PRIVACY POLICY
OF DYKES DU PLESSIS ROBERTSON ATTORNEYS
IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 (AS AMENDED FROM TIME TO TIME)

Version 4: Updated August 2025

1. INTRODUCTION

1.1 This Privacy Policy (hereinafter referred to as "**the/this Policy**") of Dykes Du Plessis Robertson Attorneys (hereinafter referred to as "**the Responsible Party**"/"**DDR**") has been prepared in terms of the Protection of Personal Information Act 4 of 2013 ("**the POPI Act**") as amended from time and has been adopted and approved by the Directors of the Responsible Party as at date hereof.

1.2 Throughout this Policy, the term "**Data Subject/s**" will refer to the client/s of the Responsible Party, who shares their Personal Information (hereinafter referred to as "**PI**") with the Responsible Party to enable the Responsible Party to render legal services to the Data Subject. A Data Subject may be a person or a juristic entity.

1.3 The Responsible Party as a law Responsible Party and specialises in all legal fields particularly litigious matters and conveyancing. Throughout this Policy, "**you/your**" refers to the Data Subject and "**we/us**" refers to the Responsible Party.

1.4 The Responsible Party is committed to protecting your privacy and to ensure that your PI is collected and used properly, lawfully and transparently. In terms of the Constitution, 1996 everyone has a right to privacy (section 14) which includes a right to protection against the unlawful collection, retention, dissemination, and use of PI.

1.5 This Policy explains how we obtain, use and disclose your PI, in accordance with the requirements of the POPI Act.

2. YOUR INFORMATION IS COLLECTED FOR A SPECIFIC PURPOSE BY US

2.1 The PI which the Responsible Party collects and processes are based on the legal services we deliver and is based on your specific instruction or mandate to us. For this purpose, we will collect your contact details including your name and/or organisation, and facts about your instruction to assist you. We will not process, and request information not required in terms of fulfilling the instruction handed to us.

3. INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS

3.1 DDR is a law firm and is the Responsible Party as defined in POPIA, based in Roodepoort, Johannesburg and specialises in all legal matters. The Information Officer is Mr B du Plessis (also a Director), whose contact details are below:

3.2 **Information Officer**
Mr Barné Jacques Du Plessis (Director) with ID no. 831019 5164 087 (Information Officer)
Telephone: +27 11 664 8188
E-mail: barne@ddrinc.co.za

3.3 **Deputy Information Officer**
Ms Brenda Croukamp

3.4 Telephone: +27 11 664 8188
E-mail: brenda@ddrinc.co.za

4. THE PURPOSE OF THE POPI ACT

4.1 The purpose of the POPI Act is to, amongst other aspects, regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy

(subject to justifiable limitations that are aimed at protecting other rights and important interests.)

4.2 **How we use your information**

We will use your personal information only for the purposes for which it was collected and agreed with you. In addition, where necessary your information may be retained for legal or research purposes. For example:

- To gather contact information;
- To confirm and verify your identity or to verify that you are an authorised user for security purposes;
- For the detection and prevention of fraud, crime, money laundering or other malpractice;
- To conduct market or customer satisfaction research or for statistical analysis;
- For audit and record keeping purposes;
- In connection with legal proceedings.

5. **WHAT IS PERSONAL INFORMATION AND PROCESSING THEREOF IN TERMS OF THE POPI ACT?**

5.1. Processing is defined in the POPI Act to include the collection, receipt, storage, recording, organisation, collation, updating or modification, usage, retrieval, retention, and destruction of PI.

5.2. PI is defined very broadly as an identifiable, living, natural person's information and, where applicable, an identifiable, existing juristic person's information, including:

5.2.1 any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other assignment to the person;

5.2.2 the name of the person as it appears with other personal information relating to that person or if disclosure of the name itself would reveal information about the person;

5.2.3 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;

5.2.4 biometric information of the person;

5.2.5 the personal opinions, views, or preferences of the person;

5.2.6 the views or opinion of another individual about the person; information relating to the education or the medical, financial, criminal or employment history of the person.

5.3 To assist the Information Officer with discharging their duties there is an appointed deputy Information Officer. Any concerns arising regarding potential and existing clients should be escalated to the Information Officer/Deputy.

