POPI - DATA PRIVACY POLICY

INDEX

		Page
1.	Definitions	2
2.	Introduction	3
3.	Objective	4
4.	POPIA Core Principles	4
5.	Consent	5
6.	Collection, Processing and Sharing of Information	5
7.	Storage of Information	6
8.	Disposal of Data Subjects' Information	6
9.	Internet and Cyber Technology	6
10.	Third Party Operators	9
11.	Banking Details	9
12.	Direct Marketing	9
13.	Data Classification	9
14.	Rights of the Data Subject – Form 1 & 2 Attached	10
15.	Information Officer	11
16.	GDPR	12
17.	Availability and Revision	13
	ANNEXURES Form 1: Objection to Processing Form 2: Request for Correction or Deletion Form 3: Consent of a Data Subject	 14 16 18

1. DEFINITIONS

"biometrics": means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

"**child**": means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.

"competent person": means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

"data subject": means the person to whom personal information relates and for the purposes of THE FIRM, this will include but not be limited to – sellers and buyers of properties, the banks in respect of mortgage bonds and other legal services rendered to the banks, commercial, litigation and other general clients, employees, external service suppliers and all associates of THE FIRM.

"direct marketing": means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – a) Promoting or offering to supply, in the ordinary course of business of THE FIRM, legal services to the data subject; or b) Requesting the data subject to make a donation of any kind for any reason.

"electronic communication": means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

"filing system": means any structured set of personal information which in the case of THE FIRM consist of physical files kept in the offices of THE FIRM together with the data filed on the various software systems used by THE FIRM.

"**THE FIRM"**: for purposes of this Policy document means the law firm registered as MEISE NKAISENG INCORPORATED, a limited personal liability company registered with the Companies and Intellectual Property Commission (CIPC) under registration number 1999/004176/21, with two offices situated at:

- 1 Fish River Street, Vanderbijlpark; and
- 153 General Hertzog Road, Vereeniging.

"Information officer": of THE FIRM will mean STEVEN MEISE.

"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.

"person": means a natural person or a juristic person.

"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: Information relating to the education or the medical, financial, criminal or employment history of the person; Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person; The biometric information of the person; The personal opinions, views or preferences of the person; Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature; The views or opinions of another individual about the person; and 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.

''private body'' means—(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity; (b) a partnership which carries or has carried on any trade, business or profession; or (c) any former or existing juristic person but excludes a public body**.**

"processing": 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.

"Promotion of Access to Information Act": means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000).

"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.

"record": means any recorded information – a) Regardless of form or medium, including any of the following: I. Writing on any material; II. Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; IV. Book, map, plan, graph, or drawing; V. Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; b) In the possession or under the control of a responsible party; and c) Regardless of when it came into existence.

"Regulator": – means the Information Regulator established in terms of Section 39 of the POPIA.

"responsible party": means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

"restriction": means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

"special personal information": means personal information as referred to in Section 26 of the POPIA which includes 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.

"this Act": means the Protection of Personal Information Act, No. 4 of 2013.

"unique identifier": means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2. INTRODUCTION

THE FIRM is an established law practice with offices in Vanderbijlpark and Vereeniging which service clients throughout the Republic of South Africa as well as various international destinations.

THE FIRM deals with many role players in the various fields of law and acknowledges that, in performing its business operations it is necessary to obtain client personal information as required by statute, often collects personal information of counter parties in respect of legal transactions administered by THE FIRM and collects personal information of other attorneys and professionals.

THE FIRM acknowledges that most of its communications are done electronically via the internet, per email and other electronic methods. In recognizing the international risk of data breach and also to ensure that lawful conditions exist surrounding its data subjects' information, THE FIRM accepts that all its South African based data subjects' Constitutional Right to Privacy is of utmost importance. THE FIRM further accepts that its data subjects based in other parts of the world are entitled to equal rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based. As such, THE FIRM is committed to comply with South Africa's POPIA.

