



POPIA POLICY

PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013

DATE OF NEXT REVIEW:

01/02/2024

1 INTRODUCTION

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. is a medical practice, that is obligated to comply with the abovementioned Act, this Act requires DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. to inform their clients as to the manner in which their personal information is used, disclosed and destroyed.

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

This Policy sets out the manner in which DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. deals with their client's personal information as well as and stipulates the purpose for which said information is used. The Policy is made available on DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. website and by request from our office.

2 VISION, MISSION AND VALUES OF POPIA REGULATOR:

2.1 Vision

We at DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. respect your right to privacy.

2.2 Mission

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. aims to protect data subjects from harm, and ensure that their personal information is protected by being a responsible party.

2.3 Purpose

Give effect to the constitutional right to privacy, by safeguarding personal information when processed by DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC., DR MPG KITSA DR VJ RADEBE

AND PARTNERS INC T/A VAAL RADIOLOGY INC. will implement this policy to protect important interests, including the free flow of information within the Republic and across international borders.

This Policy aims 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 in DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. with this Policy provides data subjects with rights and remedies to protect their personal information from processing that is not in accordance with the abovementioned Act.

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. with this Policy is establishing voluntary and compulsory measures, to ensure respect for and to promote, enforce and fulfil the rights protected by the abovementioned Act.

3 SCOPE & DEFINITIONS

3.1 Scope:

All documents and electronic transactions generated within and/or received by the Company.

3.2 Definitions:

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

Clients includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.

Company means DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.

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

Confidential Information refers to all information or data disclosed to or Obtained by the Company by any means whatsoever.

Consent means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

Constitution: Constitution of the Republic of South Africa Act, 108 of 1996.

Data refers to information in any form.

Data subject means the person to whom personal information relates;

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, any goods or services to the data subject; or

(b) requesting the data subject to make a donation of any kind for any reason;

Documents include books, records, security or accounts and any information That has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

ECTA: Electronic Communications and Transactions Act, 25 of 2002.

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

Electronic signature refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

Electronic transactions include e-mails sent and received.

Filing system means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

Information officer of, or in relation to, a—

(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

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;

PAIA: Promotion of Access to Information Act, 2 of 2000.

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—

- (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;

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;

Public record means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

Record means any recorded information—

- (a) regardless of form or medium, including any of the following:
 - (i) Writing on any material;
 - (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

Regulator means the Information Regulator established in terms of section 39

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;

4 PERSONAL INFORMATION COLLECTED:

Section 9 of POPI states that “*Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.*”

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. collects and processes client’s personal information pertaining to the client’s specific needs. The type of information will depend on the type of matter for which it is collected and will be processed for that purpose only.

Upon signature of the consent and collection of the information, DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. will inform the client as to the information required and the information deemed optional.

4.1 Examples of personal information we collect include, but is not limited to:

4.1.1 The Client’s Identity number, name, surname, address, postal code, marital status.

4.1.2 Description of the client’s residence, business, assets; financial information, banking details, etc-.

- 4.1.3 Any other information required by DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC, in order to provide clients with the services they require.
- 4.1.4 DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. also collects and processes the client's personal information for marketing purposes should they consent thereto on the consent forms.
- 4.1.5 DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. aims to have agreements in place with all Third party service providers to ensure a mutual understanding with regard to the protection of the client's personal information.

5 THE USAGE OF PERSONAL INFORMATION

The Client's Personal Information will only be used for the purpose for which it was collected and as agreed.

5.1 This may include:

- 5.1.1 Providing services to clients and to carry out the service requested.
- 5.1.2 Conducting credit reference searches or- verification and medical aid Verifications.
- 5.1.3 Confirming, verifying and updating client details.
- 5.1.4 For the detection and prevention of fraud, crime, money laundering or other malpractices.
- 5.1.5 Conducting market or customer satisfaction research.
- 5.1.6 For audit and record keeping purposes.

5.1.7 In connection with legal proceedings.

- 5.1.8 Providing communication in respect of DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. and regulatory matters that may affect clients.
- 5.1.9 To communicate with referring physicians and medical institutions identified as necessary in the medical care of the patient.
- 5.1.10 In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

5.2 Conditions of processing:

According to section 10 and Section 4 of POPIA, personal information may only be processed if certain conditions, listed below, are met:

- 5.2.1 The client's consents to the processing: - consent is obtained from clients before the first consultation.
- 5.2.2 Processing complies with an obligation imposed by law on DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC;
- 5.2.3 Processing protects a legitimate interest of the client — it is in the client's best Interest
- 5.2.4 Processing is necessary for pursuing the legitimate interests of DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.
or of a third party to whom information is supplied — in order to provide DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.
clients with services.

