Protection of Personal Information Act 4 of 2013
DATA PRIVACY
2024

By providing us with your personal information, you agree to our Data Privacy terms and you authorise us to process such information as set out herein. Our Data Privacy Terms apply to all external parties with whom we interact, including but not limited to individual clients, business partners, visitors to our offices, our own employees and agents and other users of our real estate services. ('you').

In delivering our real estate services, our agency respects the privacy of your personal information and has implemented reasonable measures to ensure that processing of your personal information is aligned to the requirements of the Protection of Personal Information Act 4 of 2013 ('POPIA'). In this document we explain how and when we process personal information. If you have questions arising from the processing of information that are not specifically listed herein, you may contact us on Information.Officer@signaturerealestate.co.za for assistance. Our agency may review and update our Data Privacy Terms from time to time.

1. INTRODUCTION

1. Our agency specialises in the sale and rental of residential properties in Cape Town.
2. In delivering these real estate services, we deal with many role players in the various real estate areas relative to the particular data subject and in performing our real estate services it is necessary to collect and process personal information as and when required, including but not limited to:
   - 2.1 The marketing of our clients' properties, either for sale or rental;
   - 2.2 Our agency complying with Regulatory requirements, both in terms of the Property Practitioners Regulatory Authority, the Consumer Protection Act and the Financial Intelligence Centre Act – amongst others;
   - 2.3 The management of client enquiries, instructions or transactions in which we act or have received instruction or are involved with in any way on a professional basis;
   - 2.4 The information required for us to attend to a matter.
   - 2.5 Some information when you browse our website or from the marketing portals on which you may have made enquiry but we will not record any of your personal details from the website or these marketing portals unless you specifically subscribe or engage with us directly from the website or portals. These details are recorded in our website terms and conditions and in the terms and conditions on the marketing portals.
3. We may collect or obtain your personal information:
   - 3.1 directly from you;
   - 3.2 in the course of our business relationship with you;
   - 3.3 in the course of providing our services to you;
   - 3.4 when you make your personal information public;
   - 3.5 when you visit and/or interact with our website, with us via the marketing portals or our social media platforms;
   - 3.6 when you register to access our services including but not limited to newsletters, information updates and similar services and products that we offer;
   - 3.7 when you visit our offices; and
   - 3.8 from third parties involved in your transaction.

3.9 We may record personal information about you such as records of your communications and interactions with us, including, but not limited to, your email and other communications with us, your details supplied for delivery of our services (such as invoicing and other such information) or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you during the course of digital or 'in person' marketing campaigns.

3.10 We treat your personal information confidentially and only use, share, record or delete it as is required by law, as part of our service delivery to you and/or as lawfully instructed by you. We primarily use your personal information only for the purpose for which it was originally or primarily collected. We will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest for you or for us and is closely related to the original or primary purpose for which your personal information was collected.

2. OBJECTIVE

Although it is not possible to ensure 100% mitigation against data breaches, the objective of our agency's Data Privacy Terms is to ensure adherence by our agency and all employees and agents associated with our agency to the provisions within POPIA together with its Regulations. Our agency recognizes that these Regulations are aimed at protecting all of our agency's data subjects from harm, 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 unless Consent for such sharing is obtained or that the sharing is lawful, to stop identity fraud and generally to protect privacy.

3. POPIA CORE PRINCIPLES

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

3.1. 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.

3.2. 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.

3.3. To ensure that the requirements of the POPIA legislation are upheld within our agency. In terms of sections 8, 17 and 18 of POPIA, our agency 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.

3.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, our agency will only collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for our operations and to process the personal information obtained from clients, employees, visitors and services suppliers only for the purpose for which it was obtained in the first place.

3.5. Processing of personal information obtained from clients, our agents, our employees, visitors and service suppliers will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the particular data subject.

3.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all our agency's data subjects will be allowed to request access to certain personal information and may also request correction or deletion of personal information within the specifications of the POPIA. Data subjects should refer to FORMS 1 & 2 attached hereto for these purposes.

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

3.8. In terms of the provisions contained within section 16 of POPIA, our agency is committed that data subjects' information is recorded and retained accurately.

3.9. Our agency will 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.

3.10. Our agency keeps effective record of personal information and undertakes not to retain information for a period longer than required.

3.11. In terms of sections 19 to 22 of POPIA, our agency ensures the integrity and confidentiality of personal information in our possession and will provide the necessary security of data and keep it in accordance with prescribed legislation.