3. OBJECTIVE

Although it is not possible to ensure 100% mitigation against data breaches, the objective of this Policy is to ensure adherence of THE FIRM to the provisions within POPIA together with its Regulations aimed at protecting THE FIRM's data subjects from harm as extensively as possible by protecting their personal information, to ensure that data subjects' consent is obtained as provided for in POPIA, to ensure that data subjects' information is not unlawfully shared with third parties to stop identity fraud and generally to protect privacy.

This Policy constitutes the EXTERNAL SET OF PRIVACY RULES applicable to the information collected and processed by THE FIRM and sets out the standard for suitable protection of personal information as required by POPIA.

4. POPIA CORE PRINCIPLES

In its quest to ensure the protection of data subjects' privacy, THE FIRM fully commits as follows:

4.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information;

4.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

4.3. To ensure that the requirements of the POPIA legislation are upheld within THE FIRM. In terms of sections 8, 17 and 18 of POPIA, THE FIRM confirms that it adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribes to a process of accountability and openness throughout its operations;

4.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, to collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for its operations and to process the personal information obtained from owners, occupiers, visitors and service suppliers only for the purpose for which it was obtained in the first place;

4.5. To not process personal information obtained from data subjects, clients, employees and service suppliers in an insensitive, derogative, discriminatory or wrongful way that can intrude on the privacy of the particular data subject;

4.6. To allow all data subjects the opportunity to request access to their information as well as correction or deletion of information according to the specifications contained within sections 23 to 25 of POPIA;

4.7. To not request or process information related to race, religion, medical condition, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. THE FIRM will also not process information of children unless the specific consent provisions contained within POPIA have been complied with;

4.8. To ensure that, in terms of the provisions contained within section 16 of POPIA**,** data subjects' information is recorded and retained accurately;

4.9. To not provide any documentation to a third party or service provider without the express consent of the data subject except where it is necessary for the proper execution of the service as expected by the data subject;

4.10. To keep effective record of personal information and not to retain information for a period longer than required;

4.11. To secure the integrity and confidentiality of personal information in its possession in terms of sections 19 to 22 of POPIA.

5. CONSENT

When data subjects' information is collected, processed or shared by THE FIRM during the process of THE FIRM delivering legal services, THE FIRM recognises its obligations to explain the reasons for the collection of information from the data subject/s and to obtain the required consent to process and disseminate the information.

If personal information is used for any other reason than the original reason of it being collected, the specific consent for such purpose must be obtained from the data subject. If special personal information is collected, processed and stored for any reason from any of THE FIRM's data subjects, a specific consent for such collection must first be obtained unless:

5.1. Processing is carried out with a prior consent of the data subject;

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

5.3. Processing is for historical, statistical or research purposes.

6. COLLECTION, PROCESSING AND SHARING OF INFORMATION

THE FIRM collects and processes personal information from its data subjects for a variety of reasons and in a variety of ways. The most pertinent reason for data collection and processing relates to the legal services being performed by THE FIRM. Once personal information is collected by THE FIRM, it is often necessary for such information to be processed and shared with other professional role players involved in the particular legal matter.

The primary method of collecting and processing personal information is electronically. By submitting personal and special personal information details to THE FIRM, all data subjects acknowledge the following:

6.1. Personal information collected by THE FIRM will be collected directly from the data subject, unless-

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

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

6.1.3. Collection of the information from another source is necessary -

- 6.1.3.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
- 6.1.3.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
- 6.1.3.3 For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
- 6.1.3.4 In the interest of national security;
- 6.1.3.5 To maintain the legitimate interests of THE FIRM or the data subject on whose behalf the information is supplied;
- 6.1.3.6 Compliance would prejudice a lawful purpose of the collection;
- 6.1.3.7 Compliance is not reasonably practical in the circumstances of the particular matter.

