

KEY ONCOLOGICS (PTY) LTD

POLICY

in terms of

PROTECTION OF PERSONAL INFORMATION ACT 04 OF 2013

(the "ACT")



TABLE OF CONTENTS

1. Purpose
2. Scope
3. Definitions
4. Abbreviations
5. Policy
6. Key Oncologics Requirements for Processing Personal Information
7. Conditions of Lawful Processing of Personal Information
8. Security and Access
9. Storage and Destruction
10. Collection of Personal Information
11. Purpose and Use of Personal Information
12. Review and Amendment
13. Training and Communication
14. Compliance
15. Information Office
16. History of Updates

Attachment 1 – Form 1

Attachment 2 – Form 2

Attachment 3 – Form 3

Attachment 4 – Form 4

Attachment 5 – Form 5



1. PURPOSE:

The policy for the Protection of Personal Information was developed to ensure compliance with the Protection of Personal Information Act, Act 04 of 2013.

2. SCOPE:

- 2.1. This policy applies to all Key Oncologics (Pty) Ltd employees, officers, members and any other person or entity that may process Personal Information for and on behalf of the Company.
- 2.2. This policy shall apply to all situations and business processes where Personal Information is collected and/or processed and more importantly, where such information may be made accessible to third parties.
- 2.3. The policy must be read with the Key Oncologics (Pty) Ltd PAIA Manual (POPI 02).

3. DEFINITIONS:

- 3.1. **“Applicable Legislation”** means all legislation applicable to the Company including POPI, 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; Skills Development Levies Act 9 of 1999; 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 8 of the Company's PAIA Manual, Medicines and Related Substances Act 101 of 1965.
- 3.2. **“The Company or Key Oncologics”** means Key Oncologics (Pty) Ltd.
- 3.3. **“Data subject”** means the person to whom personal information relates as defined under the Act.
- 3.4. **“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.
- 3.5. **“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, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.
 - 3.5.2. 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.

- 3.5.3. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other particular assignment to the person.
- 3.5.4. The fingerprints or blood type of the person.
- 3.5.5. 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.
- 3.5.6. 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.
- 3.5.7. The views or opinions of another individual about the person.
- 3.5.8. 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.
- 3.5.9. 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.
- 3.5.10. 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, organization, 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.
 - 3.7.3. Merging, linking, as well as restriction, degradation, erasure or destruction of information.
- 3.8. **“Purpose”** means Key Oncologics purpose to processing Personal Information as set out under the Key Oncologics PAIA Manual.
- 3.9. **“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, sex life or biometric information of a data subject; or (b) criminal behavior, as defined under the Act.
- 3.10. **“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.

4. ABBREVIATIONS:

CCTV	:	Closed Circuit Television
GG	:	Government Gazette
KARMP	:	Key Assist Risk Management Program
PAIA	:	Promotion of Access to Information Act
POPI	:	Protection of Personal Information
POPIA	:	Protection of Personal Information Act
SOP	:	Standard Operating Procedure
WI	:	Working Instruction

5. POLICY:

- 5.1. The purpose of the Protection of Personal Information, Act 04 of 2013 ('the Act') is to give effect to the Constitutional Right to privacy, in order to safeguard personal information as and when processed by a responsible party, subject to justifiable limitations.
- 5.2. The Act and the Regulations promulgated in terms thereof require the Information Officer 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).
- 5.3. The Company therefore developed a policy in compliance with the Act and Regulations to provide a compliance framework within which the Company, its officers and employees will be required to process Personal Information.
- 5.4. The Company, utilizing this policy, makes a commitment to protect the rights of Data Subjects as required by the Act and various pieces of legislation that apply to the processing of Personal Information.

