Data Privacy Policy in terms of Protection of Personal Information Act 4 of 2013 (POPIA)

Ref Nr	Compiled/Reviewed by	Date of last review	Signature
1	Thomson Wilks Inc.	Compiled: June 2021	

1. INTRODUCTION

Thomson Wilks Inc., established in 1995, is a full-service law firm with offices in each of the major commercial centres, being Sandton, Durban and Cape Town. The firm consists of over 30 Attorneys and the firm is 51% black owned. Clients range from individuals, corporates to JSE listed companies. Thomson Wilks Inc. is also on the panels of most of the major banks. In response to the interest from Chinese companies in South Africa we have also established a Chinese Law department.

Thomson Wilks Inc. has strategic alliances with law firms in the United Kingdom, Europe, Malta, Zimbabwe, Zambia and Mauritius.

We offer considerable expertise and experience in the following fields:

- Access to Information
- Administration of Estates
- Arbitration
- Aviation
- Banking Law
- Black Economic Empowerment
- Building & Engineering
- Commercial & Corporate
- Company Law
- Competition Law
- Constitutional Law & Human Rights
- Consumer Protection & National Credit Act
- Conveyancing
- Criminal Law
- Customs & Excise
- Debt Collection
- Debt Counselling
- Divorce & Family Law
- Environmental Law
- Evictions
- Financial Services
- Franchising Law

- Fraud Investigation
- General Civil Litigation
- Governance & Compliance
- Immigration
- Information Telecommunication Technology
- Insolvency
- Insurance, Legal Compliance & Regulatory Law
- Intellectual Property (Copyrights, Trademarks & Patents)
- International Trade
- Internet Law
- Labour & Employment
- Legal Due Diligence
- Marketing & Advertising Law
- Media, Sport & Entertainment
- Mediation
- Medical Law
- Mergers & Acquisitions
- Mining Law
- MVA Claims
- Notarial Practice
- Offshore Company Formation & Direction
- Privacy Law
- Property
- Tax Law
- Tender Response (Economic Development)
- Trusts
- Wills

2. COMPANY DETAILS AND REGISTRATION OF INFORMATION OFFICER

Postal Address: P.O. Box 78440, Sandton, 2146
Street Address: 23 Impala Road, Chislehurston, Sandton
Telephone Number: (011) 784 8984
Email: info@thomsonwilks.co.za

The following are Directors of the Company:

Anel Bestbier	900911 0178 086	073 497 8966	602 Camden Hill, 21 St. Johns Road, Cape Town, Western Cape
David Angus Dewar	690920 5073 089	082 608 0484	9 Falcon Close, Kenrock Estate, Hout Bay, Western Cape, 8001
Tumisang Reginald Kgaboesele	730515 555 0086	082 416 3886	27 East Road, Morningside, Johannesburg, Gauteng, 2196
Stephen Charles Thomson	590216 533 0186	082 444 4480	6 – 2nd Close, 50 Mount Street, Bryanston, Gauteng, 2021

3. INFORMATION OFFICER AND DUTIES

3.1. An Information Officer has been appointed and his/her responsibilities shall include:

3.1.1. the encouragement of compliance by Thomson Wilks with the conditions for the lawful processing of personal information;

3.1.2. dealing with requests made to Thomson Wilks pursuant to POPIA; and

3.1.3. working with the Regulator in relation to investigations conducted.

3.2. The delegated and registered persons with the Information Regulator of South Africa, under registration number 14390/2021-2022/IRRTT, are:

Stephen Charles Thomson	CEO – Information Officer	082 444 4480	stephen@thomsonwilks.co.za

Keri Caitlin Soldo	General Manager – Deputy Information Officer	079 586 0953	keri@thomsonwilks.co.za

4. DEFINITIONS

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

4.2. "**data subject**" means the person to whom personal information relates;

4.3. "**information officer**" of, or in relation to, a:

4.3.1. "**public body**" means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of POPIA; or

4.3.2. "**private body**" means the head of a private body as contemplated in Section 1, of POPIA;

4.4. "**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;

4.5. "**personal information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person;

4.6. "**processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information;

4.7. "**public record**" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

4.8. "**Regulator**" means the Information Regulator established in terms of Section 39 of POPIA.

5. PURPOSES OF POPIA

5.1. Thomson Wilks complies with and will continue to comply with the principles and provisions of the POPIA as more fully described herein.

5.2. The purpose of POPIA is to:

5.2.1. give effect to the constitutional right of privacy, in particular the safeguarding of personal information subject to justifiable limitations aimed at balancing the right of privacy against other rights, particularly that of access to information protecting the free flow of information;

5.2.2. prescribe minimum requirements for the lawful processing of personal information;

5.2.3. regulate the processing of personal information in harmony with international standards;

5.2.4. prescribe minimum requirements for the lawful processing of personal information;

5.2.5. provide rights and remedies to protect against abuse of personal information; and

5.2.6. establish a Regulator to promote, enforce and fulfil the rights protected by POPIA.

5.3. The Act also addresses the use of personal information in direct marketing by way of unsolicited electronic communication, the restrictions on trans-border information flows and protects the personal information of children. These are all burning issues in our information age which are being dealt with in jurisdictions across the globe.

5.4. Chapter 2 of the Act applies to processing of personal information in any form by a responsible party (the person who alone or in conjunction with others, determines the purpose of and means for processing personal information) who or which is domiciled in South Africa or if not domiciled in South Africa, makes use of automated or non-automated means in South Africa, unless the processing relates only to the forwarding of personal information through South Africa.

5.5. Personal information which is processed by non-automated means falls under the ambit of POPIA only if it forms part of a filing system or is intended to be part of a filing system.