6.1.4. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of THE FIRM;

6.1.5. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information;

6.2. THE FIRM will take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected and further processed;

When personal and special personal information are collected, processed and shared on behalf of banks for the purposes of THE FIRM registering a mortgage bond or delivering other services on behalf of the bank/s, THE FIRM will ensure that only the required information is collected, processed and shared as required by the bank/s. THE FIRM undertakes to offer a full explanation of the nature of the information being collected, processed and shared in terms of a banking instruction clearly with the affected data subject and will obtain the consent of such data subject where necessary.

7. STORAGE OF INFORMATION

THE FIRM acknowledges the risks facing data subjects with the storage of personal and special personal information on THE FIRM's software systems as well as filing copies of the physical information sheets containing personal information physically in an office. THE FIRM will:

7.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of information;

7.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required;

7.3. Continue to review its internal policies and third-party agreements where necessary to ensure that these also comply with the POPIA and Regulations in line with THE FIRM's Policy rules.

8. DISPOSAL OF DATA SUBJECTS' INFORMATION

8.1 THE FIRM is responsible to ensure that necessary records and documents of data subjects are adequately protected and maintained to ensure that records that are no longer needed or are of no value are securely disposed of at the proper time. These rules apply to all documents which are collected, processed or stored by THE FIRM and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

8.2 THE FIRM adheres to the Guidelines issued by the Law Society of South Africa and the Legal Practice Council and retains documents containing data subjects' personal information for a minimum period of 5 years.

8.3 Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.

8.4 THE FIRM undertakes to ensure that all electrical waste, electronic equipment and data on disk drives be physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.

8.5 THE FIRM will ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.

8.6 In the event that a third party is used for data destruction purposes, the Information Officer will ensure that such third party will also comply with this policy and any other applicable legislation.

8.7 THE FIRM may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, investigations or similar proceedings.

8.8 The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

****** DATA SUBJECTS ARE REFERRED TO THE ANNEXED FORMS 1 AND 2 with regards to requests to amend and delete personal information from THE FIRM's electronic database ******

9 INTERNET AND CYBER TECHNOLOGY

****** THE FIRM has implemented a full internal IT/EMAIL/Cyber Security Policy which has been circulated to all employees. The clauses herein contained constitute a summary of the appropriate IT measures in place and applicable to all employees of THE FIRM******

9.1 **Acceptable use of THE FIRM's Internet Facilities & standard Anti-Virus rules**

The repercussions of misuse of THE FIRM's systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g., computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime.

In order to ensure that THE FIRM's IT systems are not misused, everyone who uses or has access to THE FIRM's systems has received training in order to meet the following five high-level IT Security requirements:

9.1.1 Information will be protected against any unauthorised access as far as possible;

9.1.2 Confidentiality of information will be assured as far as possible;

9.1.3 Integrity of information will be preserved as far as possible;

9.1.4 Availability of information for business processes will be maintained;

9.1.5 Compliance with applicable laws and regulations to which THE FIRM is subject will be ensured by the Information Officer as far as possible.

9.2 **IT Access Control**

The Firm shall ensure that logging into the IT system and software packages is password protected and shall exercise all caution in preventing unauthorised access to the password. Passwords shall be reviewed from time to time but in particular where GOOGLE based products are used and linked (such as Facebook, WhatsApp and GMAIL based domains).

9.3 **THE FIRM's Email Rules**

The Firm acknowledges that most of its communications are conducted via email and instant messaging (IM). Given that email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately protected. In addition, email and IM are potential sources of spam, social engineering and malware attacks, so The Firm must be protected as completely as possible from these threats. The misuse of email and IM can pose numerous legal, privacy and security risks, so it is important for users to be aware of the appropriate use of electronic communications. Users of The Firm's email system are prohibited from using email to:

9.3.1 Send, receive, solicit, print, copy, or reply to text, images, or other forms of communication that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age;

9.3.2 Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory;

9.3.3 Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties;

9.3.4 Send, receive, solicit, print, copy, or reply to sexually oriented messages or images;

9.3.5 Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language;

9.3.6 Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass The Firm, negatively impact productivity, or harm morale.

