NAME:

DATE:

POPIA COMPLAINT FORM

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

Please submit your complaint to the Information Officer at:

NAME AND SURNAME:	
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:
PHYSICAL ADDRESS: SALU Building, 316 Thabo Sehume Street, Pretoria
EMAIL ADDRESS: inforreg@justice.gov.sa
WEBSITE: http://www.justice.gov.sa/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

_____
SIGNATURE
NAME:

DATE:

ANNEXURE C: POPIA NOTICE AND CONSENT FORM

POPIA NOTICE AND CONSENT FORM

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 AND SURNAME:	
CONTACT NUMBER:	
EMAIL ADDRESS:	

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:

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your insurance policies
- To process insurance claims and to take recovery action
- 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, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information and your banking details.

Consent to Disclose and Share your Information

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

Disposal of Personal Information

All your personal information will be disposed of at the end of the applicable retention period and in such a way that it cannot be reconstructed.

I hereby authorise and consent to CIC sharing my personal information with the following person/s:

.....

.....

.....

.....

SIGNATURE

_____
SIGNATURE
NAME:

DATE:

ANNEXURE D: POPIA INFORMATION OFFICER APPOINTMENT LETTER

NOTE! To be placed onto a Business Letterhead

INFORMATION OFFICER APPOINTMENT LETTER

We, Trade Avail 260 CC t/a CIC hereinafter referred to as the "CIC" herewith and with immediate effect appoint

(insert name and surname of appointed Information Officer) as the Information Officer as required by the **Protection of Personal Information Act, 4 of 2013.**

This appointment may at any time be withdrawn or amended in writing.

This appointment carries the following responsibilities:

1. Taking steps to ensure CIC's reasonable compliance with the provision of POPIA.
2. Keeping senior management updated about CIC's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise senior management of their obligations pursuant to POPIA.
3. Continually analysing privacy regulations and aligning them with CIC's personal information processing procedures. This will include reviewing CIC's information protection procedures and related policies.
4. Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
5. Ensuring that POPIA Audits referenced in (4) above are properly recorded and should any breaches be found that remedial action is taken to rectify same.
6. Ensuring that CIC makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to CIC, to do so. For instance, maintaining a "contact us" facility on CIC's website.
7. Approving any contracts entered into with operators, employees and other third parties which may have an impact on the personal information held by CIC. This will include overseeing the amendment of CIC's employment contracts and other service level agreements.
8. Encouraging compliance with the conditions required for the lawful processing of personal information.
9. Ensuring that employees and other persons acting on behalf of CIC are fully aware of the risks associated with the processing of personal information and that they remain informed about CIC's security controls.
10. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of CIC.
11. Addressing employees' POPIA related questions.
12. Addressing all POPIA related requests and complaints made by CIC's data subjects.
13. Working with the Information Regulator in relation to any ongoing investigations. The 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.

I HEREBY ACCEPT THE APPOINTMENT AS INFORMATION OFFICER

_____
SIGNATURE
NAME:

DATE OF APPOINTMENT:	

ON BEHALF OF CIC AND IN CONFIRMATION OF THE APPOINTMENT

_____
SIGNATURE
NAME:
ROLE IN CIC:

DATE:	