4. COLLECTION AND PROCESSING OF PERSONAL INFORMATION

We may subject your personal information to processing during the course of various activities, including:

4.1. The general operation of our agency;

4.2. Analysis, evaluation, review and collation of information in order to determine potential disputes, provide project advice and preparing or commenting on opinions, project projections, responding to correspondence, reports, publications, documents relating to our projects and any other documents and records;

4.3. Compliance with the law and specifically fraud prevention and the combatting of money laundering;

4.4. Transfer of information to our service providers and operators;

4.5. For recruitment purposes;

4.6. For relationship management and marketing purposes in relation to our services (including, but not limited to, processing that is necessary for the development and improvement of our services), for accounts management, and for marketing activities in order to establish, maintain and/or improve our relationship with you;

4.7. In addition, we may process your personal information for statistical purposes and for internal management and management reporting purposes, including but not limited to: conducting internal audits, conducting internal

investigations, implementing internal business controls, providing central processing facilities, for insurance purposes and for management reporting analysis.

4.8. We may process your personal information for safety and security purposes.

4.9. We may share certain personal information with other institutions as part of our service rendering or as legally required, such as sharing information with the Receiver of Revenue, local authorities, the courts, sheriffs and the like. We only share such personal information as are required for purposes of fulfilling our service mandate or as prescribed by law.

4.10. Collection of personal information from another source may be necessary –

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

4.10.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

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

4.10.4. In the interest of national security;

4.10.5. To maintain the legitimate interests of our agency or of a third party to whom the information is supplied;

4.10.6. Where compliance would prejudice a lawful purpose of the collection;

4.10.7. Where compliance is not reasonably practicable in the circumstances of a particular contract.

4.11. Our agency often collects personal information from other parties involved in our transactions as various professionals and property role players share clients in a single transaction.

4.12. Most of our communications are done electronically via the internet, per email and other electronic methods and we recognise the international risk of data and email breaches. To ensure that lawful conditions exist surrounding our data subject's information, we accept that all its South African based data subjects' Constitutional Right to Privacy is of utmost importance and that our data subjects based in other parts of the world are equally entitled to rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based.

4.13. As such, we are committed to comply with South Africa's POPIA provisions and to the education of our data subjects in respect of your rights to privacy and to make all operational amendments necessary.

5. CONSENT

When data subjects' information is collected, processed or shared by our agency, it will be for the purposes of delivering our services. In doing so, we explain the reasons for the collection of information from the particular data subject/s and obtain the required Consents to process if the Consent is necessary and where required the sharing of the information pursuant to such explanation. Our agency understands the importance of obtaining our data subjects' Consent where necessary to share their information and possibly using the information for limited marketing purposes.

If personal information is used for any other reason than the original reason of it being collected, the specific Consent for such purpose will be obtained from the data subject. Our agency does not use information for other purposes other than what it was collected for. If SPECIAL PERSONAL INFORMATION is collected, processed and stored for any reason from any of our agency's data subjects, a specific Consent for such collection will first be obtained.

There are instances in which this specific Consent will not be required:

5.1. If collection and processing are carried out with a prior consent of the data subject;

5.2. If collection and processing are necessary for the establishment, exercise or defence of a right or obligation in law;

5.3. If collection and processing are for historical, statistical or research purposes.

Our standard documentation now reflect the Consent mentioned herein and in compliance with the POPIA.

6. STORAGE OF INFORMATION

Management and all employees and agents of our agency remain aware of the risks facing data subjects with the storage of personal and special personal information on our agency's software systems as well as filing copies of the physical information sheets containing personal information physically in our office. To ensure that our best attempts are made to minimize data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorized access or disclosure of personal information generally, we will:

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

6.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. Our agency tests our systems regularly to ensure that our security mechanisms are up to date.

6.3. Continue to review our internal policies and third-party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with our agency's general Data Privacy Terms.

7. DISPOSAL OF DATA SUBJECTS' INFORMATION

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

In this regard, our agency has developed an ARCHIVING POLICY in which we have determined when and how information and communications with and to our customers are kept and stored. The archiving policy deals with:

7.1. How emails are stored and when emails are deleted destroyed;

7.2. How customer data is stored, on which software systems and when these are destroyed;

7.3. How physical copies of information and communications are stored and when these are destroyed.

As a matter of course, we do not discard or dispose of the telephone numbers, email addresses of data subjects and electronic communications with data subjects with whom we have previously dealt but will do so on request by the data subject. However, since our agency recognizes that most of the information which it collects, processes and shares with other role players in transactions is personal of nature, we do not let information lie around and keep strict controls in respect of access to our software systems. For this reason, we will dispose of information securely when no longer required or when being requested by the data subject.

