

FRAMEWORK & POLICY ON THE “PROTECTION OF PERSONAL INFORMATION ACT” 04 OF 2013 (“POPI”) (Website)

Dr Linda Sara Kantor is a Sole Proprietor in the field of Counselling Psychology specialising / focusing on Adult Individual Psychotherapy and Mindfulness Training. The practice makes up a Registered Healthcare Professional under the Health Professions Act 1974 and is subject to the rules and regulations of the Health Professions Council of South Africa (“HPCSA”) insofar as it regulates the privacy and personal information of patients and third parties.

1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013, (“POPIA/The Act”) and the Regulations promulgated thereunder give effect to the right to privacy provided by section 14 of the Bill of Rights of the Constitution of the Republic of South Africa 1996.

The Act and Regulations require the Information Officer of the responsible person as defined under the Act to develop, implement, monitor, and maintain a compliance framework, (Regulation 4 of Regulations published under GG number 42110 dated 14 December 2018).

The Practice has developed this policy in order to comply with the aforesaid requirements and to further demonstrate commitment to the spirit of the Act in respecting the rights of Data Subjects to have their Personal Information protected as set out in the Act.

Forms 1, 2 and 4 of the POPI Regulations are attached to this Policy.

2. SCOPE

This policy applies to all employees of The Practice and anyone who may process Personal Information for and on behalf of The Practice.

This policy applies to all situations and business processes where Personal Information is processed, more importantly where such information may be made accessible to third parties. This policy must be read together with the Practice’s PAIA Manual.

3. DEFINITIONS

- 3.1. **“Applicable Legislation”** means all legislation applicable to The Practice’ practice including the Act, the Medicines and Related Substances Act 101 of 1965; the National Health Act 61 of 2003; The Health Professions Act ; National Archiving Act, Income Tax Act 58 of 1962; Value Added Tax Act 89 of 1991; Labour Relations Act 66 of 1995; Basic Conditions of Employment Act 75 of 1997; Employment Equity Act 55 of 1998; Unemployment Insurance Act 63 of 2001; Electronic Communications and Transactions Act 25 of 2002; Telecommunications Act 103 of 1996; Electronic Communications Act 36 of 2005; Consumer Protection Act 68 of 2008; National Credit Act 34 of 2005; and all legislation as listed under clause 7 of The Practice PAIA Manual.
- 3.2. **“Data subject”** means the person to whom personal information relates as defined under the Act;
- 3.3. **“Employee”** means, for the purposes of this policy, any person employed permanently (full- or part-time), temporary, or on a fixed-term contract, and include contractors that may come into contract with, use, process or otherwise deal with Personal Information.
- 3.4. **“Operator”** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 3.5. **“Personal information”** shall mean, for purposes of this policy and as defined under the Act, information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:
 - 3.5.1. information relating to the race, gender, sex, pregnancy, marital status, national,
 - 3.5.2. ethnic or social origin, colour, sexual orientation, age, physical or mental health,
 - 3.5.3. well-being, disability, religion, conscience, belief, culture, language and birth of the person;
 - 3.5.4. information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;
 - 3.5.5. any identifying number, symbol or other particular assigned to the person;
 - 3.5.6. the address, fingerprints or blood type of the person;
 - 3.5.7. the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual;
 - 3.5.8. correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
 - 3.5.9. the views or opinions of another individual about the person;
 - 3.5.10. the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
 - 3.5.11. the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;
 - 3.5.12. but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years.

- 3.6. **“Policy”** means this policy developed in terms of the Act and Regulations thereto;
- 3.7. **“Processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
 - 3.7.1. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - 3.7.2. dissemination by means of transmission, distribution or making available in any other form; or
 - 3.7.3. merging, linking, as well as restriction, degradation, erasure, or destruction of information.
- 3.8. **“Purpose”** means The Practice's purpose to processing of Personal Information as set out under The Practice's PAIA Manual;
- 3.9. **“Responsible Party”** means, for purposes of this policy, all persons to whom this policy applies, whom, whether alone or in conjunction with others determines the purpose and means of processing Personal Information.
- 3.10. **“Special Personal Information”** means information relating to a person's (a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) criminal behavior, as defined under the Act.

