Protection of Personal Information Act (POPIA) 4 of 2013 Policy

for De Morgenzon Proprietary Limited

("De Morgenzon")

(Registration number: 2021/351879/07)

1. SUMMARY OF POPIA AND IMPORTANT CONCEPTS

Section 14 of the Constitution of the Republic of South Africa, 1996 provides that everyone has the right to privacy. POPIA protects individuals against the unlawful collection, retention, transfer and use of their personal information and aims to ensure that the processing of personal information does not infringe the right to privacy of the data subject.

Important concepts are defined in Section 1 of the Act:

"Data subject" means to whom the personal information relates. In this case it will be our client (you).

"Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) 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;

(g) the views or opinions of another individual about the person; and

(h) 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.

De Morgenzon may process the above personal information of a data subject.

"Process" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information.

"**responsible party**" is defined as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing information. In this case it will be **De Morgenzon.**

2. CONFIDENTIALITY OF PERSONAL AND BUSINESS INFORMATION

De Morgenzon undertakes to take reasonable steps to keep the data subject's personal and business information, held by us, safe and confidential; that the data subject's information will be processed lawfully and in a reasonable manner; to keep it only for a specified and explicit lawful purpose; to process it only in ways compatible with the purpose for which it was given initially; to keep data accurate, to not retain it for a period longer than is necessary for the specified purpose and we will also provide a copy of personal information to the data subject, on request.

You should acknowledge that any personal and business information supplied to us is accurate and may be processed by us in the context of the Protection of Personal Information Act. In terms of Section 29 of the Financial Intelligence Centre Act we are required by law to report certain suspicions or unusual transactions of which we come aware to the Financial Intelligence Centre. This statutory requirement, which applies to both prospective clients and existing clients, override the professional ethics rules of confidentiality, which we observe. This clause shall not apply when confidential information enters the public domain or when we are required to disclose it to our insurers, legal advisors or under legal obligation.

3. INFORMATION PROTECTION OFFICER

POPIA requires that an Information Protection Officer be appointed. Alastair Robert Rimmer is the Information Protection Officer for **De Morgenzon**. You can contact him at alastair@demorgenzon.com.

The duties of the Information Protection Officer are set out in Section 55(1) of the Act, that reads:

(1) Each responsible party must ensure that there are, within that body, one or more information protection officers whose responsibilities include –

(a) the encouragement of compliance, by the body, with the information protection principles;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Commission in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body;

(d) otherwise ensuring compliance by the body with the provisions of this Act.

Liability of Information Officers

Nature of offence and penalty:

1. **Offence: Section 90(1) of PAIA:** A person (including an information officer) who, with intent to deny a right of access in terms of this Act:

   a) destroys, damages or alters a record;

   b) conceals a record; or

   c) falsifies a record or makes a false record

- **Penalty:** a fine or imprisonment for a period not exceeding 2 years.

2. **Offence: Section 90(2) of PAIA:** The Information Officer who wilfully or in a grossly negligent manner fails to comply with the provisions of section 14 of PAIA.

- **Penalty**: a fine or imprisonment for a period not exceeding 2 years.

3. **Offence: Section 90(3) of PAIA:** The head of a private body who, wilfully or in a grossly negligent manner, fails to comply with the provisions of section 51 of PAIA.

- **Penalty:** a fine or imprisonment for a period not exceeding 2 years.

4. **Offence: Section 77K of PAIA:** Non-compliance with an Enforcement Notice.

- **Penalty:** a fine or imprisonment for a period not exceeding 2 years.

4. THE OPERATOR

The operator is the party that performs the actual processing of your (the data subject's) personal information on behalf of us.

If we appoint an operator then we:

- retain ultimate accountability for an operator when acting in terms of the agreement/mandate;
- must ensure that an operator only processes the information furnished to it with the knowledge or authorisation of us, must treat personal information which comes to their knowledge as confidential and must not disclose it to others (unless required by law or in the course of the proper performance of their duties);
- must, in terms of a written contract between us and the operator, ensure that the operator which processes personal information for us, establishes and maintains the security measures as prescribed under POPIA.