5.2.5 Section 4 of the POPIA lists the following 8 conditions for processing:

- Accountability
- Processing limitation
- Purpose specification
- Further processing limitation

- Information quality

- Openness
- Security Safeguards
- Data subject participation

6 DISCLOSURE OF PERSONAL INFORMATION

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. may disclose a client's personal information to any third-party service providers whose services are necessary for the care of the particular patient.

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. aims to have agreements in place to ensure that compliance with confidentiality and privacy conditions are met, with these third parties.

DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. rights.

7 SAFEGUARDING CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information. DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. will continuously review its security controls and processes to ensure that personal information is secure.

7.1 *The following procedures are in place in order to protect personal information:*

7.1.1 THE DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. is

_____ and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPIA.

- 7.1.2 **THIS POLICY** has been put in place throughout DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. and Training on this policy and the POPI Act has already taken place and will be continuous.
- 7.1.3 Each new employee will be required to sign an **EMPLOYMENT CONTRACT** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPIA;
- 7.1.3 Every employee currently employed within DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC. will be required to sign an addendum to their **EMPLOYMENT CONTRACTS** containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI, and to ensure their compliance with the Act as Operators of DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC;
- 7.1.5 **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** archived client information is stored on site and offsite which is also governed by POPI, access is limited to these areas to authorized personal.
- 7.1.6 **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** third party service providers will be required to sign a **SERVICE LEVEL AGREEMENT** guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as Needed, and in some instance provision by the third party of their POPIA Policy will be sufficient.
- 7.1.7 All electronic files or data are **BACKED UP** by the IT Division which is also responsible for system security that protects third party access and physical threats. The IT Division is responsible for Electronic Information Security;

8 ACCESS AND CORRECTION OF PERSONAL INFORMATION

Clients have the right to access the personal information **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** holds about them. Clients also have the right to ask **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** to update, correct or delete their personal information on reasonable grounds.

Once a client objects to the processing of their personal information, **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** may no longer process said personal information. **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

9 ACCESS TO DOCUMENTS

9.1 *Disclosing information:*

All Company and client information must be dealt with in the strictest Confidence and may only be disclosed, without fear of redress, in the following circumstances
(Also see clause 9.2 below):

9.1.1 where disclosure is under compulsion of law;

9.1.2 where there is a duty to the public to disclose;

9.1.3 where the interests of the Company require disclosure; and

9.1.4 where disclosure is made with the express or implied consent of the client.

9.2 *Disclosure to 3rd parties:*

All employees have a duty of confidentiality in relation to the Company and clients. In addition to the provisions of clause 4.1 above, the following are also applicable:

9.2.1 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.

9.2.2 Requests for company information:

9.2.2.1 These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

9.2.2.2 In terms hereof, requests must be made in writing on the prescribed form to the Company in terms of PAIA. The requesting party has to state the reason for wanting the information.

9.2.2.3 Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.

9.2.3 The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

10 AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least once a year. Clients are advised to access **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** website periodically to ensure they are aware of any changes. Where material changes take place, clients will be notified directly or changes will be stipulated on **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** website.

11 RECORDS THAT CANNOT BE FOUND

If **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.**

searches for a record and it is believed that the record either does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken the attempt to locate the record, **DR MPG KITSA DR VJ RADEBE AND PARTNERS INC T/A VAAL RADIOLOGY INC.** will then also comply with the informant of the Regulator of the data breach.

12 STORAGE OF DOCUMENTS

Documents are stored in archive on location for compliance with various Acts for various reasons.

13 ELECTRONIC STORAGE

- 13.1** The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.
- 13.2** Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
- 13.3** Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for

as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

14 DESTRUCTION OF DOCUMENTS

- 14.1** Documents may be destroyed after the termination of the retention period specified by applicable legislation. Upon request of a data subject that their information be destroyed this request will be attend to as soon as possible, subject to timelines laid down by legislation.
- 14.2** Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.
- 14.3** After completion of the process in 14.2 above, the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Registration.
- 14.4** The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.
- 14.5** Documents may also be stored off-site, in storage facilities approved by the Company.