5.6. POPIA will not apply to the processing of personal information:

5.6.1. for purely personal or household activity;

5.6.2. that has been de-identified;

5.6.3. processed by or on behalf of a public body for the purposes of:

5.6.3.1. safeguarding national security;

5.6.3.2. the investigation and prosecution of criminal matters;

5.6.3.3. processed by the cabinet and its committees or the executive council of a province; or

5.6.3.4. relating to the judicial functions of a court.

5.7. The exclusions referred to in 5.6 relating to processing by or on behalf of a public body for the purposes of national security and the investigation of crime, do not free any organ of State from providing adequate safeguards to ensure that the controls contemplated in POPIA that do not influence national security or the investigation of crime are established and maintained.

5.8. POPIA does not apply to:

5.8.1. the processing of personal information for the purposes of journalistic, literary or artistic expression in defined circumstances;

5.8.2. the exclusion for journalistic purposes requires the journalist to be subject to a code of ethics and provides adequate safeguards for the protection of personal information.

6. APPLICABLE LEGISLATION AND REGULATORY FRAMEWORK

No	Ref	Act
1	*No 61 of 1973*	*Companies Act*

2	*No 55 of 1988*	*Employment Equity Act*
3	*No 95 of 1967*	*Income Tax Act*
4.	*No 66 of 1995*	*Labour Relations Act*
5.	*No 66 of 1995*	*Labour Relations Act*
6.	*No 89 of 1991*	*Value Added Tax Act*
7.	*No 37 of 2002*	*Financial Advisory and Intermediary Services Act*
8.	*No 75 of 1997*	*Basic Conditions of Employment Act*
9.	*No 25 of 2002*	*Electronic Communications and Transactions Act*
10.	*No 2 of 2000*	*Promotion of Access of Information Act*
11.	*No 30 of 1996*	*Unemployment Insurance Act*
		Any additional – LPC, FICA etc

6.1. The Protection of Personal Information Act 4 of 2013 (POPIA) regulates the processing of personal information in South Africa. Its purposes include:

6.1.1. the regulation of the processing of personal information in harmony with international standards; and

6.1.2. the provision of rights and remedies to Data Subjects (those whose personal information is processed.

6.2. Personal information broadly means any information relating to an identifiable, natural person or juristic person. This includes, but is not limited to:

6.2.1. contact details: email, telephone, address;

6.2.2. demographic information: age, sex, race, birth date, ethnicity;

6.2.3. history: employment, financial, educational, criminal, medical history;

6.2.4. biometric information: blood type;

6.2.5. opinions of and about the person;

6.2.6. private correspondence.

6.3. The processing of information entails anything done with the personal information, including collection, usage, storage, dissemination, modification or destruction (whether such processing is automated or not).

6.4. Some of the obligations under POPIA are to:

6.4.1. only collect information that is needed for a specific purpose;

6.4.2. apply reasonable security measures to protect it;

6.4.3. ensure it is relevant and up to date;

6.4.4. only hold as much as you need, and only for as long as you need it;

6.4.5. allow the subject of the information to see it upon request.

6.5. The right of privacy is enshrined in the South African Constitution which expressly states that everyone has the right to privacy. POPIA acknowledges the relative nature of the right to privacy and attempts to balance competing interests by providing that one of its purposes is to “balance the right to privacy against other rights, particularly the right of access to information”.

6.6. POPIA sets out a range of principles which must be considered when complying therewith. Organisations are required to take “appropriate, reasonable technical and organisational measures” to protect the integrity and confidentiality of personal information. What exactly the measures are is left open for interpretation. POPIA itself does not prescribe what these measures are.

6.7. As such, in defending oneself should a dispute arise, it would become necessary to prove that those measures put in place by Thomson Wilks Limited (Thomson Wilks), were in fact appropriate, reasonable technical and organisational measures and therefore it should not incur liability.

6.8. Thomson Wilks as an organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

6.9. In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

6.10. Thomson Wilks describes in this policy document our compliance with legislation relevant to our organisation.

6.11. Thomson Wilks binds all its employees, directors, suppliers and third-party service providers who have access to our information systems to comply with this policy.

6.12. Compliance demands identifying Personal Information and taking reasonable measures to protect the data. This will minimise the risk of data breaches and the associated public relations and legal ramifications for the organisation.

6.13. Non-compliance with the POPIA could expose the responsible party to a penalty of a fine and/or imprisonment of up to 12 months. In certain cases, the penalty for non-compliance could be a fine and / or imprisonment of up 10 years.

7. THE ACT

7.1. The ACT grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

7.2. Requests in terms of the ACT shall be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of the Act.

8. COMPLIANCE AND ACCOUNTABILITY

8.1. Thomson Wilks recognises the need to comply with the provisions of POPIA. It has in turn undertaken to put in place various policies and safeguards to ensure that it complies with the provisions of POPIA. Thomson Wilks will review its policies on an annual basis to ensure that they are up to date, relevant and fit for purpose.

8.2. Thomson Wilks will ensure that on an ongoing basis:

8.2.1. the purpose for collecting data is clearly stated;

8.2.2. controls are in place for transfers of personal data to other countries;

8.2.3. data retention schedules are in place together with mechanisms for alteration, deletion/erasure and withdrawal of consent;

8.2.4. system administration, user access and controls are in place;

8.2.5. the legal basis for processing personal data has been clearly established;

8.2.6. an Information Officer is appointed in writing with specific responsibilities for ensuring data protection;

8.2.7. all staff involved in processing of personal data receive training regarding their responsibilities of our data protection and safeguarding;

8.2.8. POPIA consent provisions are followed;

8.2.9. data subjects are made aware of their rights and we have systems and forms in place to assist them in the exercising of those rights;

8.2.10. impact risk assessments are carried out for all new projects and existing data processing.