Duties of the operator

POPIA prescribes that an operator must notify us immediately where there are reasonable grounds to believe that your personal information has been accessed or acquired by any unauthorised person.

5. EXCLUSIONS

If the information that has been processed does not fall within the definition of personal information, it is excluded from POPIA and the processing of the information may proceed without compliance with POPIA.

<u>The following types of processing are excluded, namely information:</u>

- processed for purely personal or household activity;
- that has been de-identified (if the information which links it to a specific data subject has been deleted or the link between a data subject and their personal information has been broken to such an extent that someone cannot link the information back to

the relevant data subject again. An example would be a medical report without the name or any contact detail of the person to whom it relates);

- processed on behalf of the State or used by the Cabinet, Executive Council of a province and any municipality;
- processed for investigation and prosecution of criminal matters;
- used exclusively for journalistic purposes;
- required for the judicial functions of courts, and/or
- which is exempted by the Regulator (in terms of section 34 of POPI).

6. INFORMATION PROTECTION PRINCIPLES

You have a number of rights in terms of POPIA, which **De Morgenzon** must be aware of. The staff of **De Morgenzon** will be educated on the principles of POPIA and the information Protection Officer will be aware of the personal information that is being held.

How **De Morgenzon** will implement the information protection principles in POPIA:

1. **De Morgenzon** may not store personal information about anyone else without getting your direct consent.
2. You may request to review any personal information stored about you at any time and **De Morgenzon** may not withhold such information.
3. You may request for corrections to be made to erroneous information and **De Morgenzon** will be obliged to make such corrections.
4. No Personal Information may be disclosed to any person without your direct authorisation. A breach in this regard will be considered a serious and punishable offence.
5. **De Morgenzon** may not make alterations or changes of any nature to the personal information or data kept on you, without your direct authorisation.
6. **De Morgenzon** may not release data to any person resulting in your distinctive identification for the purposes of research, statistics or any other similar purpose.

7. HOW DE MORGENZON WILL COLLECT YOUR DATA

We may collect personal data in a number of ways, for example: from the information you provide to us when meeting with one of our employees, when you communicate with us by telephone, email or other forms of electronic communication (in this respect, we may

monitor, record and store any such communication), when you complete or we complete on your behalf client or employee on-boarding application or other forms, from publicly available sources or third parties where we need to conduct background checks about you.

We will process your personal information in line with the following conditions:

Processing condition 1: accountability

- We ensure that the conditions set out in POPIA, and all 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.

Processing condition 2: processing limitation

- The information we collect is not excessive, legally justifiable, and is not collected from third parties without good reason.
- There are six justification grounds in order to lawfully process personal information:
    1. when we get your consent;
    2. where processing is necessary to carry out actions for the conclusion or performance of a contract to which you are party;
    3. processing complies with an obligation imposed by law on us;
    4. processing protects your legitimate interest;
    5. processing is necessary for pursuing our legitimate interests or those of a third party to whom the information is supplied; or
    6. processing is necessary for the proper performance of a public law duty by a public body.

Processing condition 3: purpose specification

- Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of us.
- Retention records of personal information is retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.

Processing condition 4: further processing limitation

- further processing is in accordance or compatible with the purpose for which personal information is collected.
- Further processing is allowed:
    - where you have consented to the further processing of the information; or
    - where the information is used for historical, statistical or research purposes and we ensure that the processing is carried out solely for such purposes and will not be published in an identifiable form.