Our agency acknowledges that electronic devices and media hold vast amounts of information, some of which can linger indefinitely, and we follow the following rules strictly:

7.4. 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.

7.5. Our agency will ensure that all electrical waste, electronic equipment and data on disk drives are physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.

7.6. Our agency will also ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.

7.7. In the event that a third party is used for data destruction purposes, our agency's Information Officer will ensure that such third party also complies with our rules and any other applicable legislation.

7.8. Our agency may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings and we undertake to notify employees and agents of applicable documents where the destruction has been suspended to which they have access.

7.9. In the event that a document and/or information is no longer required to be stored in accordance with either legislation or in line with our own rules, it should be deleted and destroyed.

7.10. Our agency's Information Officer will give direction where there is uncertainty regarding the retention and destruction of a document and/or information.

7.11. DATA SUBJECTS ARE REFERRED TO THE ANNEXED FORMS 1 AND 2 with regards to requests to amend and delete personal information from our agency's database.

8. CYBER TECHNOLOGY

8.1 Standard Anti-Virus rules

The repercussions of misuse of our agency'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 our agency's IT systems are not misused and in accordance with **ANNEXURE A (the IT security measures summarised)**, everyone who uses or has access to our systems have received training and internal guidelines in order to meet the following five high-level IT Security requirements:

8.1.1. Information will be protected against any unauthorized access as far as possible;

8.1.2. Confidentiality of information will be assured as far as possible;

8.1.3. Integrity of information will be preserved as far as possible;

8.1.4. Availability of information for business processes will be maintained;

8.1.5. Compliance with applicable laws and regulations to which our agency is subject will be ensured by our Information Officer as far as possible.

Every user of our IT systems takes responsible for exercising good judgment regarding reasonable personal use.

8.2 IT Access Control

Only authorized employees and agents may log into our agency's IT system and software packages, and these are password controlled. All employees and agents of our agency exercise caution in allowing unauthorized access to a password and our agency's IT department ensure that the passwords are reviewed and renewed from time to time - in particular where GOOGLE based products are used and linked (such as Facebook, WhatsApp and GMAIL based domains).

8.3 Email Rules

In accordance with **ANNEXURE A**, most of our agency's digital 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 potentially sources of spam, social engineering attacks and malware. The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users of our agency's services to be aware of the appropriate use of electronic communications.

It is of use to note that all users of our agency's employees and agents are prohibited from using email to:

8.3.1 Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

8.3.2 Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.

8.3.3 Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.

8.3.4 Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.

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

8.3.6 Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass our agency, negatively impact productivity, or harm morale.

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

8.4 Our agency's rules related to handheld devices

In accordance with **ANNEXURE A**, many users do not recognize that mobile devices represent 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. Our agency safeguards the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices like PC's and Notebooks and our agency's Information Officer and the IT department ensure that:

8.4.1 The agency's users of handheld devices diligently protect their devices from loss and disclosure of private information belonging to or maintained by our agency and that this is achieved with constant awareness training.

8.4.2 Before connecting a mobile handheld device to the network at our agency, users are expected to ensure it is on the list of approved devices issued by the IT support wherever necessary.

8.4.3 In the event of a security incident or if suspicion exists that the security of our agency's systems has been breached, the person in our agency who becomes aware of the breach shall notify the IT support team immediately together with our agency's Information Officer especially when a mobile device may have been lost or stolen.

8.5 Anti-virus rules

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

8.5.2 Our agency's employees and agents are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from our agency's networks, stop using the infected computer immediately and notify the IT support.

It is further worth noting that our agency's users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. All employees and agents have received and will continue to receive internal training in respect of such viruses and how to identify them and what to do if a virus is suspected.

8.6 Physical access control

All of our agency's premises that include computers and other types of information technology resources will be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of

the building, locked and/or barred windows, security cameras, registration of visitors at entrances, security guards, and fire protection.

9 THIRD PARTY OPERATORS

In order for our agency to deliver our services efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to our service delivery. As referenced in clauses 1 to 5 above, where necessary we will obtain the necessary Consent where required from the particular data subject.