8.3. Data subject individual rights.

8.4. POPIA grants rights to data subjects, such as;

8.4.1. the right to be informed;

8.4.2. the right of access;

8.4.3. the right to rectification;

8.4.4. the right to erasure;

8.4.5. the right to restrict processing;

8.4.6. the right to data portability;

8.4.7. the right to object; and

8.4.8. rights in relation (objection) to automated decision making and profiling.

8.5. Each of the aforestated rights are supported by appropriate procedures within Thomson Wilks that allow the required action to be taken within the timescales stated in POPIA.

8.6. Thomson Wilks takes cognisance of these rights and has in place procedures designed to deal with and accommodate a data subject's rights within the legislative timescales provided for in POPIA. The timescales are reflected in our related documents or reference to our POPIA request procedure:

8.6.1. request register;

8.6.2. notification of security compromise in terms of Section 22 of POPIA;

8.6.3. registering a complaint as per Section 74 of POPIA;

8.6.4. data subject request form; and

8.6.5. request procedure flowchart (step by step process).

9. PROCESSING PRINCIPALS AND CONDITIONS

9.1. The conditions constitute a collection of conditions which interact with one another, sometimes overlapping and sometimes complementing and supplementing one another. The conditions are set out and discussed more fully below.

9.2. **Condition 1 – Accountability**

9.2.1. The “responsible party” is identified as the Information Officer and Deputy Information Officer/s. They are tasked with ensuring conditions for lawful processing in accordance with the provisions of POPIA, ensuring that the conditions set out in POPIA, together with the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

9.2.2. The clear implication of accountability is that the responsible party remains responsible for the processing of information regardless of it having transferred or communicated that personal information to a third party (defined as an “Operator”), to process the personal information.

9.2.3. A responsible party should designate and properly empower the designated person or persons to manage and safeguard its information, including its personal information or personal information in its custody. In order to safeguard this information, it is critical that an organisation establishes an appropriate information security management system.

9.3. **Condition 2 – Processing Limitation**

9.3.1. Personal information must be processed:

9.3.1.1. lawfully; and

9.3.1.2. in a reasonable manner that does not infringe the privacy of the data subject.

9.3.2. The processing limitation condition embraces and underlines the other conditions of personal information protection. The element of “lawfulness” is fairly straight forward and the responsible party must not act unlawfully in its collection or processing of personal information.

9.3.3. The second element of “reasonableness” is perhaps not as straight forward. The notion of fairness incorporates the requirements of balance and proportionality. Responsible parties must therefore take into account the interests and reasonable expectations of data subjects

as well as all of the provisions which are incorporated in these conditions. In most instances the foundation for this determination will be the “Purpose Specification” contained in Condition 3, which in turn will inform the data subject’s expectation.

9.3.4. Minimality

“Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.”

9.3.4.1. This condition is closely linked to the purpose for which information may be processed. It is intended to ensure that only personal information which is appropriate for the purpose it is being collected, is collected. It should also be noted that it also relates to the nature of the processing which is being contemplated.

9.3.4.2. In those circumstances where a data subject’s consent to processing is obtained, it is likely to be viewed in a more relaxed light than where the processing of personal information is used legitimately but without the consent of the data subject.

9.3.5. Consent, Justification And Objection

9.3.5.1. Personal information may only be processed if:

9.3.5.1.1. the data subject or a competent person where the data subject is a child consents to the processing;

9.3.5.1.2. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

9.3.5.1.3. processing complies with an obligation imposed by law on the responsible party;

9.3.5.1.4. processing protects a legitimate interest of the data subject;

9.3.5.1.5. processing is necessary for the proper performance of a public law duty by a public body; or

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

9.3.6. The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)(a) of the act.

9.3.7. The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)(a), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)(b) to (f) of the act will not be affected.

9.3.8. A data subject may object, at any time, to the processing of personal information—

9.3.8.1. in terms of subsection (1)(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

9.3.8.2. for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

9.3.9. If a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information.

9.3.10. A responsible party may request a data subject's consent in writing on a form which corresponds substantially with Form 4 for the processing of personal information of that data subject for the purpose of direct marketing as contemplated in section 69(2) of POPIA.

9.3.11. Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (8).

9.3.12. It is not necessary to comply with subsection (7) if:

9.3.12.1. the information is contained in or derived from a public record or has deliberately been made public by the data subject;

9.3.12.2. the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

9.3.12.3. collection of the information from another source would not prejudice a legitimate interest of the data subject;

9.3.12.4. collection of the information from another source is necessary:

9.3.12.4.1. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

9.3.12.4.2. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997;

9.3.12.5. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

9.3.12.6. in the interests of national security; or

9.3.12.7. to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

9.3.12.8. compliance would prejudice a lawful purpose of the collection; or

9.3.12.9. compliance is not reasonably practicable in the circumstances of the particular case.

9.3.13. Processing is lawful and justifiable if it is carried out in terms of the provisions of Sections11(1)(b) to (f) of POPIA. Thus, it must be stressed that POPIA is not “consent” driven. This is clear from the provisions of Sections 11(1)(b) to (f) of POPIA which provide

for the processing of information without the consent of the data subject but for the specific purposes that include:

9.3.13.1. the processing is necessary in terms of a contract to which the data subject is a party;

9.3.13.2. processing complies with law;

9.3.13.3. processing which protects a legitimate interest of a data subject;

9.3.13.4. processing necessary to fulfil a public law duty; and

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

9.3.14. Condition 2 is intended to promote the principle that the data subject must bear knowledge of the information which is being collected by a responsible party. The section should also be read together with the "Purpose Specification Condition" and in particular Section 13 of POPIA, which requires that steps must be taken to ensure that the data subject is aware of the purpose of the collection of information by the responsible party. Thus, even where information is collected from a third party, the data subject should be made aware of the processing of the information and the purpose for which the information has been collected. Clearly in certain instances this would not apply but it would be incumbent on the responsible party to show that it was not possible to collect the information directly from the data subject and that the responsible party was justified in not making the data subject aware of the purpose for which the information was collected.