6. **RIGHTS OF DATA SUBJECTS**

6.1 In terms of section 5 of the POPI Act certain rights are afforded to Data Subjects. These rights include:

6.1.1 **Notification of the information being collected and for what purpose**

6.1.2 **Data Subjects may establish what information the Responsible Party holds and the right to request access to such information.**

A request for access to information may, depending on the circumstances, be subject to the Promotion of Access to Information Act ("**PAIA**") and the PAIA Manual of the Responsible Party. Please note that such request for access to information may be subject to a payment of a legally allowable fee in terms of the PAIA Manual.

6.1.3 **Object to the processing of the Data Subject's information.**

Data Subjects are not obliged to consent to the processing of their PI or to provide their PI for the purposes of being included in the Responsible Party's marketing database. Please note that the Responsible Party must comply with FICA (Financial Intelligence Centre Act 38 of 2001 as amended from time to time) and the Responsible Party is required to obtain and retain certain PI as an *accountable institution* as defined in the FICA.

6.1.4 **Request correction, destruction, or deletion of their PI.**

6.1.5 **Refuse processing of PI for purposes of sending direct marketing**

Direct marketing via electronic communication (like emails, SMSs, and automated calls) requires explicit consent from the data subject, with exceptions for existing customers and a one-time consent request for

non-customers.

6.1.6 **Lodge a complaint at the Information Regulator**
A Data Subject may complain to the Information Regulator and institute civil proceedings if the Data Subject is of the opinion that their rights were breached in terms of the POPI Act.

7. OBLIGATIONS OF THE RESPONSIBLE PARTY AND THE CONDITIONS OF LAWFUL PROCESSING –

7.1. In terms of Chapter 3 of the Popi Act, the establishment of minimum requirements for processing of PI consist of eight conditions, namely:

7.1.1 Condition 1 - Accountability.
7.1.2 Condition 2 - Processing limitation (consent needed).
7.1.3 Condition 3 - Specific purpose.
7.1.4 Condition 4 - Further processing limitation.
7.1.5 Condition 5 - Information quality.
7.1.6 Condition 6 - Openness.
7.1.7 Condition 7 - Security safeguards.
7.1.8 Condition 8 - Data subject participation.

7.2 **Accountability**
The responsible party must ensure that the conditions and all the measures set out in the Act that give effect to such conditions, are complied with at the time of the determining the purpose and means of the processing.

7.3 **Processing Limitation**
Any further processing must be compatible with the original purpose for which the information was collected. This means that if information is collected for one specific purpose, it cannot be used for a completely different purpose without the data subject's proper justification and consent.

7.4 **Purpose Specification**
The PI of the client shall be retained to carry out the mandate, for birthday notifications, anniversary notifications and/or for marketing the services of the Responsible Party and its affiliates as provided for in the Responsible Party. As provided for in the Responsible Party Consent Form the PI of the Data Subject shall be retained until the Data

Subject requests for the destruction or deletion of such information or otherwise requests to be removed from the Responsible Party's marketing database. At such time the Information Officer shall as soon as practicable ensure that such information is destroyed and deleted. In terms of FICA, records are stored for 5 years.

7.5 **Further Processing**
Further processing of PI may occur if approved by management from time to time, in accordance with the consent contained in the Responsible Party Consent Form. By signing the consent form, you agree hereto, should this ever be necessary, in line with the services rendered by the Responsible Party and/or its nominated service provider's operations in terms of processing data.

7.6 **Information Quality**
The Information Officer must take all reasonable steps to ensure that the information uploaded to the relevant physical and electronic/marketing databases are complete and accurate, are not misleading and are updated where necessary.

7.7 **Openness**
7.7.1 A Data Subject may request a copy of the Responsible Party's PAIA Manual (Promotion of Access to Information Act) a copy of which will be provided by the Information Officer on request. This Manual will indicate the process to follow, should a Data Subject require access to certain information, at a fee set

out in the Manual.

7.7.2 Use of Cookies on the website

7.7.2.1 Cookies, in their simplest form, are small clusters of data. A web server passes these data clusters through to your computer after you've landed on a website. Your computer then stores the data as files inside your browser cache.

7.7.2.2 The website of the Responsible Party makes use of cookies, which cookies use the data of Data Subjects visiting the website. Almost all websites contain cookies that, for example, assist with the following:

- to remember what sites you've visited in the past so you can view your browser history
- verify user login details
- improve the overall functionality of the website
- cookies may be used by other third-party entities (e.g. the server) but this is not a danger and can be managed.