6. KEY ONCOLOGICS REQUIREMENTS FOR PROCESSING PERSONAL INFORMATION:

- 6.1. All Processing of Personal Information held by the Company must be done on a written consent document signed by the Data Subject.
- 6.2. The Company has developed and approved standard consent forms, refer to WI 20 – Creating and Managing Consent Forms and KARMP for official documents. All persons processing Personal Information for and on behalf of the Company shall only use said consent forms. Any deviation from this provision or material amendment to the form must only be affected with the prior written consent of the Information Officer.
- 6.3. The consent forms can be located on the company's share drive.
- 6.4. A new form must be downloaded for use for each recording to ensure that the most recently updated template is used.



- 6.5. Where there is a legal requirement to disclose or process Personal Information and consent is not required by law, the Data Subject must still be notified of such disclosure, unless the applicable law, or section thereof proves otherwise.
- 6.6. Personal information collected by the Company and/or any of its representatives or subsidiaries, will not be collected directly from the data subject, unless:
- 6.6.1 The information is contained or derived from a public record or has deliberately been made public by the data subject.
 - 6.6.2 The data subject or a competent person where the data subject is a minor, has consented, to the collection of the information from another source.
 - 6.6.3 Collection of the information from another source would not prejudice a legitimate interest of the data subject.
 - 6.6.4 Collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; in the interest of national security; or to maintain the legitimate interests of the Company or of a third party to whom the information is supplied.
 - 6.6.5 Compliance would prejudice the lawful purpose of the collection.
 - 6.6.6 Compliance is not reasonably practicable in the circumstances of that instance.
- 6.7. Personal information must only be collected for a specific, explicitly, defined and lawful purpose, related to the function or activity of the Company.

7. 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 of the Company must do so in terms of the below conditions in order to ensure compliance with the Act. The provisions are:

- 7.1 There are 8 conditions that shall apply, and which are relevant for the lawful processing of personal information:
- 7.1.1 Accountability
 - 7.1.2 Processing limitation
 - 7.1.3 Purpose specification
 - 7.1.4 Further processing limitation
 - 7.1.5 Information quality
 - 7.1.6 Transparency (honesty and integrity)



7.1.7 Security safeguards

7.1.8 Data subject participation

- 7.2 Ensure that all the conditions and measures required by 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.
- 7.3 Personal Information must only be processed with the consent of the Data Subject, for a specific, explicit and lawfully defined purpose. This must be related to the functions and activities of the Company, unless the processing is a legal requirement and consent is not required, in which case clause 0 will be applicable. Refer to Attachment 4 – Form 4.
- 7.4 In the event of a requirement to use Personal Information outside the scope of the consented purpose, (“further processing”), then a follow-up consent for the further processing must be obtained from the Data Subject, prior to such further processing.
- 7.5 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 to the collection.
- 7.6 Only current and correct Personal Information must be processed. The Responsible Persons must ensure that the security measures put in place by Key Oncologics, refer to the Company’s PAIA Manual, are used to secure the confidentiality and privacy of the Personal Information.
- 7.7 No one should sell or otherwise make available the Company databases for the distribution of any material without the Data Subjects’ consent.
- 7.8 Only relevant Personal Information required for the specified purpose should be collected.
- 7.9 All communications of a marketing or general communications nature must be subject to an “opt out” functionality, which has to be strictly adhered to. 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. The only exception to this requirement is information that the Company is required by the constitution to communicate, such as informing Members of important developments in the industry, issuing of invoices for membership fees, etc.
- 7.10 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 Company’s PAIA Manual (POPI 02) and in line with this policy.
- 7.11 The Data Subject shall be provided access to their Personal Information, which was released, only on his/her written request.
- 7.12 Any other request for access to personal and other information from any person or entity must be dealt with in terms of the Company PAIA Manual (POPI 02) compliant with this policy.
- 7.13 If the Company allows the transfer of Personal Information across borders, such transfer is only allowed in compliance with conditions set out under section 72 of the Act. This requires,

inter alia, that the Data Subject consents to the transfer, unless not allowed by the applicable law and ensure prior to such transfer that the recipient is subject to a law, binding corporate rules or binding agreement which provide adequate protection to the Data Subject's Personal Information.