9.4. **Condition 3 – Purpose specific**

9.4.1. Collection for Specific Purpose

9.4.1.1. Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

9.4.1.2. Steps must be taken in accordance with section 18(1) of POPIA to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of Section 18(4) of POPIA are applicable.

9.4.2. Retention and Restriction of Records

9.4.2.1. Subject to Sections 14(2) and 14(3) of POPIA, records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

9.4.2.1.1. retention of the record is required or authorised by law;

9.4.2.1.2. the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

9.4.2.1.3. retention of the record is required by a contract between the parties thereto; or

9.4.2.1.4. the data subject or a competent person where the data subject is a child has consented to the retention of the record.

9.4.2.2. Records of personal information may be retained for periods in excess of those contemplated in paragraph 9.4.2.1 above, for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

9.4.2.3. A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must:

9.4.2.3.1. retain the record for such period as may be required or prescribed by law or a code of conduct; or

9.4.2.3.2. if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity,

taking all considerations relating to the use of the personal information into account, to request access to the record.

9.4.2.4. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of paragraphs 9.4.2.1 or 9.4.2.2.

9.4.2.5. The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

9.4.2.6. The responsible party must restrict processing of personal information if:

9.4.2.6.1. its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

9.4.2.6.2. the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

9.4.2.6.3. the processing is unlawful, and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

9.4.2.6.4. the data subject requests to transmit the personal data into another automated processing system.

9.4.2.7. Personal information referred to in paragraph 9.4.2.6 may, with the exception of storage only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

9.4.2.8. Where processing of personal information is restricted pursuant to paragraph 9.4.2.6, the responsible party must inform the data subject before lifting the restriction on processing.

9.4.2.9. Condition 4 – Further Processing Limitation

9.4.3. Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.

9.4.4. To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of:

9.4.4.1. the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

9.4.4.2. the nature of the information concerned;

9.4.4.3. the consequences of the intended further processing for the data subject;

9.4.4.4. the manner in which the information has been collected; and

9.4.4.5. any contractual rights and obligations between the parties.

9.4.5. The further processing of personal information is not incompatible with the purpose of collection if:

9.4.5.1. the data subject or a competent person where the data subject is a child has consented to the further processing of the information;

9.4.5.2. the information is available in or derived from a public record or has deliberately been made public by the data subject;

9.4.5.3. further processing is necessary:

9.4.5.3.1. to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

9.4.5.3.2. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in Section 1 of the South African Revenue Service Act, 1997;

9.4.5.3.3. for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

9.4.5.3.4. in the interests of national security;

9.4.5.4. the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

9.4.5.4.1. public health or public safety; or

9.4.5.4.2. the life or health of the data subject or another individual;

9.4.5.4.3. the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

9.4.5.4.4. the further processing of the information is in accordance with an exemption granted under Section 37 of POPIA.

9.5. **Condition 5 – Information Quality**

9.5.1. A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

9.5.2. In taking the steps referred to in paragraph 9.5.1 above, the responsible party must have regard to the purpose for which personal information is collected or further processed.

9.5.3. In essence this condition requires that appropriate information security measures safeguarding the integrity of the personal information be employed. This is an information security principle which needs to be taken into account in considering compliance with the Electronic Communications and Transactions Act, 2002. Chapter III of Electronic Communications and Transactions Act, 2002 explicitly requires that the integrity, reliability and accuracy of electronic information be maintained if they are to enjoy the efficacy that the Electronic Communications and Transactions Act, 2002 bestows on them. The same principles that need to be employed in protecting the integrity of information and its updating apply equally in with respect to information in respect to the provisions of POPIA.

9.6. **Condition 6 – Openness**

9.6.1. Quality Information

9.6.1.1. The purpose of this condition is to ensure transparency and fairness in the processing of personal information.

9.6.1.2. A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in Section 14 or 51 (as the case may be) of the Promotion of Access to Information Act, 2000.

9.6.2. Notification to Data Subject when collecting Personal Information

9.6.2.1. If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of:

9.6.2.1.1. the information being collected and where the information is not collected from the data subject, the source from which it is collected;

9.6.2.1.2. the name and address of the responsible party;

9.6.2.1.3. the purpose for which the information is being collected;

9.6.2.1.4. whether or not the supply of the information by that data subject is voluntary or mandatory;

9.6.2.1.5. the consequences of failure to provide the information;

9.6.2.1.6. any particular law authorising or requiring the collection of the information;

9.6.2.1.7. the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

9.6.2.1.8. any further information such as the:

9.6.2.1.8.1. recipient or category of recipients of the information;

9.6.2.1.8.2. nature or category of the information;

9.6.2.1.8.3. existence of the right of access to and the right to rectify the information collected;

9.6.2.1.8.4. existence of the right to object to the processing of personal information as referred to in Section 11(3) of POPIA; and

9.6.2.1.8.5. right to lodge a complaint to the Information Regulator and the contact details of the Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

9.6.2.2. The steps referred to in paragraph 9.6.2.1 must be taken:

9.6.2.2.1. if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or

9.6.2.2.2. in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

9.6.2.3. A responsible party that has previously taken the steps referred to in paragraph 9.6.2.1 complies with paragraph 9.6.2.1 in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

9.6.2.4. It is not necessary for a responsible party to comply with paragraph 9.6.2.1 if:

9.6.2.4.1. the data subject or a competent person where the data subject is a child has provided consent for the non - compliance;

9.6.2.4.2. non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of POPIA;

9.6.2.4.3. non-compliance is necessary:

9.6.2.4.3.1. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

9.6.2.4.3.2. to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997;

9.6.2.4.3.3. for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

9.6.2.4.3.4. in the interests of national security;

9.6.2.4.3.4.1. compliance would prejudice a lawful purpose of the collection;

9.6.2.4.3.4.2. compliance is not reasonably practicable in the circumstances of the particular case; or

9.6.2.4.3.4.3. the information will:

9.6.2.4.3.4.3.1. not be used in a form in which the data subject could be identified; or

9.6.2.4.3.4.3.2. be used for historical, statistical or research purposes.