4. THE PRACTICE REQUIREMENTS FOR PROCESSING PERSONAL INFORMATION

- 4.1. All Processing of Personal Information must be done **after a written and signed consent** in a form developed and approved form by The Practice, has been received from the Data Subject.
- 4.2. Where there is a legal requirement to disclose Personal Information to authorities, and consent is not required by law, the Data Subject must still be notified of such disclosure, unless the Applicable Law provides otherwise.

5. NOTIFICATIONS

- 5.1. The Practice will inform all persons whose information is being processed, of that fact.
- 5.2. This is done via the Practice's Terms and Conditions, on specific consents to disclosure, and, where bulk-mailers or communications are sent out, with a statement relating to the rights of the Data Subject, attached thereto.
- 5.3. The rights of Data Subjects are as follows:
 - 5.3.1. Notification when personal information is being collected, the type of information collected, for what purpose, whether the information is to be supplied voluntarily or is collected mandatory, and whether the information would be transferred to a third country and the protections afforded there;
 - 5.3.2. Notified if there has been unlawful access or acquisition of his/her/its personal information;
 - 5.3.3. Request a record of your Personal Information;
 - 5.3.4. Request the correction, deletion and/or destruction of your Personal Information;
 - 5.3.5. Object to the processing of your Personal Information;
 - 5.3.6. Exercise the right to withdraw the consent to processing, if voluntarily given;
 - 5.3.7. Not be subjected to unsolicited electronic communication, unless you are our customer and we have sold goods or services to you, or where you have consented to the communication and you had and have the opportunity to object to the communication;
 - 5.3.8. Not to be subjected to automated decision-making based on the personal information in contravention of section 71, POPI Act;
 - 5.3.9. Submit a complaint to the Information Regulator at <https://www.inforegulator.org.za/>; and
 - 5.3.10. Institute civil proceedings regarding an alleged interference with his/her/its personal information in terms of section 99, POPI Act.
- 5.4. The details of the Information Officer, and the responsible Deputy Information Officer will also be included in all Notifications, and also appear on the PAIA Manual / PAIA Guide.

6. CONDITIONS OF LAWFUL PROCESSING OF PERSONAL INFORMATION

Section 4(1) of the Act requires that all Processing of Personal Information be done in a lawful manner. Anyone who Processes Personal Information for and on behalf The Practice must do so in terms of the below conditions in order to ensure compliance with the Act:

- 6.1. Ensure that all the conditions and measures giving effect to conditions of the lawful processing of Personal Information as set out in the Act and this policy are complied with at the time of the determination of the purpose and means of the Processing and during the Processing.
- 6.2. Personal Information must only be processed with the consent of the Data Subject, for a specific, explicit, and lawfully defined purpose, related to the functions and activities of The Practice, or if under a statutory obligation, with a notification to the person of the specific statutory mandate (quote Act, section and/or Regulation and number thereof).
- 6.3. All **consents to processing** and/or **notifications of processing** will be reviewed by responsible employees or office bearers to ensure that it is specific. In cases of uncertainty, the Information Officer or one of his/her deputies will be contacted for support. Where standard consents or notifications have been developed, employees are obligated to use those.
- 6.4. In the event of a requirement to use Personal Information outside the consented purpose, (**“further processing”**), then a further consent for the further processing must be obtained from the Data Subject prior to such further processing.
- 6.5. Personal Information must be collected directly from the Data Subject, should there be a need to collect the information from another source, the consent of the Data Subject must be obtained prior thereto. Where databases are bought or provided by a third party, a **warranty** must be included in the contract that such database have been compiled and is sold in compliance with POPIA.