Processing condition 5: information quality

We take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

Processing condition 6: openness

- Documentation
    - PAIA Manual - which you can find on our website (www.demorgenzon.com)
    - POPIA Manual – which you can find on our website (www.demorgenzon.com)
- Notification to a data subject
    - We take reasonably practicable steps to ensure that you are aware of:
        - the information being collected;
        - the source from which it is collected, if not collected from you itself
        - Our name and address;
        - whether or not the supply of the information by you are voluntary or mandatory;
        - the consequences of failure to provide the information;
        - any particular law authorising or requiring the collection of the information;
        - any intended transborder transfers;
        - any further information 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 you to be reasonable.

Processing condition 7: security safeguards

We secure the integrity and confidentiality of personal information in our possession or under our control by taking appropriate, reasonable technical and organisational measures to prevent-

- loss of, damage to or unauthorised destruction of personal information; and
- unlawful access to or processing of personal information.

In order to give effect to this we take reasonable measures to-

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;
- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

Processing condition 8: data subject participation

Your rights under POPIA are recognised by us:

- the right to confirmation;
- the right to access;
- the right to correction, destruction or deletion; and
- the right to objection

8. HOW DE MORGENZON WILL PROCESS YOUR DATA OTHER

THAN WITH YOUR CONSENT, HOW WE USE THAT DATA AND WHO WE SHARE IT WITH

- We may process your personal data because it is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract.
- Complies with an obligation imposed by law on us.
- Protects your legitimate interest.
- Is necessary for pursuing our legitimate interests or those of a third party to whom the information was supplied.

9. DATA TRANSFERS OF PERSONAL INFORMATION

De Morgenzon should adhere to the following –

1. Make use of secure online channels.
2. Make use of strong passwords.
3. Make use of a secure email that will encrypt the data.
4. A written agreement should be put in place before data will be transferred to a third party. The agreement with the third party should set out the purpose for the required information.

10. THE REGULATOR FOR DATA PROTECTION

POPIA introduces and provides for the establishment of an independent supervisory authority, the Information Regulator. It is specifically tasked with the duty to monitor and police compliance with the data protection provisions contained in POPIA.

10.1 SUBMITTING COMPLAINTS TO THE REGULATOR

Any person (you, as our client) may, either orally or in writing submit a complaint to the Information Regulator in the event of alleged interference with their rights to privacy.

After receipt of a complaint, the Information Regulator is obliged to investigate the complaint, act as a conciliator where appropriate and take further action as contemplated by POPIA. In exercising its investigative powers, the Information Regulator may, amongst other things:

- summon and enforce the appearance of persons;
- compel the provision of written or oral evidence under oath;
- receive evidence irrespective of whether such evidence is admissible in a court of law; and
- enter and search any premises occupied by a us.

Where necessary, the Information Regulator may apply to a judge of the High Court or a magistrate to issue a warrant to enable the Information Regulator to enter and search premises.

11. SPECIAL NOTIFICATION/REGISTRATION REQUIREMENTS

No registration or notification requirements for the processing of personal information are prescribed by POPIA other than prior authorisation with regard to certain limited categories

of processing under Section 57 of POPIA which relates to the cross-border transfer of special personal information or personal information concerning children.

12. STEPS DE MORGENZON MUST IMPLEMENT TO BECOME COMPLIANT AND MARKETING

13.1 WHAT COMPLIANCE WILL BE REQUIRED OF DE MORGENZON.

- **Our information officer's role:** An information Officer is registered in line with POPIA.
- **Buy-in and staff training:** In order to ensure effective compliance, buy-in from senior management all the way down the chain of command is needed. Employees will be informed of what data privacy is about and what their duties are in terms of POPIA.
- **Find the personal information in our agency:** We will do a self-check/GAP analysis/ impact assessment. We will perform a detailed check on when and how information is collected, how it is stored and used and ultimately deleted or destroyed and whether it was collected with the necessary consent or otherwise obtained lawfully where consent is not required. Once such a "self-audit" is completed, there should be a clear understanding of how data is being processed in our agency. Gaps and risks should become identifiable.
- **Design a practicable compliance framework, which usually include identified processes and policies**: A proper gap analysis will help identify which processes and policies have to be put in place. These often include:
    - updates to employment contracts
    - updates to supplier agreements
    - changes to marketing practices
    - implementation of policies such as privacy policy, data breach policy, data subject record access request policy, employee device policy, and so forth.
- **Implementation:** The compliance framework should be implemented, monitored and maintained. Policies and procedures do nothing to aid compliance if they are not properly implemented.