9.7. **Condition 7 – Security safeguards**

9.7.1. Security Measures on Integrity of Personal Information

9.7.1.1. The security safeguards condition underlines the obligation of the responsible party to ensure that personal information of a data subject in its possession or under its control is appropriately safeguarded against loss, destruction or unlawful access.

9.7.1.2. A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:

9.7.1.2.1. loss of, damage to or unauthorised destruction of personal information; and

9.7.1.2.2. unlawful access to or processing of personal information.

9.7.1.3. In order to give effect to paragraph 9.7.1, the responsible party must take reasonable measures to:

9.7.1.3.1. identify all reasonably foreseeable internal and external risks to personal;

9.7.1.3.2. information in its possession or under its control;

9.7.1.3.3. establish and maintain appropriate safeguards against the risks identified;

9.7.1.3.4. regularly verify that the safeguards are effectively implemented; and

9.7.1.3.5. ensure that the safeguards are continually updated in response to new risks;

or

9.7.1.3.6. deficiencies in previously implemented safeguards.

9.7.1.4. The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

9.7.2. Information Processed by Operator or Person Acting Under Authority of a Responsible Party

9.7.2.1. An operator or anyone processing personal information on behalf of a responsible party or an operator, must:

9.7.2.1.1. process such information only with the knowledge or authorisation of the responsible party; and

9.7.2.1.2. treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

9.7.2.2. The responsible party is also obliged to ensure that an operator not domiciled in the Republic, adheres to the laws governing the processing of personal information.

9.7.3. Security Measures regarding Information Processed by Operator

9.7.3.1. A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in Section 19 of POPIA.

9.7.3.2. The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

9.7.4. Notification of Security Compromises

9.7.4.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify:

9.7.4.1.1. the Regulator; and

9.7.4.1.2. subject to paragraph 9.7.6, the data subject, unless the identity of such data subject cannot be established.

9.7.5. The notification referred to in subsection (1) of the act must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

9.7.6. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

9.7.7. The notification to a data subject referred to in paragraph 9.7.4.1 must be in writing and communicated to the data subject in at least one of the following ways:

9.7.7.1. sent via post to the data subject's last known physical or postal address;

9.7.7.2. sent by e-mail to the data subject's last known e-mail address;

9.7.7.3. placed in a prominent position on the website of the responsible party;

9.7.7.4. published in the news media; or

9.7.7.5. as may be directed by the Regulator.

9.7.8. The notification referred to in subsection 9.7.4.1 must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

9.7.8.1. a description of the possible consequences of the security compromise;

9.7.8.2. a description of the measures that the responsible party intends to take or has taken to address the security compromise;

9.7.8.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

9.7.8.4. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

9.7.9. The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

9.8. **Condition 8 – Data Subject Participation**

9.8.1. Access to Personal Information

9.8.1.1. A data subject, having provided adequate proof of identity, has the right to:

9.8.1.1.1. request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

9.8.1.1.2. request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:

9.8.1.1.2.1. within a reasonable time;

9.8.1.1.2.2. at a prescribed fee, if any;

9.8.1.1.2.3. in a reasonable manner and format; and

9.8.1.1.2.4. in a form that is generally understandable.

9.8.2. If, in response to a request in terms of paragraph 9.8.1.1, personal information is communicated to a data subject, the data subject must be advised of the right in terms of Section 24 of POPIA to request the correction of information.

9.8.3. If a data subject is required by a responsible party to pay a fee for services provided to the data subject in terms of paragraph 9.8.2 to enable the responsible party to respond to a request, the responsible party:

9.8.3.1. must give the applicant a written estimate of the fee before providing the services; and

9.8.3.2. may require the applicant to pay a deposit for all or part of the fee.

9.8.4. A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of paragraph 9.8.1 to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act, 2000 apply.

9.8.5. The provisions of sections 30 and 61 of the Promotion of Access to Information Act, 2000 are applicable in respect of access to health or other records.

9.8.6. If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of paragraph 9.8.5, every other part must be disclosed.

9.8.7. Correction of Personal Information

9.8.7.1. A data subject may, in the prescribed manner, request a responsible party to:

9.8.7.1.1. correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

9.8.7.1.2. destroy or delete a record of personal information about the data subject that in terms of Section 40 of POPIA the responsible party is no longer authorised to retain in terms of Section 14 of POPIA.

9.8.8. On receipt of a request in terms of paragraph 9.8.7.1 a responsible party must, as soon as reasonably practicable:

9.8.8.1. correct the information;

9.8.8.2. destroy or delete the information;

9.8.8.3. provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or

9.8.8.4. where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always

be read with the information, an indication that a correction of the information has been requested but has not been made.

9.8.9. If the responsible party has taken steps under paragraph 9.8.8 that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

9.8.10. Manner of Access

9.8.10.1. The provisions of Sections 18 and 53 of the Promotion of Access to Information Act, 2000 apply to requests made in terms of Section 23 of POPIA.

10. PROCESSING OF SPECIAL PERSONAL INFORMATION

10.1. Prohibition On Processing Of Special Personal Information

10.1.1. Special personal information is information that relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject.

10.1.2. Special personal information also includes criminal behaviour relating to alleged commissions of offences or any proceeding dealing with alleged offences.

10.1.3. Unless a general authorisation, alternatively a specific authorisation relating to the different types of special personal information applies, a responsible party is prohibited from processing special personal information.