- 7.14 All processing of Personal Information must immediately cease in the event that the Data Subject withdraws its/his/her consent to the processing or objects to the processing of Personal Information in the manner prescribed by law. The exception being where the Company is by law obliged to continue such processing. Refer Attachment 1 – Form 1.
- 7.15 Personal Information must be corrected or deleted upon written request by the data subject if so requested. Refer Attachment 2 – Form 2.

8. SECURITY AND ACCESS:

The Company uses the following security measures to secure Personal Information in its possession:

- 8.1 Electronic information is secured by firewalls, anti-virus programmes, cloud and data encryption, password secured access and endpoint security software. If an accidental access to shared drive occurs, this must be reported immediately to the Information Officer. Access to data servers is protected by security gates and biometric fingerprint access control.
- 8.2 No information, including Personal Information, may be downloaded from shared drives onto hard drive devices or any external device.
- 8.3 Physical records are kept at the office and protected by lockable cabinets:
- 8.3.1 KARMP information is held in the office of the KARMP Manager, where the cabinets and the office are locked with a separate key which only the KARMP Manager has access to.
- 8.3.2 Financial and Human Resource information is held in the office of the Financial Manager, where the cabinets and the office are locked with a separate key which only the Financial Manager has access to.
- 8.3.3 Warehouse related information is held in the warehouse, where the cabinets are locked with a key and the warehouse is locked with biometric fingerprint access. Only authorised personnel have access to the key and the warehouse.
- 8.3.4 Pharmacovigilance and Medical Affairs information are held in the office of the Pharmacovigilance and Medical Affairs Manager, where cabinets and the office are locked with a separate key which only the Pharmacovigilance and Medical Affairs Manager has access to.



- 8.3.5 Marketing and Access information is held in the office of the Marketing Manager, where the cabinets and the office are locked with a separate key which only the Marketing Manager has access to.
- 8.3.6 Quality Assurance information is held in the office of the Responsible Pharmacist, where the cabinets and the office are locked with a separate key which only the Responsible Pharmacist has access to.
- 8.3.7 Quality Assurance and Compliance information is held in the office of the Quality Assurance Pharmacist, where the cabinets and the office are locked with a separate key which only the Quality Assurance Pharmacist has access to.
- 8.4 The office building can only be accessed through biometric fingerprint access control and key-lock, located at the entrance.
- 8.5 An independent armed response contractor is on 24-hour duty, patrolling the premises and controlling access to the premises.
- 8.6 CCTV is implemented for 24-hour surveillance and the security cameras are located on the outside of the office building. All recordings are stored on-site and can be accessed in cases of alleged breaches of processing, including unlawful access or destruction of personal information. The records are permanently destroyed after 3 months.
- 8.7 Anyone who requires access to Personal Information to fulfil the purposes of the Company and any legal obligations and under such circumstances where the information is legally required to be provided, is given access to the Personal Information.
- 8.8 The Company regularly verifies that the abovementioned safeguards are effectively implemented and continually assessed and updated in response to any new risks or deficiencies.
- 8.9 The Company shall notify the Data Subject in writing and report to the Information Regulator, should the Personal Information relating to the data subject was compromised or should there be a suspicion of such compromise; it is therefore each Employee's obligation to report immediately any compromise or suspected compromise of Personal information to the Information Officer in writing.

9. STORAGE AND DESTRUCTION:

- 9.1 All Personal Information in the possession of the Company must be stored, retained and destroyed in accordance with the legislation applicable to that specific information and according to SOP D11 – Document retention and destruction.
- 9.2 Personal Information shall not be retained for longer than may be required to fulfil the Purpose for the Processing or longer than required by Applicable Legislation.

- 9.3 Once the purpose for Processing or the retention period provided under the consent or Applicable Legislation expires, the Personal Information must be destructed and/or deleted and/or returned to the Data Subject as may be required and in compliance with the Applicable Law.