- 6.6. Only up to date and correct Personal Information can be processed, and Data Subjects must request the correction of their Personal Information on Form 2 as set out in Regulations published under GG number 42110 dated 14 December 2018. All consents, notifications and contracts must include a hyperlink or attach Form 2.
- 6.7. The Responsible Persons must ensure that the security measures are put in place by The Practice, for every database and type / category of personal information processed, to protect against:
- 6.7.1. **Unauthorised access**, which means that access privileges must be stipulated, and where applicable, indicated in documents, minutes, etc. as follows (just add applicable row or rows in a header or footer of a document):

Accessible by:	Public
Patient files	Administrative staff authorized to work with such structure(s): Ms Vivienne Sheila Zaacks
	Dr Linda Sara Kantor = Access to <u>all</u> Information
	Ms Vivienne Sheila Zaacks (Admin Assistant) = Access to all information <u>except</u> for Patient Files
	MEDWAY Medical Bureau (Billing) = Access to Contact Details & Medical Scheme Details
	Progressive Business Services (PTY) Ltd (Accountant) = Access to Tax-Related Information

- 6.7.2. **Loss and/or damage of personal information**, through *back-ups onto external hard drives, remote wiping of computers and devices stolen / lost, marking scheme property (such as devices, books, etc. that could contain personal information as “confidential, property of Dr Kantor, if found please return to Dr Kantor), IT protections against file corruption, version control systems.* At the practice there is a security sign-in desk downstairs, cameras on the floor, the door to the office is locked, and the patient files are locked in cupboard. At home there is a security sign-in desk downstairs and camera. The files are locked in cupboard inside the home. Any patient related information that is on the PC, is password protected and has an anti-virus program installed.
- 6.7.3. At the Practice Office there is a security sign-in desk downstairs, cameras on the floor, the door to the office is locked, and the patient files are locked in cupboard. At the Home Office there is a security sign-in desk downstairs and camera. The files are locked in cupboard inside the home. Any patient related information that is on the PC, is password protected and has an anti-virus program installed.
- 6.7.4. **Archiving and Destruction** will only take place in accordance with the Practice Document Retention and Destruction policy and guide, and all **archiving** and **destruction** will be documented in **one register** kept with **Dr Kantor**.
- 6.8. No Practice database, list, personal information of any person in its, or any staff member or office bearer's possession may be used, made known and/or distributed without the concerned Data Subjects' consent. In case of doubt, the advice of the Information Officer or his/her Deputy will be sought. Even casual provision of contact details to a third party could constitute a breach of the POPI Act.
- 6.9. Only relevant Personal Information required for the specified purpose should be collected - nothing in excess of that. The data fields (see definition of “personal information” and “special information”) in all existing and new databases and types of information (e.g. contracts, financial information, marketing lists, etc.) will be evaluated as to whether that specific data field is:
- 6.9.1. Necessary, given the specific purpose for which the personal information will be used.
- 6.9.2. Relevant for that purpose.
- Red flag data fields are titles (relevant for communication, but not necessarily for the allocation of benefits), family relation (relevant for membership, but not for communication, etc.), information on race, gender, ethnicity (unless required by the B-BBEE Act, EEA, or other law), physical address, views / opinions of persons, contact details (only was person consented to and what is relevant for that database should be kept), etc. The physical address of a trustee is necessary, but the address of a payments clerk at a customer or vendor is not required.
- 6.10. All communications of a marketing or general communications nature must be subject to an “opt out” functionality, which has to be adhered to strictly by The Practice or anyone processing Personal Information for and on behalf of The Practice. The Data Subject's consent must be obtained on Form 4 as set out in the Regulations published under GG number 42110 dated 14 December 2018. Information related to changes to practice policies, etc. or any right or legitimate expectation of a staff member or a supplier / vendor cannot opt out of. Neither can they opt out of statements and similar information directly related to their contractual or other legal relationship with the Practice.
- 6.11. All requests for Personal Information and other information from any person or entity whatsoever shall be dealt with in accordance with the provisions of The Practice PAIA Manual and in line with this policy.
- 6.12. The Data Subject must be provided access to their Personal Information related upon written request and other request for access to personal and other information from any person or entity must be dealt with in terms of The Practice PAIA Manual and in line with this policy.
- 6.13. All processing of Personal Information must immediately cease, in the event that the Data Subject withdraws its consent to the processing or objects to the processing of Personal Information in the manner prescribed by law, except where The Practice is by law obliged to continue with such processing. Such requests must be made to the scheme on **Form 1** of the POPI Regulations.
- 6.14. Personal Information must be corrected or deleted upon request contained in Form 2 by the Data Subject to do so.