10.2. General Authorisation

10.2.1. The prohibition on the processing of special personal information does not apply if:

10.2.1.1. consent of the data subject has been obtained;

10.2.1.2. processing is necessary for the establishment, exercise or defence of a right or obligation in law;

10.2.1.3. processing is necessary to enable compliance with an obligation of International Public Law;

10.2.1.4. processing is for historical, statistical or research purposes, subject to stipulated safeguards;

10.2.1.5. the data subject has deliberately made the information public; or

10.2.1.6. where specific authorisation has been obtained in terms of the Act.

10.2.2. If the data subject has not been notified of the processing of the personal information for purposes other than the information being retained in a public record it is likely that such processing would be unlawful.

10.3. Specific Authorisation

10.3.1. The Act provides separate sections for the authorisation of processing of special personal information. These differ and regard should be had to the specific section governing the authorisation required for processing special personal information.

11. LAWFUL PROCESSING

11.1. Thomson Wilks ensures the lawfulness of data processing and by deploying the measures set out more fully below to ensure continued compliance with POPIA.

11.2. Consent

11.2.1. Thomson Wilks obtains consent from data subjects whose information we need for normal business purposes in writing or, in some cases, when responding to enquiries made by users of our website, using rights notices, including the right to withdraw consent at any time, and a consent button on the website. The privacy notices explain our use and purpose of the data in our organisation. Personal information concerning a child may not be processed save if this is done in accordance with the provisions of Section 35 of the POPIA.

11.3. Contractual Obligations

11.3.1. In certain instances, consent is assumed to be automatically given in concluding specific types of contracts. Examples would be data subject details when purchasing product or rendering a physical address to which a delivery of product or services is to be made. Documented records will be retained where such processing takes place.

11.3.2. Thomson Wilks will ensure that any third-party service providers or operators appointed that will include the service provider processing of personal data are subject to a written contract that binds the service provider and the information processed to full compliance with the terms and provisions of POPIA.

11.4. Normal Legal Obligations

11.4.1. Employee data required for tax purposes and sales tax purposes or by other authorities with a lawful interest is collected by us and processed for these purposes.

11.4.2. Thomson Wilks will not affect any of the rights of a data subject when processing personal information for a lawful reason. Documented records will be retained where such processing takes place.

11.5. Legitimate Interests of the Data Subject and Public Interest

11.5.1. Thomson Wilks will process information where it is in the interest of the data subject. This may include obtaining permission from various statutory authorities for specific actions our organisation might be undertaking on the data subject's behalf. This may form part of a contractual obligation with the data subject or in the public interest and specific consent will not be sought in such cases.

11.5.2. Documented records will be retained where such processing takes place.

11.6. Data Risk and Impact Assessment

11.6.1. Thomson Wilks undertakes an impact and risk assessment on all new projects requiring personal information to ensure the rights of data subjects are protected. These assessments are also undertaken when contemplating or implementing any system changes to our information technology and processing formats.

11.6.2. The impact and risk assessment takes the following into account:

11.6.2.1. the purpose of the data collection and processing;

11.6.2.2. analysis of whether the personal data processing is necessary and proportional to the requirement for data;

11.6.2.3. assessment of the risks and vulnerability to individuals in processing the personal data;

11.6.2.4. compliance via controls over identified risks are identified and implemented.

11.7. Cross Border/International Transfers of Personal Data

11.7.1. A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless they comply with the provisions of Section 72 of the POPIA.

11.7.2. As and when it may become necessary for Thomson Wilks to transfer personal information it shall fully ensure compliance with the provisions of POPIA.

11.8. Incidents and Security Breach

11.8.1. Thomson Wilks has a policy and procedure in place (Incident and Breach Policy) which is rigidly followed if a breach or incident involving personal data is discovered. Our response procedure for handling of information security incidents includes the notification time scales to the relevant supervisory authorities and affected data subjects in accordance with the POPIA.

11.8.2. We take cognisance of the fact that in terms of the provisions of POPIA any person convicted of an offence is liable, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment.

12. SCHEDULE OF RECORDS

Records	Subject	Availability
Public Affairs	Services information	www.thomsonwilks.co.za
	Public Corporate Records	www.cipc.org.za
	Media Releases	www.thomsonwilks.co.za
Financial	Financial statements	Request in terms of PAIA
	Financial and Tax records – company and employees	Request in terms of PAIA
	Asset register	Request in terms of PAIA
	Management Accounts	Request in terms of PAIA

Marketing	Market Information and strategies	Request in terms of PAIA
	Customer Database	Request in terms of PAIA

13. REQUEST FOR PERSONAL INFORMATION

13.1. Data subjects have the right to:

13.1.1. request what personal information Thomson Wilks holds on them and why;

13.1.2. request access to their personal information;

13.1.3. be informed how to keep their personal information up to date.

13.2. To facilitate the processing of your access to information request, kindly:

13.3. Use the prescribed form, available from the Deputy Information Officer and on the website of Thomson Wilks at www.thomsonwilks.co.za.

13.4. Address your request to the Deputy Information Officer on keri@thomsonwilks.co.za.

13.5. Once the completed form is received, the Deputy Information Officer will verify the identity of the data subject prior to handing over any personal information.

13.6. All requests will be processed and considered against Thomson Wilks' POPIA Policy. The Deputy Information officer will process all requests within a reasonable time.

14. POPIA COMPLAINTS PROCEDURE

14.1. Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed on. Thomson Wilks takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

14.1.1. POPIA complaints must be submitted to the organisation in writing. Where so required, the Deputy Information Officer will provide the data subject with a "POPIA Complaint Form".

14.1.2. Where the complaint has been received by any person other than the Deputy Information Officer, that person will ensure that the full details of the complaint reach the Deputy Information Officer within one (1) working day.

14.1.3. The Deputy Information Officer will provide the complainant with a written acknowledgement of the receipt of the complaint within two (2) working days.