10. COLLECTION OF PERSONAL INFORMATION:

- 10.1 The Company collects Personal Information from various Data Subjects for varying purposes, but mainly from customers, KARMP and reporting of adverse events. Such information must be collected in accordance with the provisions of the Act and this policy.
- 10.2 Personal information is collected from staff for employment purposes, such as payroll, tax and deductions, leave administration, etc. Information on staff interviews and applications is also retained until no longer needed.
- 10.3 Personal information from the representatives, staff, agents or contractors of vendors and suppliers is processed for the purpose of facilitating the goods and services to be rendered. The information of people responsible for accounts / finances, repair people, key account managers and the likes is processed by the Company for legitimate business purposes.

11. PURPOSE AND USE OF PERSONAL INFORMATION:

- 11.1 When Processing Personal Information as part of any activity, the Responsible Party must:
- 11.1.1 Identify the nature and extent to which one will deal with (a) Personal Information and (b) Special Personal Information.
 - 11.1.2 Identify the types of processing that will take place (e.g., collection, dissemination and destruction, or collection, recording and storage, etc.).
 - 11.1.3 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, CPD requiring qualifications, Advisory Boards etc.).
 - 11.1.4 Confirm that consent has been obtained from Data Subjects, unless the applicable law does not require consent, which consent shall constitute a contract between the Company and the Data Subject and shall describe:
 - 11.1.4.1 the purpose of the Processing or further processing of the Personal Information.
 - 11.1.4.2 the type of Processing of the Personal Information.
 - 11.1.4.3 timelines related to the processing.
 - 11.1.4.4 the destruction or storage of the Personal Information; and
 - 11.1.4.5 Utilize the security assurances and measures undertaken by Key Oncologics to protect the data and personal information.

11.2 Information held by the Company

The Company retains information as set out under the Key Oncologics PAIA Manual (POPI 02) and only for its purposes.

11.3 Personal information about children and special personal information

11.3.1 The Company does process information about children. Such processing can only be done in the following instances:

11.3.1.1 with the prior consent of a competent person.

11.3.1.2 if processing is necessary for the establishment, exercising a right, or defense of a right, or an obligation in law.

11.3.1.3 processing is necessary to comply with an obligation of international public law.

11.3.1.4 processing is for historical, statistical or research purposes with the proviso that:

11.3.1.5 the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

11.3.1.6 it appears to be impossible or would involve a disproportionate effort to obtain consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

11.3.1.7 if the processing is of Personal Information which has deliberately been made public by the child with the consent of a competent person.

11.3.2 Special Personal Information must only be processed with Data Subject's consent or otherwise if required by law.

11.4 Information shared by the Company

Key Oncologics (Pty) Ltd will only share information with third parties:

11.4.1 upon receiving specific consent of the Data Subject and on written declaration that such third parties also comply with the Act and related data legislation and regulations, or

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

12. REVIEW AND AMENDMENT:

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



13. TRAINING AND COMMUNICATION:

All existing employees, officers and Executive Committee members and any person who may Process Personal Information for and on behalf of the Company, shall be trained on an annual basis on this policy and underlying legal sources on which it is based. The training will also form part of new employee induction.

14. COMPLIANCE:

15.1 The designated Information Officer of Key Oncologics (Pty) Ltd is: Magriet de Wet, magriet@keyoncologics.co.za.

15.2 The designated Deputy Information Officer is: Anlee Snyman, anlee@keyoncologics.co.za

15.3 The Information Officer shall maintain a report in relation to POPIA and PAIA regarding:

14.3.1 remedial steps taken in instances of non-compliance, including but not limited to:

14.3.1.1 Destruction of personal information;

14.3.1.2 De-identification of personal information;

14.3.1.3 Implementation of compulsory security measures;

14.3.1.4 Implementation of access control measures;

14.3.1.5 Implementation of consents, contracts and policies or service level agreements within business activities and/or with third parties and contractors;