7. SECURITY AND ACCESS

The Practice uses the following security measures to secure Personal Information in her possession:

- 7.1. Electronic information is secured by firewalls, anti-virus and password secured access;
- 7.2. Electronic information on shared drives operates on access control and permissions, accidental access must be reported to the Information Officer and IT immediately.
- 7.3. No information, including personal information, may be downloaded from shared drives onto device hard drives or any external device.
- 7.4. Physical records are kept at the office and at home and protected by locked cupboards and locked rooms and the keys are kept by [Dr Linda Kantor](#) & [Mrs. Lina Kantor](#) ([Dr Kantor's mother](#)):
 - 7.4.1. At the practice there is a security sign-in desk downstairs, cameras on the floor of her office, the door to the office has a keypad, and the files are locked in cupboard inside the rooms. At home there is a security sign-in desk downstairs, and the patient files are locked in cupboard. Any patient related information that is on the PC, is password protected and has an anti-virus program installed.
- 7.5. The office has a keypad on the door.
- 7.6. There are security cameras on the floor of the office building.
- 7.7. There are security cameras *in the building*, notices are put up to this effect. All such recordings are stored off-site and will only be accessed in cases of alleged breaches of processing, including unlawful access or destruction, of personal information.
- 7.8. The office building is accessed through a *sign-in system at the main desk with security personnel, which is locked at night*. The security company act as an Operator and an Operator agreement is in place, ensuring that no personal information provided is stored for longer than necessary and are permanently destroyed after its use. Frequent visitor information is stored indefinitely at the security company in full compliance with the provisions of the POPI Act, or until a contract or assignment comes to an end. [MNG Security Services](#) is responsible for destruction of information.
- 7.9. Notification in writing to the affected Data Subjects and reporting to the Information Regulator, should the Personal Information relating to the Data Subject be compromised or should there be a suspicion that the Personal Information is compromised. Notification may have to be made to the Information Regulator. All security and access breaches or suspected or potential breaches of personal information must be reported to the Information Regulator or hi/her designated Deputy immediately after such breach or potential; breach becomes known.

8. STORAGE AND DESTRUCTION

- 8.1. All Personal Information in the possession of The Practice must be stored, retained, and destroyed in accordance with the legislation applicable to the specific information and according to the Practice Document Retention and Destruction Policy.
- 8.2. Personal Information shall not be retained longer than required to fulfil the purpose for the Processing or longer than required by Applicable Legislation.
- 8.3. Once the purpose for Processing or the retention period provided under Applicable Legislation expires, the Personal Information must be destroyed and/or deleted and/or returned to the Data Subject as may be required by the Applicable Law and in a manner that complies with such Applicable Law.
- 8.4. Retention periods, and the destruction of personal information, must be specified in consents and notifications.

9. COLLECTION OF PERSONAL INFORMATION

- 9.1. The Practice collects Personal Information from various Data Subjects for varying purposes, but mainly from patients, e.g. for patient treatment, submission of claims to medical schemes, etc. Such information must be collected in accordance with the provisions of the Act and this policy.
- 9.2. Personal information is also collected from staff for employment purposes, such as payroll, tax, and deductions, leave administration, etc. Information on staff interviews and applications are also kept until no longer needed.
- 9.3. Personal information from the staff is also processed for purposes of facilitating the goods and services to be rendered. The information of persons responsible for accounts / finances, repair persons, key account managers and the likes are processed by the practice for legitimate business purposes.