14.1.4. The Deputy Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Deputy Information Officer will endeavour to resolve the complain in a fair manner and in accordance with the principles outlines in POPIA.

14.1.5. The Deputy Information Officer must also determine whether the complaint relates to an error or a breach of confidentiality that has occurred and which may have a wider impact on Thomson Wilks' data subjects.

14.1.6. Where the Deputy Information Officer has reason to believe that the personal information of the data subjects has been accessed or acquired by an unauthorised person, the Deputy Information Officer will consult with Thomson Wilks' Management Committee whereafter the affected data subjects, and the Information Regulator will be informed of this breach.

14.1.7. The Deputy Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Deputy Information Officer and/or the Management Committee of Thomson Wilks within seven (7) working days of receipt of the complaint. In all instances, Thomson Wilks will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

14.1.8. The Deputy Information Officer response to the data subject may comprise of any, or all of, the following:

14.1.8.1. a suggested remedy for the complaint;

14.1.8.2. a dismissal of the complaint and reasons for the dismissal thereof;

14.1.8.3. 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 Deputy Information Officer suggested remedies, the data subject has a right to complain to the Information Regulator.

14.1.10. The Deputy 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 reasons for any complaint will also be reviewed to ensure avoidance of repeat occurrences of complaints.

15. EMPLOYEE CONSEQUENCES OF NON-COMPLIANCE

15.1. Any employee of Thomson Wilks Inc. who fails to comply with the provisions of the POPI Act, its Regulations and this Policy Document, whether through negligence or intent, will be formally disciplined in accordance with our disciplinary policy and procedure.

15.2. If it is found, during the hearing, that the contravention was committed through gross negligence or intent, and that this placed Thomson Wilks Inc. or its employees at risk of being given administrative sanctions and penalties, and found liable in terms the POPI Act, such a person shall be dismissed.

16. CONSULTANT CONSEQUENCES OF NON-COMPLIANCE

16.1. Any consultant of Thomson Wilks Inc. who fails to comply with the provisions of the POPI Act, its Regulations and this Policy Document, whether through negligence or intent, will be duly consulted to investigate why such provisions were not complied with.

16.2. If it is found, during the consultation process, that the contravention was committed through gross negligence or intent, and that this placed Thomson Wilks Inc. or its employees at risk of being given administrative sanctions and penalties, and found liable in terms the POPI Act, such a person shall be in breach of the consultancy agreement.

17. DUTY TO MAINTAIN RECORDS

17.1. In keeping with the POPI Act, Thomson Wilks Inc. will ensure that all personal records of data subjects in a safe and secure environment to prevent breaches of the requirements of the POPI Act.

17.1.1. Soft / Electronic Records

17.1.1.1. All IT infrastructure is maintained by an external provider, being Peter Stevenson (PS Computers), who is duly qualified and experienced in ensuring Thomson Wilks complies with this POPIA Manual.

17.1.1.2. IT local security is managed through local anti-virus and anti-ransomware software along with standard built-in Windows Firewalls and Internet Gateways, PS Computers also monitors WAN connections and connection attempts in correlation with BitCo Telecoms, our ISP in Sandton, who provide and monitor the firewall full-time.

17.1.1.3. Access to server room is strictly for authorised personnel only. Passwords and access credentials to servers are not shared with any service provider other than PS Computers and all passwords and network information sheets are held securely by the office manager.

17.1.1.4. Data backups are done daily and can be recovered immediately and cloud backups are done in real-time.

17.1.2. Physical / Hard Copy Records

18. DUTY TO REPORT

Thomson Wilks has a duty to report breaches, or suspected breaches to the Information Regulator. These breaches may occur without the data subject's knowledge, and without having been brought to Thomson Wilks' attention through a complaint. The duty to report however remains, and is on each and every employee of Thomson Wilks. Thomson Wilks takes all complaints very seriously.

19. POPIA AUDIT

19.1. Thomson Wilks' Deputy Information Officer will schedule periodic POPIA Audits. The purpose of the audit is to:

.

19.1.1. identify the process used to collect, record, store, disseminate and destroy personal information;

19.1.2. determine the flow of personal information throughout Thomson Wilks, including the various divisions, branches and other related organisations;

19.1.3. redefine the purpose for gathering and processing personal information;

19.1.4. ensure that the processing parameters are still adequately limited;

19.1.5. ensure that the new data subjects are made aware of the processing of their personal information;

19.1.6. re-establish the rationale for any further processing where information is received via a third party;

19.1.7. verify the quality and security of personal information;

19.1.8. monitor the extent of compliance with POPIA and this policy;

19.1.9. monitor the effectiveness of internal controls established to manage Thomson Wilks' POPI related risk.

19.2. In performing the POPIA Audit, Information Officers and the Deputy Information Officer will liaise with Management Committee and division heads in order to identify areas within Thomson Wilks' operation that are most vulnerable or susceptible to the unlawful processing of personal information. Deputy Information Officers and the Information Officer will be permitted direct access to and have demonstrable support from line managers and the organisations Management Committee in performing their duties.

20. DUTY TO TRAIN EMPLOYEES

20.1. Thomson Wilks Inc. will provide ongoing training to all its employees to enable them to comply with the provisions of the POPI Act, as amended and the Policy Manuals and implementation as it may apply to them.

20.2. Training will be conducted as follows:

20.2.1. New Permanent Staff/Consultants: Thomson Wilks Inc. will ensure that every new employee receives POPI training and refresher POPI training within sixty (60) days after their appointment.

20.2.2. Existing employees: All other employees must receive refresher POPI Training on an annual basis by completing the internal POPI course. Certificates of completion will be issued by the Deputy Information Officer for recordkeeping.

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

Please submit the completed form to the Deputy Information officer:

Name	Keri Caitlin Soldo
Contact Number	011 784 8984
Email address:	keri@thomsonwilks.co.za

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.