The purpose of this Email and IM policy is to ensure that information sent or received via THE FIRM's IT systems is appropriately protected, that these systems do not introduce undue security risks to THE FIRM and that users are made aware of what THE FIRM deems as acceptable and unacceptable use of its email and IM.

9.4 **THE FIRM's Rules related to Handheld Devices**

Many users do not recognise that mobile devices present a threat to IT and data security. As a result, they often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers. These rules outline both The Firm's requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets and other mobile devices, PC's and Notebooks.

Users of handheld devices are expected to diligently protect their devices from loss and disclosure of private information belonging to or maintained by The Firm.

In the event of a security incident or if suspicion exists that the security of The Firm's systems has been breached, The Firm shall be obliged to notify the IT support immediately, especially when a mobile device may have been lost or stolen.

9.5 **Anti-Virus Rules**

Management of THE FIRM is responsible for creating procedures that ensure that anti-virus software is run at regular intervals and that computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programmes into THE FIRM's programmes (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

9.6 **Usage Data**

Usage Data is collected automatically when using the internet services of THE FIRM. Usage Data may include information such as data subjects' device's internet protocol address (e.g., IP address), browser type, browser version, details of the pages of THE FIRM'S website that are visited by data subjects, the time and date of the website visit, the time spent on those pages, unique device identifiers and other diagnostic data. When data subjects access the website services of THE FIRM by or through a mobile device, THE FIRM may collect certain information automatically, including, but not limited to, the type of mobile device used by the data subject, unique ID, the IP address of the mobile device, the mobile operating system, the type of mobile Internet browser used, unique device identifiers and other diagnostic data. THE FIRM may also collect information that the user's browser sends whenever THE FIRM's website is visited.

9.7 **Tracking Technologies and Cookies**

Cookies and similar tracking technologies are used to track the activity on THE FIRM's website and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyse the efficiency of the website. The technologies which may be used to track may include:

9.7.1 Cookies or Browser Cookies. A cookie is a small file which may be placed on a data subject's device. Data subjects can instruct their browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if this function of THE FIRM's website is not accepted, data subjects may not be able to use some parts of the website. Unless the browser settings have been adjusted THE FIRM's website may use Cookies;

9.7.2 Flash Cookies. Certain features of the website may use local stored objects (or Flash Cookies) to collect and store information about data subjects' preferences or activity on the website. Flash Cookies are not managed by the same browser settings as those used for Browser Cookies. For more information on how Flash Cookies can be deleted the following process can be followed: "Where can I change the settings for disabling, or deleting local shared objects?" available at https://helpx.adobe.com/flashplayer/kb/disable-local-shared-objects;

9.7.3 Web Beacons. Certain sections of the website and emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit THE FIRM for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity);

9.7.4 Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on data subjects' personal computer or mobile device even when offline, while Session Cookies are deleted as soon as data subjects' web browsers are closed.

10 THIRD PARTY OPERATORS

THE FIRM recognises that, in fulfilling its service offering to its client base and in order to operate efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to THE FIRM's service delivery. As referenced in clauses 5 and 6 above, THE FIRM will obtain the necessary consent where required from the particular data subject.

THE FIRM shall moreover and where possible enter into an OPERATORS' AGREEMENT with the relevant third party with which THE FIRM shares data subjects' information in order to ensure that the third-party operator treats the personal information of THE FIRM's data subjects responsibly and in accordance with the provisions contained in the Act and Regulations thereto.

11 BANKING DETAILS

It is a known fact that law firms are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of the transaction.

THE FIRM has implemented clear warnings on all its correspondences warning data subjects of the risks of email hacking and interceptions. In the event that banking details are sent to data subjects or received from data subjects for purposes of payment, the banking details will be confirmed with a telephone call.