15 STRATEGIC RISK AND IMPACT MITIGATION:

15.1 Record in Master File sheet:

All the below information is recorded in the Master File. The following information is recorded and managed by the Information officer:

- 15.1.1** An inventory of all data subject's types and their personal information

15.1.2 Data subject consent and instruction to:

- hold data and reason for data held;
- use data and reason for data used;
- destroy data and reason for the destruction;
- including a time frame on all of the above
-

15.1.2 The identities of the data processors/operators

15.1.3 How the data flows into and through the Company to date of destruction

15.1.4 how access control is addressed

15.1.5 Reasons for holding subject data

15.1.6 The purpose for holding subject data

The Information officer will identify the probability factor of risks for the data subject and actively and annually manage the risks.

16 DATA PROTECTION POLICY:

The Company commits to continually uphold that the person responsible for instructing the Information Technology contractors to the Company, is the person responsible for the processing of the information.

The Company addressed all security on all personal information. Personal information is at least secure, but not limited to, in the following areas:

1. On end-points;
2. Data in transit;
3. Data stored in cloud;
4. In terms of antivirus, malware, Trojans, worms, phishing employed etc.

All Company officials, employees, vendors and clients are appropriately informed of measures taken to protect personal information and the processing of personal

information. Unauthorized persons have no access to personal information and all persons who do have access, have minimum appropriate access to personal information.

Those who hold or process information consent to full surveillance of processing of personal information and consented to personal accountability for such processing. All operators and processors committed to protect personal information and to procure instruction from the responsible party on deemed processing.

The Company procured the commitment of all operators and processors of personal information to employ maximum security and secrecy on all personal information, and to personally assume the responsibility to employ measures to protect personal information on all electronic equipment.

Mobile devices are to be treated like firearms. Devices are always kept on the processor's person. Neither the device nor any information on the device is ever given to third parties who do not hold the written consent of the data subject. Business data will always be kept separate from personal data – i.e., personal information.

Data is encrypted in order to safeguard data against unauthorized exposure to third parties. Data pertains to non-electronic files, end-point data, data in transit and hosted or cloud data. Least number of security codes are kept by least number of employees. The data specialist appointed by the Company will take into account all risk factors and address same to the satisfaction of the POPI Act. Where possible, the number of data storages is maximized.

The Company has done a risk and impact assessment on all cloud computing and is satisfied that its cloud computing adheres to the requirements of the POPI Act.

All non-electronic personal information is kept safe and rules and regulations are applicable to access of filing facilities and office spaces. Risk is reduced to the minimum on all aspects of processing personal information in that information is held behind the maximum practical guarded physical barriers as the environment allows.

All handlers of physical security acknowledged that they are responsible for compliance and undertake to ensure full compliance to the POPI Act. All personal

information will always be kept and attended to in a secure manner.

Personal information is only used for the purpose obtained as instructed by the data subject.

17 INCIDENT MANAGEMENT:

The Company has approved procedures to manage incidents that may have an impact on the POPI Act. Roles and responsibilities are known to all responsible 4 operators and data processors, and ready to be implemented when incidents occur.

All heads of department are in full control of all personal data and vowed to keep personal data safe and secure. Steps have been taken to reduce incidents and to increase the speed in which incidents are attended to. Operators and processors of personal information are forewarned to report incidents as soon as possible and managers are forewarned to attend to reports as soon as possible.

17.1 Data breach action plan:

17.1.1 All parties related to the incident will assist one another to attend to a breach as soon as possible with maximum allowed force.

17.1.2 When an incident occurs, the incident, in compliance with the POPI Act will not be discussed with anyone but the employee's direct manager.

17.1.3 Managers may only discuss incidents with the CEO.

17.1.4 The CEO may only discuss the matter with the board of directors, whereafter the board will direct the CEO.

17.1.5 Once a breach is confirmed, the CEO will communicate, as prescribed by the POPI Act, with the affected data subject, the Regulator and with those who may be influenced by the breach.

17.1.6 The following will be documented:

- All risks, incidents, and threats.
- All responses to the above.

- Number of data subjects involved, with their contact details
- Details of the breach, i.e. time, place, format of data, size of breach, reasons and possible consequences, etc.
- An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
- The Company has forms and written procedures for all steps related to the stages of breach.

18 LODGING A COMPLAINT:

If you believe we are using your personal information unlawfully, please let us know first (on _____).

You may lodge a complaint to the Information Regulator (South Africa) with the following contact details:

- Website: <https://www.justice.gov.za/infoereg/index.html>.
- Contact number: 012 406 4818.
- Fax number: 086 500 3351.
- Email: infoereg@justice.gov.za.