Particulars of data subject	
Name and Surname:	
Identity Number:	
Postal address:	
Contact number:	
Email address:	

Request

I request the organisation to: (circle selection)

1. Inform me whether it holds any of my personal information
2. provide me with a record or description of my personal information
3. correct or update my personal information
4. destroy or delete a record of my personal information

Instructions:

Signature

_____ _____

Signature Date

ANNEXURE B: POPIA 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 Deputy Information Officer:

Name	Keri Caitlin Soldo
Contact Number	011 784 8984
Email address:	keri@thomsonwilks.co.za

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

Address:	Braampark Forum 3, 3rd Floor 33 Hoofd Street, Braampark Office Park
Postal Address:	PO Box 31533, Braamfontein, 2017
Telephone:	010 023 5200

Particulars of complainant	
Name and Surname:	
Identity Number:	
Postal address:	
Contact number:	
Email address:	

Details of complaint:

Desired outcome

Signature	
_____ Signature	_____ Date

ANNEXURE C: POPIA NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be hesitant about disclosing it. Your privacy is of the utmost importance to us and we are committed to safeguarding it and only processing your information in a lawful manner.

We want to ensure 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 the correct manner, or that your information is being used for a purpose other than for what it was originally intended, you are more than welcome to contact our Deputy Information Officer.

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

Our Deputy Information Officer's contact details:

Name	Keri Caitlin Soldo
Contact Number	011 784 8984
Email address:	keri@thomsonwilks.co.za

Purpose for processing your information:
We collect, hold and use your information mainly to provide you with access to the services we provide. We only process your information for the purpose which you would reasonably expect, including:

a. Providing you with advice, and services to suit your needs as requested
b. Issue action on your behalf in relation to a dispute you have instructed us on
c. Negotiate on your behalf in terms of dispute resolution, or concluding legal agreements
d. To confirm, verify and update your details
e. To comply with any legal and regulatory requirements

Some of your information that we may hold on you may include, your full names, email address, home, postal and physical address, other contact information, your title, birth date, identity number, gender, income tax details and occupation.

Signature	
_____	_____
Signature	Date

ANNEXURE D: STAFF AND CONSULTANT DECLARATION, CONSENT AND CONFIDENTIALITY CLAUSE

1. I hereby confirm that the POPI Act and this policy manual has been made available to me and training has been conducted. I confirm that I will comply with the requirements of this manual and understand that non-compliance might result in disciplinary action.

2. I confirm and understand that my responsibilities in terms of this manual include (but are not limited to remaining in compliance with the "Processing Principles and Conditions".

3. Immediately notifying the Deputy Information Officer of any breach, or suspected breach in personal information of any of Thomson Wilks' data subjects.

4. Immediately notifying the Deputy Information Officer of any complaint by a data subject against Thomson Wilks.

5. 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 education or 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, biometric information of the person; the personal views, opinions 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.

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

7. 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 employers relevant policy available to the employee on request and only to the extent that 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.

8. 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:
   - 8.1. That he/she is notified of the purposes 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.
   - 8.2. That he/she consents and authorizes 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.
   - 8.3. Without degrading from the generality of the aforesaid, the employee consents to the employer's collection and processing of 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.
   - 8.4. To make available to the employer all necessary PI required by the employer for the purposes of securing and furthering facilitating the employee's employment with the employer.

8.5. To absolve the employer from any liability in items of POPIA from 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.

8.6. 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.

8.7. 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.

8.8. the employee authorizes 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.

8.9. 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 with treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

8.10. 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 the appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

8.11. Employees may not directly or indirectly, utilize, disclose or make public in any manner to any person or third party, either within the organization 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.

This done and signed on this _____ day of _____20_____

_____ _____

Name Signature

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

1. "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 options, views or preferences of the person; correspondence sent by the person implicitly or explicitly of a private or confidential nature of 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.

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

3. 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.

4. The parties agree that they will at all times comply with the POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

5. The parties agree that is shall put in place, and at all times maintain, appropriate physical, technologies and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorized individuals comes into contact with pursuant to this agreement.

6. 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.

ANNEXURE F: CHECKLIST IDENTIFYING PERSONAL INFORMATION

Information is regarded as personal information if you tick/check any of the following questions

NUMBER	INFORMATION	COMMENT	CHECK
	NAMES Does the information include the name of a natural or juristic person? If "yes" does the name appear with other personal information or does the disclosure of the name itself reveal information relating to that person		
	IDENTIFIERS Does the information include an identifying number or symbol? This includes for example identity numbers or passport numbers.		
	Does the information include an online identifier i.e., a trace left by the online activities of a data subject		
	CONTACT DETAILS Does the information include contact details? This includes: • Telephone numbers; • Email addresses • Physical addresses ; and • Location details		
	DEMOGRAPHICS Does the information include demographic details? This includes: • Race • Gender • Colour • Age • Culture • Language or national, ethnic or social origin		
	GENDER AND SEXUALITY Does the information include details relating to gender or sexuality. This includes: • Gender • Sex • Sexual orientation • Pregnancy • Marital status		
	HEALTH Does the information include details relating to health? This includes: • Physical / mental health and wellbeing • Disabilities		
	BIOMETRICS Does the information include biometrical information? this includes: • Blood type; • DNA Analysis; • Retinal scanning; • Fingerprint scanning; • Voice recognitions		
	HISTORY Does the information include details on the person's educational, financial or employment history?		

ANNEXURE G: DIRECTOR ACCOUNTABILITY

The Directors hereby accept ownership, accountability and responsibility for compliance with the POPI Act, as amended and hereby approves this version of the manual by signing in the table below.

Name	Capacity	Date	Signature
Stephen Thomson	Director		
Tumisang Kgaboesele	Director		
Anel Bestbier	Director		
David Dewar	Director		