14.3.1.6 Disciplinary action against employees violating this policy;

14.3.1.7 The submission of regular progress reports;

14.3.1.8 Obtaining expert assistance, where required; and

14.3.1.9 Training on POPIA and PAIA of designated staff.

15. INFORMATION OFFICE:

15.1. The following may be directed to the Deputy Information Officer in writing to anlee@keyoncologics.co.za

15.2.1 Complaints

All complaints received from and by any person, including employees, third parties or any regulator, on any allegation or confirmed violation of this policy or data privacy, may be directed to the Deputy Information Officer, 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 Company, when doing so.

The Information Office may constitute a committee to investigate the matter, to make findings on the complaint and recommend action by the relevant departments, units or structures of the Scheme.



15.2.2 Objections, Withdrawals, Amendments and Deletions

14.2.2.1 Any objections to processing of personal information, withdrawal of consents, requests to amend or delete Personal Information.

14.2.2.2 Objections, requests for withdrawals, amendments and deletions must be made on the forms as provided for in the Regulations published under GG number 42110 dated 14 December 2018, which forms shall be made available on our website and attached to this policy.

16. HISTORY OF UPDATES:

VERSION	EFFECTIVE DATE	REASON FOR UPDATE
01	01/07/2021	New Policy
02	01/07/2023	Routine Update
03	01/07/2025	Routine Update. Format Consistency. Addition of Abbreviations. Addition of Form 3, Form 4 and Form 5.



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, 2017 [Regulation 2(1)]

Note:

1. Affidavits or other documentary evidence in support of the objection must 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.

Reference Number....

A	DETAILS OF DATA SUBJECT	
Name and surname of data subject:		
Residential, postal or business address:		
	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		
B	DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if the responsible party is a natural):		
Residential, postal or business address:		
	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		

Name of public or private body (if the responsible party is not a natural person):	
Business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
C	REASONS FOR OBJECTION <i>(Please provide detailed reasons for the objection)</i>

Signed at this day of 20.....

.....
Signature of data subject (applicant)

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, 2017 [Regulation 3(2)]

Note:

1. Affidavits or other documentary evidence in support of the request must 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.

Reference Number....

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	
Surname:		
Full names:		
Identity number:		
Residential, postal or business address:		
	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		
B	DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if the responsible party is a natural person):		
Residential, postal or business address:		
	Code ()	
Contact number(s):		
Fax number:		
E-mail address:		

FORM 3


APPLICATION FOR THE ISSUE OF A CODE OF CONDUCT IN TERMS OF SECTION 61(1)(b) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017 [Regulation 5]

A	DETAILS OF PRIVATE OR PUBLIC BODY (APPLICANT)
Indicate whether applicant is a private or a public body:	
List class of bodies, or of any industry, profession, or vocation, you represent: <i>(Attach proof of representation)</i>	
Business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address	
B	DETAILS OF PERSON WHO COMPLETES THIS FORM
Full names of person completing this Form:	
Capacity in body:	
Does the person completing this Form have the authorisation of the body he/she represents to lodge this application? <i>(Attach authorisation)</i>	
Business address (if different from body's address):	
	Code ()

Contact number(s):	
Fax number:	
E-mail address:	
C	REASONS FOR APPLICATION FOR INFORMATION REGULATOR TO ISSUE A CODE OF CONDUCT <i>(Please provide detailed reasons for the request)</i>

Signed at _____ this _____ day of _____ 20____.

 _____

Signature of person completing form

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, 2017
[Regulation 6]**

TO:

(Name and address of data subject)

FROM:

Contact number(s):

Fax number:

E-mail address:

(Name, address and contact details of responsible party)

Dear *Mr/Ms/Dr/Adv/Prof

PART A

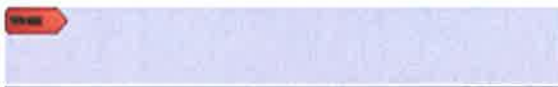
1. In terms of section 69 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), the processing of personal information of a data subject (the person to whom personal information relates) for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless written consent to the processing is given by the data subject. You may only be approached once for your consent by this responsible party. After you have indicated your wishes in Part B, you are kindly requested to submit this Form either by post, facsimile or e-mail to the address, facsimile number or e-mail address as stated above.

