Protection of Personal Information (POPI)

EXTERNAL PRIVACY POLICY

1. DEFINITIONS

"data subject": means the person to whom personal information relates and for the purposes of THE FIRM, this will include but not ne limited to – sellers, buyers, clients, employees, external service suppliers and all associates of THE FIRM;
"**THE FIRM"**: for purposes of this Policy document means the law firm registered as Adriaan Groenewald Inc, Registration Number 2021/631462/21, situated at 12 Saffery Street, Humansdorp.
"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;
"Information officer": of THE FIRM will means Adriaan Groenewald ID 610315 5079 086
"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; e) 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 business or profession, but only in such capacity;
"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;
"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 operates in the following fields of law: Conveyancing, valuations, Commercial Law and Water Law. THE FIRM facilitates the registration of property transactions, mortgage bonds, rendering of advice in terms of the National Water Act, litigation in the Magistrate and High Court and deals with commercial transactions on behalf of THE FIRM's commercial clients. In the fulfillment of its legal services, THE FIRM deals with many role players in the various fields of law and acknowledges that, in performing its business operations most of its communications are done electronically via the internet and that personal information is collected and processed electronically in compliance with the Electronic Communications and Transaction Act 25 of 2002. In recognizing the international risk of data breach and also to ensure that lawful conditions exist surrounding its data subject's 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. THE FIRM is further committed to the education of its data subjects in respect of their rights to privacy and will make all operational amendments necessary.

3. OBJECTIVE

The objective of this Policy is to ensure adherence to the provisions within POPIA together with its Regulations aimed at protecting all THE FIRM's data subjects from harm by protecting their personal information, to stop identity fraud and generally to protect privacy. This Policy is the EXTERNAL SET OF PRIVACY RULES 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 organisation. 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 subscribe to a process of accountability and openness throughout its operation.

4.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPI, THE FIRM undertakes to collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for operations and to process the personal information obtained from clients only for the purpose for which it was obtained in the first place.

4.5. Processing of personal information obtained from clients will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the client.

4.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all data subjects of THE FIRM 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.

4.7. To 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. THE FIRM will also not process information of juveniles.

4.8. In terms of the provisions contained within section 16 of POPIA**,** THE FIRM is committed that 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 undertakes not to retain information for a period longer than specified in the property industry's Code of Conduct or any other direction issued by the Estate Agency Affairs Board.

4.11. In terms of sections 19 to 22 of POPIA, THE FIRM will secure the integrity and confidentiality of personal information in its possession. THE FIRM will provide the necessary security of data and keep it in accordance with prescribed legislation.

5. CONSENT

If data subjects' information is collected, processed or shared 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, specific Consent for such collection must first be obtained

The prohibition on collection and processing of special personal information does not apply if:-

5.1. Processing is carried out with the consent of the data subject;
5.2. Processing is necessary for the establishment, exercise or defense of a right or obligation in law;
5.3. Processing is for historical, statistical or research purposes.

6. COLLECTION AND PROCESSING 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 property transaction being facilitated by THE FIRM and the integrated nature of operation between THE FIRM and the other primary role players in the transaction. Various South African laws apply to the collection and processing of information by THE FIRM:

- In terms of the Financial Intelligence Centre Act 2001, THE FIRM is defined as an Accountable Institution and as such, is subject to the Regulatory obligations to assess the Money Laundering and Terrorism risk in dealing with its clients. As such, the identities of all clients are to be confirmed and verified and clients' details are screened against lists published by the Financial Intelligence Centre;
- The Deeds Registry Act 1937 require full descriptions of the parties and property related to the transaction and all information lodged at the Deeds Office becomes public record. Clients' marital status, dates of birth and full names are to be verified for purposes of the property transaction;
- In terms of the National Credit Act 2005, parties in a property transaction who intend taking a bank loan to fund a portion or all of the purchase price are obliged to supply all relevant and requested financial information to a variety of role players in the transaction, including THE FIRM.

The primary way of collection and processing of personal information is electronically. By submitting personal and special personal information details to THE FIRM, all data subjects acknowledge the terms of this Policy.

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. The data subject or a competent person;
6.1.3. Collection of the information from another source would not prejudice a legitimate interest of the data subject;
6.1.4. Collection of the information from another source is necessary -
  6.1.4.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
  6.1.4.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
  6.1.4.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
  6.1.4.4. In the interest of national security;
  6.1.4.5. To maintain the legitimate interests of THE FIRM or of a third party to whom the information is supplied;
  6.1.4.6. Compliance would prejudice a lawful purpose of the collection;
  6.1.4.7. Compliance is not reasonably practicable in the circumstances of the particular case.
6.1.5. Personal information is collected for a specific, explicitly defined and lawful purpose related to a function or activity of THE FIRM;
6.2. Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.
6.3. THE FIRM will take reasonably practicable 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.
6.4. Where personal information is collected form a data subject directly, THE FIRM will take reasonably practicable steps to ensure that the data subject is aware of: -
6.4.1. The nature of the information being collected and where the information is not collected from the data subject, the source from which it is collected;

6.4.2. The name and address of THE FIRM;
6.4.3. The purpose for which the information is being collected;
6.4.4. Whether or not the supply of the information by the data subject is voluntary or mandatory;
6.4.5. The consequences of failure to provide the information;
6.4.6. Any particular law authorising or requiring the collection of the information;

7. STORAGE OF INFORMATION

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

7.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.
7.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. THE FIRM tests its systems regularly to ensure that our security mechanisms are up to date.
7.3. Continue to review its internal policies and third party agreements where necessary to ensure that these are also complying with the POPIA and Regulations in line with THE FIRM's Policy rules.