13. EMPLOYEES AND EMPLOYMENT CONTRACTS

Refer to our *'Employment Contracts and POPIA'* document.

The general provisions under POPIA will apply equally to any personal information and special personal information processed as part of a data subject's employment. POPIA does specifically include a data subject's employment history within the definition of personal information. This means that POPIA applies to the collection and use of personal information of prospective employees, current employees and past employees, as well as the monitoring employees' email, internet access, location data and the video surveillance of employees in the employment context.

We must ensure:

- lawful justification for the processing of personal information;
- the personal information being processed must be relevant, adequate and not excessive having regard to the purpose for which it is processed;
- the employee must be notified of the purposes of collection and processing of personal information, and the employer must consider each employees' right to access, modification and erasure in light of POPIA requirements.

It is further advisable to include provisions in the employment contract recording the employee's obligation to adhere to the privacy policies of the employer, both with regard to the private information of the employer and the private information of clients and service providers that the employee may come in contact with in the course of his/her employment.

De Morgenzon will also make every effort to maintain awareness of compliance with the privacy policies of the employer by way of regular training/updates of employees on the requirements of the Act and the employer's own policies.

14. EFFECT ON CERTAIN MARKETING PROCEDURES

14.1 DIRECT MARKETING

Electronic direct marketing and consent

According to POPIA, direct marketing is electronic communication that is directed at an individual or entity and which promotes or offers to supply any goods or services. Examples include emails, SMS messages, messages sent via social media platforms directly to a specific

individual and advertising sent to a custom audience via social media platforms (ie, where it is known who the recipients are).

Once categorised as (electronic) direct marketing, we must ascertain whether an opt-in consent must be obtained. There are two scenarios.

- If this is a **first approach** to the person, consent must be obtained for any unsolicited (ie, that person did not ask for it) marketing to that person. In other words, where we want to contact a person for the first time with marketing communication which was not requested (unsolicited), we must obtain consent before sending electronic marketing to individuals. We may approach someone for direct marketing consent once only, and provided that they have not withheld consent previously. There is a form (Form 4) in the Regulations to POPIA that sets out an example of such a consent. We may use it as is, or choose to adapt it and make it more attractive than the legislature's attempt (whilst making sure the necessary information is contained therein so that the person knows at all times what marketing he is consenting to and from whom it will be received).
- **On the other hand**, when it comes to contacting our existing customers, there are three criteria that need to be met before we can start marketing to them directly:
    1. If the client's contact information was obtained in the context of a rendering a service;
    2. If we want to inform that client of similar offerings;
    3. If the client is given opportunities to refuse the direct marketing, both at the time the information is collected and every time marketing is directed to him/her. Marketing to that client will generally be in order provided an opt-out option appears in each electronic marketing message.

We must further manage our own client databases effectively and keep records of where, how and when the personal information was initially obtained; whether the person is an existing customer and, if so, in respect of what products or services; whether the person has consented to receiving direct marketing; and whether the person has unsubscribed from receiving direct marketing.

It is advisable therefore to:

- use bulk email and SMS software that keeps track of opt-in and opt out information and automatically includes an automatic opt out on each message sent to existing clients and others that have opted-in to receive marketing; and to
- ask people directly if they may be added to the agency's database.