2. "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.

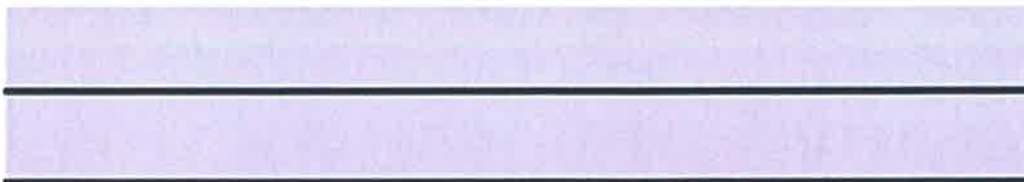
3. "Personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

- (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- (b) information relating to the education or the medical, financial, criminal or employment history of the person;
- (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- (d) the biometric information of the person;
- (e) the personal opinions, views or preferences of the person;
- (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual about the person; and
- (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.



(Signature of person authorised by responsible party)

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



Date:



PART B

I, _____ (full names) hereby:

Consent to goods and services to be marketed by means of unsolicited electronic communication.

SPECIFY GOODS AND SERVICES:

SPECIFY METHOD OF COMMUNICATION: FAX : ☐

E - MAIL : ☐

SMS : ☐

OTHERS - SPECIFY: _____

☐

Give my consent.

☐

Do not give my consent.

Signed at _____ this _____ day of _____, 20____

Signature of data subject

FORM 5

COMPLAINT REGARDING INTERFERENCE WITH THE PROTECTION OF
PERSONAL INFORMATION/COMPLAINT REGARDING DETERMINATION OF
AN ADJUDICATOR IN TERMS OF SECTION 74 OF THE PROTECTION OF
PERSONAL INFORMATION ACT, 2013(ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL
INFORMATION, 2017
[Regulation 7]

Note:

1. Affidavits or other documentary evidence in support of the request must 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.

Reference

Number.....

Mark the appropriate box with an "x".
Complaint regarding:

☐

Alleged interference with the protection of personal information

☐

Determination of an adjudicator.

PART I	
ALLEGED INTERFERENCE WITH THE PROTECTION OF THE PERSONAL INFORMATION (Section 74(1) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013))	
A	PARTICULARS OF COMPLAINANT
Surname of complainant:	
Full names of complainant:	
Identity number of complainant:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
B	PARTICULARS OF BODY/RESPONSIBLE PARTY INTERFERING WITH PERSONAL INFORMATION

Full names and surname of person interfering with personal information (if the person is a natural person)	
Name of public or private body (if not a natural person):	
Residential address (if applicable,,: postal address or business address:	
	(Code)
Contact number(s):	
Fax number:	
E-mail address:	
C	REASONS FOR COMPLAINT (Please provide detailed reasons for the complaint)
PART II	GRIEVANCE REGARDING DETERMINATION OF ADJUDICATOR (Section 74(2) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013))
A	PARTICULARS OF COMPLAINANT
Surname of complainant:	
Full names of complainant:	
Identity number of complainant:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
B	PARTICULARS OF ADJUDICATOR

Full names and surname of adjudicator	
Name and surname of responsible party (if it is a public or private body):	
Name of responsible party (if it is a public or private body):	
Residential, postal or business address:	
	(Code.)
Contact number(s):	
Fax number:	
E-mail address:	
C	REASONS FOR COMPLAINT (Please provide detailed reasons for the grievance)

Signed at _____ this _____ day of _____ 20_____

Signature of complainant/person aggrieved