12 DIRECT MARKETING

THE FIRM will not share data subjects' information with third parties for the sole purpose of such third-party marketing to such data subjects. In the event that any associated third party uses the data subjects' information shared by THE FIRM with such third party in the fulfilment of its legal services, THE FIRM takes no responsibility for any consequences suffered by the data subject which may have been caused by the third party's actions.

THE FIRM does not send out bulk marketing emails to its database of existing clients. In the event that THE FIRM adopts a new direct marketing strategy in which it will start sending out these bulk emails, they will contain the required OPTING OUT/UNSUBSCRIBE options which allow the recipients of the emails to request a removal of their details from these bulk emails.

13 DATA CLASSIFICATION

All of THE FIRM's employees share in the responsibility for ensuring that THE FIRM's information assets receive an appropriate level of protection as set out hereunder:

13.1 Managers of THE FIRM are responsible for assigning classifications to information assets according to the standard information classification system presented below;

13.2 Where practical, the information category shall be embedded in the information itself;

13.3 All employees of THE FIRM shall be guided by the information category in their security-related handling of THE FIRM's information. All information of THE FIRM and all information entrusted to THE FIRM from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	**Examples**	**Category**
Unclassified Public	Information is not confidential and can be made public without any implications for THE FIRM	Product brochures widely distributed

		Information generally available in the public domain, including publicly available web site areas of THE FIRM Financial reports required by regulatory authorities Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorised access could influence THE FIRM's operational effectiveness, cause financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	Passwords and information on corporate security procedures Know-how used to process client information Standard Operating Procedures used in all parts of THE FIRM's activities
Client Confidential Data	Information collected and used by THE FIRM in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. Access to this information is restricted within THE FIRM. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data Accounting data and internal financial reports Confidential customer business data and confidential contracts Non-disclosure agreements with clients / vendors Company business plans

14 **RIGHTS OF THE DATA SUBJECT- FORMS 1 & 2 ATTACHED**

14.1 The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information is not affected.

14.2 A data subject may object, at any time, to the processing of personal information – a) In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or b) For purposes of direct marketing by means of unsolicited electronic communications.

14.3 A data subject, having provided adequate proof of identity, has the right to – a) Request THE FIRM to confirm, free of charge, whether or not THE FIRM holds personal information about the data subject; and b) Request from THE FIRM a record or a description of the personal information about the data subject held by THE FIRM, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information – within a reasonable time; at a prescribed fee as determined by the Information Officer; in a reasonable manner and format; and in a form that is generally understandable.

14.4 A data subject may, in the prescribed manner, request THE FIRM 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 FIRM is no longer authorised to retain.

14.5 Upon receipt of a request referred to in clause 14.4, THE FIRM will, as soon as reasonably practical – a) Correct the information; b) Destroy or delete the information; c) Provide the data subject, with credible evidence in support of the information; or d) Where an agreement cannot be reached between THE FIRM 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.

15 INFORMATION OFFICER

15.1 **Appointed Information Officer:**

STEVEN MEISE

TELEPHONE NUMBER: +27 (0)16 420 2600

EMAIL: stevenm@mnlaw.co.za

STEVEN MEISE will serve as THE FIRM's primary contact when meeting with law enforcement agencies. In such meetings STEVEN MEISE may include any of THE FIRM's employees who assist him in the compliance functions.

15.2 **The general responsibilities of THE FIRM's Information Officer include the following:**

15.2.1 The encouragement of compliance, by THE FIRM, with the conditions for the lawful processing of personal information;

15.2.2 Managing requests made to THE FIRM pursuant to POPIA;

15.2.3 Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the business;

15.2.4 Perform data backups, store at least weekly backups offsite, and test those backups regularly for data integrity and reliability;

15.2.5 Review policy rules regularly, document the results, and update the policy as needed;.

15.2.6 Update information security policies and network diagrams;

15.2.7 Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates;

15.2.8 Perform continuous computer vulnerability assessments and audits;

15.2.9 The Information Officer may appoint any number of Deputy Information Officers as is necessary to perform the duties of the Information Officer as set out above. The Information Officer has control over every Deputy Information Officer(s) appointed;