Cold calling

As mentioned before, **De Morgenzon** may not without consent send unsolicited SMS's or automated calls, as these fall within the definition of direct marketing in POPIA. We may still do cold calling though, as this is a personal (not electronic) way of direct marketing and therefore not prohibited by the provisions of POPIA. The recipient of the call may ask **De Morgenzon** to stop contacting him or her, and this must then be adhered to. However, where **De Morgenzon** uses lists purchased from a lead generation business, the position is trickier, as we will have to obtain confirmation from the lists provider that the records have been obtained and stored in a way that is compliant with POPIA and that consent is in place, as indicated above. That is generally difficult, as this was not the practice in the past to record the additional detail or to obtain consent. When obtaining these records, it will be advisable for **De Morgenzon** to obtain confirmation from the provider of the records, that the data provided has been obtained and recorded in a way that is POPIA compliant.

15. FURTHER COMPLIANCE CONSIDERATIONS

15.1 DATA BREACH NOTIFICATION

Where there are reasonable grounds to believe that your personal information has been accessed or acquired by an unauthorised person, **De Morgenzon** or any third-party processing personal information on instruction from **De Morgenzon** (the operator), must notify you and the Information Regulator. (Take note: Notice to the data subject is not required if the identity of the data subject cannot be established as a result of the breach, in the hands of the recipient.)

Notification to you (the data subject) must be:

- made as soon as reasonably possible after the discovery of the breach;
- sufficiently detailed;

- in writing; and
- communicated to you by mail to your last known physical or postal address; or by email to your last known email address; or by placement in a prominent position on our website; or by publication in the news media; or as may be directed by the Information Regulator.

15.2 SANCTIONS

It has been noted above that the Information Regulator is responsible for the investigation and enforcement of POPIA. A person contravenes the provisions of POPIA if he/she:

- hinders, obstructs or unlawfully influences the Information Regulator;
- fails to comply with an information or enforcement notice;
- gives false evidence before the Information Regulator on any matter after having been sworn in or having made an affirmation;
- contravenes the conditions;
- knowingly or recklessly, without our consent obtains, discloses, or procures the disclosure, sell, or offers to sell your details to another person; and will be guilty of an offence.

Contravention of POPIA could result in far-reaching sanctions, these include the imposition of fines up to R10 million, imprisonment for a period of 12 months to 10 years and/or a damage claim by you.

15.3 DATA RETENTION

In terms 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.

<u>Unless:</u>

- Retention of the record is required or authorised by law (as in the Companies Act 71 of 2008);
- **De Morgenzon** reasonably requires the record for lawful purposes related to its functions or activities;
- Retention of the record is required by a contract between the parties thereto; or

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

If De Morgenzon has used a record of personal information of a data subject to make a decision about the data subject, we must—

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

When must De Morgenzon 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 the above. The destruction or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible form.

De Morgenzon must restrict processing of personal information if—

1. its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;
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;
3. the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or
4. the data subject requests to transmit the personal data into another automated processing system.

The above personal information 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.

Where processing of personal information is restricted in accordance with the above, the responsible party must inform the data subject before lifting the restriction on processing.

15.4 DATA TRANSFERS AND OUTSOURCING

POPIA provides that **De Morgenzon** may not transfer personal information about a data subject to a third party in a foreign jurisdiction unless:

- the recipient is subject to a law or contract which: upholds principles of reasonable processing of the information that are substantially similar to the principles contained in POPIA;
- includes provisions that are substantially similar to those contained in POPIA relating to the further transfer of personal information from the recipient to third parties;
- you consent to the transfer;
- the transfer is necessary for the performance of a contract between you and us, or for the implementation of pre-contractual measures taken in response to your request;
- the transfer is necessary for the conclusion or performance of a contract concluded in your interest between us and a third party; or
- the transfer is for your benefit and it is not reasonably practicable to obtain your consent to that transfer; and if it were reasonably practicable to obtain such consent, you would be likely to give it.

16. DATA SUBJECT ACCESS REQUEST POLICY

If the Data subject (you) wants **De Morgenzon** to confirm that we are holding personal information about you; wants a description of the information or wants to correct such personal information held, the following process, set out in the below sections, should be followed.