10. PURPOSE AND USE OF PERSONAL INFORMATION

When Processing Personal Information as part of any activity, the Responsible Party must:

Identify the nature and extent to which one will deal with (a) Personal Information and (b) Special Personal Information (i.e., measure the data fields through which information it is collecting to assess whether it is **relevant, necessary, and not excessive**), and then amend its processing accordingly.

- 10.1. Identify the types of processing that will take place (e.g., collection, dissemination and destruction, or collection, recording and storage, etc.).
- 10.2. Identify the purpose for which the specific processing is undertaken, clearly indicating whether such purpose is permitted by a law (e.g., invoicing requiring a VAT number).
- 10.3. Confirm that consent has been obtained from Data Subjects, which consent shall constitute a contract between The Practice and the Data Subject shall describe:
 - 10.3.1. the purpose of the Processing or further processing of the Personal Information;
 - 10.3.2. the type of Processing of the Personal Information;
 - 10.3.3. timelines related to the Processing;
 - 10.3.4. the destruction or storage of the personal information; and
 - 10.3.5. the security assurances and measures undertaken by The Practice to protect the data and Personal Information.

10.4. If processing is mandated by law, describe in a notification what that specific law says, and how processing will take place. Here the Practice refers to its Retention and Destruction Policy.

10.5. **Personal Information about children and special personal information**

10.5.1. The Practice also have information of "child-dependents" older than 18, but who are still dependent on their parents – such persons are handled, for POPIA purposes, the same as any adult dependent on the scheme.

10.5.2. The Practice will take all reasonable measures to protect the confidentiality of adult dependents and children who has the right to confidentiality but acknowledge the limitations of a medical schemes system that obligates, under regulation 5 to the Medical Schemes Act, the inclusion of ICD10 (diagnostic) codes on accounts to medical schemes, and hence on statements issued by the scheme to the main member.

10.6. **Information shared by managed care organisations or pursuant to a managed care arrangement**

The Practice has managed care arrangements with certain medical schemes. In such cases the Personal Information of the patient and/or main member is provided to the medical scheme as well as a diagnostic code in order for the Practice to submit claims to the medical scheme in order to get reimbursed for the services rendered. In the Terms and Conditions of the Practice, consent for this is obtained from the patient.

The Practice undertakes to obtain the written consent of the patient in the event that other additional personal information of the patient is required by the medical scheme other than the information that is necessary for the processing of claims.

10.7. **Information shared by The Practice**

The Practice will only share information with third parties:

10.7.1. upon the specific consent of the Data Subject in terms of the Act and on written declaration that such third parties comply with the Act and related data legislation and regulations, or

10.7.2. if otherwise required to do so by any Applicable Law.

11. **REVIEW AND AMENDMENT**

This policy shall be reviewed every two years or more frequently as may be required and may be amended from time to time as may be required by law, for corrections of material errors, as the case may be.

12. **TRAINING AND COMMUNICATION**

Although the practice does not employ employees, the [Administrative Assistant](#) will be aided in attending POPI webinars or other training that may become available and to which [Dr Kantor](#) will discuss with the [Administrative Assistant](#) to attend. When [Dr Kantor](#) feels the need to appoint a full-time employee in the future, such person will be duly trained on the processing of the **Personal Information** of the patients.

Operator agreements are in place with a [Billing Company](#) for Billing & Practice Management, and an [Accountant](#) for the Accounting Company to ensure the protection of personal information of patients.

13. **COMPLIANCE**

13.1. The Information Officer of the Practice: [Dr Linda Sara Kantor](#), Cell: 083 684 9358, Email: lindakantor@icloud.com

13.2. The Deputy Information Officer of the Practice: [Ms Vivienne Sheila Zaacks](#), Cell: 084 47 00047, Email: vszaacks1@gmail.com

13.3. [Dr Linda Kantor](#) shall maintain a report in relation to POPI and PAIA regarding steps and remedial steps taken in instances of non-compliance, including but not limited to:

13.3.1. Rewording of consents, standard clauses, and notifications.

13.3.2. Reporting loss, breach and/or unauthorized access of Personal Information to relevant authorities, recommending disciplinary action, etc.