Where data subjects' information is shared with these third-party operators, our agency enters into OPERATORS' AGREEMENT with the relevant third-party where possible. These OPERATORS' AGREEMENTS are necessary in order to ensure that the third-party operator treats the personal information of our data subjects responsibly and in accordance with the provisions contained in the POPI Act and Regulations thereto. When we present our OPETARORS' AGREEMENTS to a third-party for signature, we usually request copies of the third-party operators' POPIA Policy, rules, internet rules and details of the third-party's Information Officer.

10 BANKING DETAILS

It is a known fact that South African businesses are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of transactions. Our data subjects are open to large amounts of damages and losses if emails are intercepted, and banking details are fraudulently amended without the data subject's knowledge.

We have implemented an INTERNAL PAYMENTS POLICY which has been circulated to all employees and agents and in accordance with which our employees and agents are formally held liable when not following our rules as well as clear warnings within all our correspondences (emails and physical letters) 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 sent via a secure channel (other than email) and must be confirmed with a telephone call and a follow up WhatsApp. It is recorded that, in certain instances, data subjects' bank details are to be shared with relevant third parties but in such event, all care shall be taken to ensure encryption of emails.

11 DIRECT MARKETING

Our agency does not share data subjects' information with third parties for the sole purpose of such third-party marketing to such data subjects. Marketing of property occurs mostly via the various property portals and any interaction via these portals are subject to the particular portal's Data Terms and Conditions and our agency cannot control how such portals use your information. In the event that any associated third-party using the data subjects' information it collected from our agency, our agency takes no responsibility for any consequences suffered by the data subject which may have been caused by the third-party's actions.

Our agency does not send out bulk emails to our database of existing clients. In the event that our agency adopts a new direct marketing strategy in which we start sending out these bulk emails, we will ensure that the required OPTING OUT/UNSUBSCRIBE options which allow the recipients of the emails to request a removal of their details from these bulk emails are clearly implemented.

12 DATA CLASSIFICATION

In accordance with our agency's INTERNAL DATA CLASSIFICATION POLICY, all of our agency's employees and agents share in the responsibility for ensuring that our information assets receive an appropriate level of protection as set out hereunder:

12.1 Our managers are responsible for assigning classifications to information assets according to the standard information classification system presented below.

12.2 Where practicable, the information category shall be embedded in the information itself.

12.3 All employees and agents of our agency shall be guided by the information category in their security-related handling of our information. All information entrusted to us 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 our agency	Product brochures widely distributed Information widely available in the public domain, including publicly available web site areas. Financial reports required by regulatory authorities. Newsletters for external transmission
Proprietary	Information restricted to management, approved internal access and protected from external access. Unauthorized access could	Passwords and information on corporate security procedures.

	influence our agency's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	Know-how used to process client information. Standard Operating Procedures used in all parts of our agency's activities. All software codes developed by our agency whether used internally or sold to clients.
Client Confidential Data	Information collected and used by our agency in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. 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.

13 RIGHTS OF THE DATA SUBJECT- FORMS 1 & 2 ATTACHED

13.1 All of our data subjects 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.

13.2 Any of our data subjects may object, at any time, to the processing of personal information–

13.2.1 In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

13.2.2 For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

13.3 All of our data subjects, having provided adequate proof of identity, have the right to–

13.3.1 Request from us to confirm, free of charge, whether we hold personal information about the data subject; and

13.3.2 Request from our agency a record or a description of the personal information about the data subject held by us 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 our agency's Information Officer; in a reasonable manner and format; and in a form that is generally understandable.

13.4 Our data subjects may, in the prescribed manner, request our agency to –

13.4.1 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

13.4.2 destroy or delete a record of personal information about the data subject that our agency is no longer authorised to retain.

13.5 Upon receipt of a request referred to in clause 13.4, our agency will, as soon as reasonably practicable –

13.5.1 correct the information;

13.5.2 destroy or delete the information;

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

13.5.4 where an agreement cannot be reached between our agency and the data subject, and

13.5.5 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.

13.6 Our agency will inform the data subject, who made a request as set out in clause 13.5 of the action taken as a result of the request.

14 INFORMATION OFFICER

Appointed Information Officer:

INFORMATION OFFICER: DANNI MARTIN

Tel: +27 (0)76 538 8558
Email: Information.Officer@signaturerealestate.co.za

Postal Address: 8 Beach Crescent, Scott Estate, Hout Bay, 7806
Street Address: 8 Beach Crescent, Scott Estate, Hout Bay, 7806

14.1 The general responsibilities of our agency's Information Officer include the following:

14.1.1 Ensure that the INTERNAL INCIDENT RESPONSE POLICY is circulated and managed;

14.1.2 The encouragement of compliance, by all employees and agents with the conditions for the lawful processing of personal information;

14.1.3 Managing requests made to our agency pursuant to POPIA and PAIA;

14.1.4 Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the firm.