9. DISPOSAL OF DATA SUBJECTS' INFORMATION

THE FIRM is responsible to ensure that necessary records and documents of their data subjects are adequately protected and maintained 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 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.

THE FIRM adheres to the Guidelines issued by the Law Society of South Africa and retains documents containing data subjects' personal information for a minimum period of 5 years. THE FIRM does not discard or dispose of the telephone numbers and email addresses of data subjects with whom it has previously dealt but will do so on request by the data subject. THE FIRM recognizes that most of the information which it collects, processes and shares with other role players in the transaction is personal of nature and will dispose of information securely when no longer required. Secure disposal maintains data security and supports compliance with this THE FIRM's policy. THE FIRM acknowledges that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely.

9.2. 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.
9.3. 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.
9.4. THE FIRM will ensure that all paper documents that should be disposed of, be shredded locally and then be recycled.
9.5. 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.
9.6. THE FIRM may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. THE FIRM undertakes to notify employees of applicable documents where the destruction has been suspended to which they have access to.
9.7. In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed.
9.8. The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

10. INTERNET AND CYBER TECHNOLOGY

10.1. Acceptable use of THE FIRM's Internet Facilities & standard Anti-Virus rules

The repercussions of misuse of THE FIRM 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 must meet the following five high-level IT Security requirements:

10.1.1. Information must be protected against any unauthorized access;
10.1.2. Confidentiality of information must be assured;
10.1.3. Integrity of information must be preserved;
10.1.4. Availability of information for business processes must be maintained;
10.1.5. Compliance with applicable laws and regulations to which THE FIRM is subject must be ensured.

Every user of THE FIRM's IT systems is responsible for exercising good judgment regarding reasonable personal use.

10.2. **IT Access Control**

THE FIRM shall ensure that logging into the IT system and software packages is password controlled and shall exercise all caution in allowing unauthorized access to the password. The password 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).

10.3. **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 FIRM information, the information involved must be appropriately protected. In addition, email and IM are potentially sources of spam, social engineering attacks and malware, so THE FIRM must be protected as completely as possible from these threats. The misuse of email and IM can post many 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:

10.3.1. 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.
10.3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
10.3.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
10.3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
10.3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
10.3.6. 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 these 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.

10.4. **THE FIRM's Rules related to handheld devices**

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. This policy outlines Dole's requirements for safeguarding the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices that PC's and Notebooks.

10.4.1. 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.
10.4.2. Before connecting a mobile handheld device to the network at THE FIRM, users are expected to ensure it is on the list of approved devices issued by the IT support where ever necessary.
10.4.3. 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.

10.5. **Anti-virus rules**

10.5.1. Management of THE FIRM 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 THE FIRM's programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

10.5.2. Users are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from THE FIRM's networks, stop using the infected computer immediately and notify the IT support.

10.5.3. Users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

10.6. **Physical access control**

10.6.1. All of THE FIRM'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.

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's 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.

THE FIRM has implemented clear warnings within all its 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 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.

12. DIRECT MARKETING

In the event that THE FIRM utilizes data subjects' personal contact particulars as stored on THE FIRM's existing database or obtained from a third party, THE FIRM shall ensure that it engages with the data subject responsibly and with respect. THE FIRM will develop a specific narrative that will need to be used when data subjects are telephoned and which narrative will include a series of questions to establish whether the data subject wishes to discuss an offering by THE FIRM, wishes to remain on the database for future offering or whether the data subject wishes to be deleted from THE FIRM database. Record of the telephone conversation is required.

In the event that THE FIRM sends emails to data subjects of a marketing nature or in the form of a newsletter, such emails shall clearly display the options of OPTING OUT of the email sender list. The requests for OPTING OUT must be recorded.

13. INFORMATION OFFICER

13.1. **Appointed Information Officer:**

Contact details Name	Information Officer Adriaan Groenewald
Postal Address: PO Box 2, Humansdorp 6300 Street Address: 12 ffery Street, mansdorp	
Tel./Mobile: 082 579 05	Office: 042 291 1634
E-Mail: riaan@groenewalds.com	

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

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

13.2.2. Managing requests made to THE FIRM pursuant to POPIA;

13.2.3. 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.

13.2.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
13.2.5. Review policy rules regularly, document the results, and update the policy as needed.
13.2.6. Continuously update information security policies and network diagrams.
13.2.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
13.2.8. Perform continuous computer vulnerability assessments and audits

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

13.3.1. Ascertain whether personal data was breached;

13.3.2. Assess the scope and impact by referring to the following:
13.3.2.1. Estimated number of data subjects whose personal data was possibly breached
13.3.2.2. Determine the possible types of personal data that were breached
13.3.2.3. List security measures that were already in place to prevent the breach from happening.

13.3.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:
13.3.3.1. The Information Regulator
13.3.3.2. Communication should include the following:
- Contact details of Information Officer
- Details of the breach,
- Likely impact,
- Actions already in place, and those being initiated to minimise the impact of the data breach.
- Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

13.3.4. Review and monitor
13.3.4.1. 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.
13.3.4.2. All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

14. AVAILABILITY AND REVISION

A link to this Policy is made available on the THE FIRM company website www.groenewalds. com

Postal Address: PO Box 182, Humansdorp 6300
Street Address: 12 Saffery Street, Humansdorp 6300
Telephone Number: 042 291 1634
Fax Number: ……..
Email: adriaan@groenewalds.com

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

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)

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):	
Fax number / 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):	
Fax number/ 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*

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)

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):	
Fax number/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):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ 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

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 PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018
[Regulation 6]

TO: _____
_____
_____

FROM: *(Name of data subject)*

_____
_____
_____
_____

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:
OTHERS – SPECIFY:

Signed at ..... this ..... day of .....20……...
……*Signature of data subject*