13.3.3. The destruction of personal information.

13.3.4. The de-identification of personal information.

13.3.5. The implementation of specific security measures.

13.3.6. The implementation of (additional or new) access control measures.

13.3.7. The implementation of consents or notifications *ab initio*.

13.3.8. Research and verification of legislative mandates.

13.3.9. Addenda to contracts and service level agreements within business activities and/or with third parties and contractors.

13.3.10. Amendments to contract templates.

13.3.11. Disciplinary action against employees violating this policy.

~~13.3.12. Action against office bearers violating this policy, in conjunction with the Board of Trustees. (n/a)~~

13.3.13. Requirements on the submission of (regular) progress reports.

13.3.14. Obtaining expert assistance, where required.

13.3.15. Undergoing additional or further training on POPI and PAIA.

14. INFORMATION OFFICE

- 14.1. This office houses the Information Officer and her deputies: *Suite 405, the Link, Christiaan Barnard Memorial Hospital, 48 Salazar Plain, Cape Town City Centre, Cape Town, 8000*
- 14.2. Any requests or complaints may be directed to the Information Officer in writing to: *Dr L S Kantor, Suite 405, the Link, Christiaan Barnard Memorial Hospital, 48 Salazar Plain, Cape Town City Centre, Cape Town, 8000*

15. COMPLAINTS

Any complaints by any person including members and beneficiaries, employees, office-bearers, third parties or any regulator, on any allegation or actual violation of this policy or data privacy, may be directed to the Information Officer or a designated Deputy, who will handle the complaint in line with the principles of natural justice, and apply this policy, as well as the applicable laws and related policies of the Practice when doing so.

The Information Office may constitute a committee to investigate the matter, and to make findings on the complaint, and recommend action by the relevant departments, units, or structures of the Scheme. [Dr Kantor](#) will follow up with the patient to find out what the patient is unhappy about and hold a discussion to resolve the matter.


POPI ACT: OBJECTIONS, WITHDRAWALS, AMENDMENTS AND DELETIONS

- 15.1. Any person can object to processing of Personal Information, withdraw a consent to processing, requests amend or deletion of personal Information.
- 15.2. The forms to object, consent to marketing, change or request destruction of personal information are attached to the Policy, as prescribed by the Regulations to the POPI Act published under GG number 42110 dated 14 December 2018, which forms shall be made available at The Practice's offices and our [website](#). These forms will be updated upon the publishing of new forms by the Information Regulator.

Signed on this 1st day of November 2021 by:



The Practice Information Officer



Deputy Information Officer

[Forms 1, 2 & 4 are found below]

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)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2.]

<i>Note:</i>	
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:	
Postal 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:	
Postal Code:	
Contact number(s):	
Fax number / E-mail address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11 (1) (d) to (f) <i>(Please provide detailed reasons for the objection)</i>

Signed at

Day

Month

Year

Sign or Print Name 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)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3.]

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:	
Postal 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:	
Postal Code:	
Contact number(s):	
Fax number/ E-mail address:	
C	INFORMATION TO BE CORRECTED / DELETED / DESTROYED / 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 <i>(Please provide detailed reasons for the request)</i>

Signed at

Day

Month

Year

Sign or Print Name of data subject/designated person

FORM 4

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.]

PART A	
TO:	
<i>(Name of data subject)</i>	
FROM:	
Contact number(s):	
Fax number:	
E-mail address:	
<i>(Name, address, and contact details of responsible party):</i>	
<i>Full names and designation of person signing on behalf of responsible party:</i>	
<i>Signature of designated person:</i>	
DATE:	

PART B	
I,	
<i>(Full names of data subject):</i>	
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:	
Email:	
SMS:	
OTHER - SPECIFY:	

Signed at

Day

Month

Year

Sign or Print Name of data subject/designated person