14.1.5 Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.

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

14.1.7 Continuously update information security policies and network diagrams.

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

14.1.9 Perform continuous computer vulnerability assessments and audits.

14.2 The data breach responsibilities of our agency's Information Officer include the following:

14.2.1 Ascertain whether personal data was breached;

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

14.2.2.1 Estimated number of data subjects whose personal data was possibly breached
14.2.2.2 Determine the possible types of personal data that were breached
14.2.2.3 List security measures that were already in place to prevent the breach from happening.

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

14.2.3.1 The Information Regulator
14.2.3.2 Communication should include the following:
14.2.3.2.1 Contact details of Information Officer
14.2.3.2.2 Details of the breach,
14.2.3.2.3 Likely impact,
14.2.3.2.4 Actions already in place, and those being initiated to minimise the impact of the data breach.
14.2.3.2.5 Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

14.3 Review and monitor

14.3.1 Once the personal data breach has been contained, our agency 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.

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

15. FINANCIAL INTELLIGENCE CENTRE ACT

Due to International pressures, the South African FINANCIAL INTELLIGENCE CENTRE has vastly amended its anti-corruption, anti-money laundering and anti-terrorism laws and expanded the list of industries who must now apply FICA to their transactions. All operations of our agency are now subjected to these new FICA rules and all our clients are required to undergo the new FICA processes. These processes oblige our agency to collect in-depth personal and often special personal information from our clients and assess this information internally. Some information which our agency collects may be shared with the FIC from time to time. The FIC Act clarifies the issue of data privacy of client information for our agency who will often be collecting, verifying and screening client information without a specific consent form such client. The processing of personal and special personal information of clients for the purposes of the FIC Act compliance may only be done within the confines of the POPI Act. While the processing and further processing of personal information of a client for purposes of FIC Act requirements is allowed in terms of the POPI Act, our agency will observe caution when verifying clients' details using third-party data sources.

Our agency acknowledges section 37(1) of the FIC Act which states that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by our agency to report with the exception of the common law right afforded to legal professional privilege as between an attorney and the attorney's client noted in section 37(2) of the FIC Act in respect of communications made in confidence.

In terms of section 41A of the FIC Act, the FIC will ensure that it has appropriate measures in place to protect the confidentiality of personal information received by establishing and maintaining appropriate safeguards against the foreseeable internal and external risks identified.

In compliance with sections 21, 21A, 21B, 21C and 21E of the FIC Act, our agency's FICA QUESTIONNAIRE includes questions in relation to our data subjects' personal information, our data subjects' occupation, our data subjects' general wealth profile, whether our data subjects may or may not be politically connected or not, whether our data subjects may receive benefit from any industry identified by the UN as higher risk (such as transportation businesses, courier businesses etc); and whether our data subjects hold business interests and/or bank accounts abroad.
We value our relationship with our clients and will keep all information supplied to us confidential in terms of our Data Privacy Rules. Although we are very aware of the inconvenience of having to send and resend the information and documents to the many institutions involved in the transaction, our agency is bound by law in this regard and wish to avoid the possibility of all clients in the transaction, including ourselves, contravening the provisions in the Financial Intelligence Centre Act and the need in such instance, to address a report to the FIC.

16. AVAILABILITY AND REVISION

A copy of this Policy is made available at Our agency's offices in Hout Bay since our agency does not have an active website at present.

This policy will continually be updated to comply with legislation, thereby ensuring that personal information will be secure.

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 our agency, this will include but not be limited to – real estate services for both public and private entities and other general clients, employees, external service suppliers and all associates of our agency;
"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 our agency, real estate 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 our agency consists of physical files kept in the offices of our agency together with the data filed on the various software systems used by our agency;
"Information officer": of our agency will mean **DANNI MARTIN, Identity Number 840724 0250 08 3**;
"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 visuals 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;

"**Our agency"**: for purposes of the Data Privacy Terms means SIGNATURE REAL ESTATE (PTY) LTD, Registration number 2017/006317/07 situated at 8 Beach Crescent, Scott Estate, Hout Bay, 7806**;**

"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 pa