15.2.10 The Information Officer may delegate, in writing, his/her power of duty conferred or imposed by this Act, to a Deputy Information Officer(s). In his/her decision to delegate power of duty, the Information Officer must give due consideration to the need to render THE FIRM as accessible as reasonably possible for requests of its records;

15.2.11 The Deputy Information Officer's duties must only be exercised or performed subject to any conditions set by the Information Officer. The delegation of power does not prohibit the Information Officer from performing these duties himself/herself. The Information Officer may at any time withdraw or amend, in writing, the delegation of power of duty;

15.2.12 Any right or privilege acquired, or any obligation or liability incurred as a result of the delegation of power, is not affected by any subsequent withdrawal or amendment of that delegation.

15.3 **The data breach responsibilities of THE FIRM's Information Officer include the following:**

15.3.1 Ascertain whether personal data was breached;

15.3.2 Assess the scope and impact by referring to the following:

15.3.2.1 Estimated number of data subjects whose personal data was possibly breached;

15.3.2.2 Determine the possible types of personal data that were breached;

15.3.2.3 List security measures that were already in place to prevent the breach from happening.

15.3.3 Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:

15.3.3.1 The Information Regulator;

15.3.3.2 Any data subjects who have been affected by such data breach;

15.3.3.3 THE FIRM will only delay notification to a 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;

15.3.4 Review and monitor:

15.3.4.1 Once the personal data breach has been contained, THE FIRM will conduct a review of existing measures in place and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.

15.3.4.2 All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

16 GDPR

THE FIRM fully supports and complies with the 6 (Six) protection principles of the GDPR related to data subjects of THE FIRM who fall within the EU and which are summarised below:

16.1 **Lawfulness, fairness and transparency**: The personal information of European citizens will be processed lawfully, fairly and in a transparent manner in relation to the data subject.

16.2 **Purpose limitation:** The personal information of European citizens will be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose.

16.3 **Data Minimisation**: The personal information of European citizens will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

16.4 **Accuracy**: The personal information of European citizens will be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.

16.5 **Storage Limitation**: The personal information of European citizens will be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

16.6 **Integrity and Confidentiality**: The personal information of European citizens will be processed in a manner that ensures appropriate security of the personal data, including protection against

unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

17 **AVAILABILITY AND REVISION**

A copy of this Policy is made available at both offices of THE FIRM situated at 1 Fish River Street, Vanderbijlpark and 153 General Hertzog Road, Vereeniging and, where possible, a copy of this Policy will be placed on THE FIRM's website.

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) AND REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	**DETAILS OF DATA SUBJECT**
Name(s) and surname/registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	

C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) TO (f) *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20.....

_____

Signature of data subject/designated person

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) AND REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	**DETAILS OF THE DATA SUBJECT**
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**

Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
E-mail address:	

C	INFORMATION TO BE CORRECTED/DELETED/DESTROYED

D	**REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or** **REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.** *(Please provide detailed reasons for the request)*

Signed at ..... this ..... day of .....20.....

_____

Signature of data subject/ designated person

FORM 3

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE POTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) AND REGULATIONS RELATING TO THE PROTECTION OF PERSONLA INFORMATION, 2018
[Regulation 6]

PART A

TO: _____

(Name of data subject)

FROM: _____

Address: _____

Contact number(s): _____

Fax number: _____

E-mail address: _____

(Name, address and contact details of responsible party)

Full names and designation of person signing on behalf of responsible party:

_____

_____

Signature of designated person

Date: _____

PART B

I,_____*(full names of data subject)*hereby:

☐ Give my consent

To receive direct marketing of goods or services to be marketed by means of electronic communication.

SPECIFY GOODS or SERVICES: _____

SPECIFY METHOD OF COMMUNICATION:

FAX: _____

E - MAIL: _____

SMS: _____

OTHER – SPECIFY: _____

Signed at ..... this ..... day of .....20.....

_____

Signature of data subject