16.1 THE PROCESS TO REQUEST FOR ACCESS AND CHANGES TO PERSONAL INFORMATION UNDER POPIA

Section 23 of the POPIA states that a data subject may request a responsible party to confirm that they are holding personal information about the data subject and may obtain a description of that information and details about who has had access to it. Where such a request is received, the matter must be referred to the Information Protection Officer who will ensure that the correct procedures are adopted.

Section 24 of the POPIA, provides for a right to request correction of personal information held by a responsible party if it is inaccurate, incomplete, misleading, out of date, and

obtained unlawfully, irrelevant or excessive. Where such a request is received, the matter must be referred to the Information Protection Officer who will ensure that the correct procedures are adopted.

Section 23 states that:

1. "A data subject, having provided adequate proof of identity, has the right to—
    1. request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and
    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—
        1. within a reasonable time;
        2. at a prescribed fee, if any;
        3. in a reasonable manner and format; and
        4. in a form that is generally understandable.
2. If, in response to a request in terms of subsection (1), personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.
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 subsection (1)(b) to enable the responsible party to respond to a request, the responsible party—
    1. must give the applicant a written estimate of the fee before providing the services; and
    2. may require the applicant to pay a deposit for all or part of the fee.
4. A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (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 apply.

5. The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.
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 subsection (4)(a), every other part must be disclosed."

Section 24 states that:

1. "A data subject may, in the prescribed manner, request a responsible party to—
    a) 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
    b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14.
2. On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable—
    a) correct the information;
    b) destroy or delete the information;
    c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or
    d) 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.
3. If the responsible party has taken steps under subsection (2) 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.

4. The responsible party must notify a data subject, who has made a request in terms of subsection (1), of the action taken as a result of the request.

Section 25, regulates the manner of access to information, and reads as follow:

The provisions of sections **18** and **53** of the Promotion of Access to Information Act apply to requests made in terms of section **23** of this Act.

Section 18, regulates the Notification to Data subject when collecting personal information, and reads as follow:

1. If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—
    a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;
    b) the name and address of the responsible party;
    c) the purpose for which the information is being collected;
    d) whether or not the supply of the information by that data subject is voluntary or mandatory;
    e) the consequences of failure to provide the information;
    f) any particular law authorising or requiring the collection of the information;
    g) 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;
    h) any further information such as the—
        i. recipient or category of recipients of the information;
        ii. nature or category of the information;
        iii. existence of the right of access to and the right to rectify the information collected;
        iv. existence of the right to object to the processing of personal information as referred to in section 11(3); and

v. right to lodge a complaint to the Information Regulator and the contact details of the Information 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.

2. The steps referred to in subsection (1) must be taken—
    a) 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
    b) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.
3. A responsible party that has previously taken the steps referred to in subsection (1) complies with subsection (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.
4. It is not necessary for a responsible party to comply with subsection (1) if—
    a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;
    b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;
    c) non-compliance is necessary—
        i. to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
        ii. 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 (Act No. 34 of 1997);

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

iv. in the interests of national security;

d) compliance would prejudice a lawful purpose of the collection;

e) compliance is not reasonably practicable in the circumstances of the particular case; or

f) the information will—

i. not be used in a form in which the data subject may be identified; or

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

Section 53, regulates the protection of the Regulator, and states:

Any person acting on behalf or under the direction of the Regulator, is not civilly or criminally liable for anything done in good faith in the exercise or performance or purported exercise or performance of any power, duty or function of the Regulator in terms of this Act or the Promotion of Access to Information Act.

17. CONCLUSION

POPIA requires **De Morgenzon** to establish appropriate policies and procedures to protect the various forms of personal information that are part of their business operations. Strict adherence to this Policy together with the awareness of all staff will ensure that the company complies with the relevant legislation and safeguards the personal information entrusted to them.