7.8 **Direct Marketing**

The Consent Form to receive Direct Marketing must be signed by the Data Subject personally or given telephonically and thereafter recorded as to ensure that the Data Subject's choices are respected. In the event that the Responsible Party sends direct marketing, Data Subject consent may be obtained via phone or an automated system and the call will be recorded and stored for future access.
Consent for direct Marketing communication may be stored on file or on the Responsible Party's electronic database. Consent to receive direct marketing from the Responsible Party must be explicit and is cost-free.

7.9 **Security Safeguards**

7.9.1 The Responsible Party must secure the integrity and confidentiality of PI in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –

7.9.1.1 loss of, damage to or unauthorised destruction of personal information; and

7.9.1.2 unlawful access to or processing of personal information.

7.9.2 The transmission to the Responsible Party of information via the internet or a mobile phone network connection may not be completely secure, and any transmission is at the Data subject's risk. The Responsible Party will use its best endeavours to provide adequate protection for the PI held and to stop unauthorized access.

7.9.3 Security policies and procedures of the Responsible Party cover:

7.9.3.1 physical security;
7.9.3.2 computer and network security;
7.9.3.3 access to personal information;
7.9.3.4 secure communications;
7.9.3.5 security in contracting out activities or functions;
7.9.3.6 retention and disposal of information;
7.9.3.7 acceptable usage of personal information; and
7.9.3.8 governance and regulatory issues.

7.9.4 When contracting with third parties, the Responsible Party impose appropriate security, privacy, and confidentiality obligations on them to ensure that personal information that we remain responsible for, is kept secure. The Information Officer shall identify all reasonably foreseeable internal and external risks to PI in its possession or under its control.

7.9.5 The Information Officer shall take such steps and shall ensure that the Responsible Party's POPI Act obligations are carried forward into any such services contract and that service providers that may store and/or process such information from time to time agree to comply with the terms of this Policy and the applicable statutory obligations.

7.9.6 If PI is accessed or acquired by any unauthorised person, the Information Officer must notify the Information Regulator and the Data Subject as soon as reasonably possible.

7.9.7 PI is not kept for longer than necessary after the mandate is carried out (subject to FICA obligations placed on the Responsible Party).

7.10 **Data Subject Participation**

7.9.1 Data Subjects may object to the use of their personal information / request corrections via any communication channel, including virtual platforms and includes using SMS, WhatsApp, phone, and/or email. Businesses must respond to such requests within 30 days.

7.9.2 On request from a client and subject to the Financial Intelligence Centre Act 38 of 2001 (as amended), the Information Officer shall as soon as reasonably possible correct, destroy or delete the personal information.

8. PROCESSING OF PERSONAL INFORMATION RELATING TO CHILDREN

Information regarding children shall only be stored and processed with the prior consent of a competent authorised person (guardian, parent, next of kin) as provided for in the Responsible Party Consent Form. Prior authorisation may be required from the Information Regulator particularly if this information is to be processed abroad.

9. DISCLOSURE OF INFORMATION

9.1 We may disclose your PI to the service providers who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with the privacy requirements as required by the POPI Act. We may also disclose your information:

9.1.1 where we have a duty or a right to disclose in terms of law; and/or

9.1.2 where we believe it is necessary to protect the Responsible Party's rights.

10. AMENDMENTS TO THIS POLICY

Amendments to this Policy may occur from time to time and will be available on the Responsible Party's website with the date of the amendment/s to the Policy provided on page 1.

11. TRAINING

11.1 Training on the practises employed by the Responsible Party to try and protect the PI of data subjects will be explained to staff in training sessions as and when required. The manner of implementing this will be done by scheduling any of the below:

11.1.1 meetings involving staff and administrative personnel and for all new employees of the Responsible Party;

11.1.2 face-to-face training or online group sessions, when important changes occur in legislation or based on company policy and as frequently as the board of Directors may direct. Training and individual refresher training will also be available to employees on request.

12. NON-COMPLIANCE AND PENALTIES FOR NON-COMPLIANCE

12.1 Compliance will be enforced by an Information Regulator, which will have far-reaching powers. The legislation provides for the following penalties for non-compliance:

12.1.1 months to ten years' imprisonment; or

12.1.2 Up to R 10 million fine or civil remedies.

12.2 Failure by any employee to comply with this Policy and/or the POPI Act will expose such employee to disciplinary procedures or may expose the staff member and the Responsible Party to criminal penalties which could be severe in the event of non-compliance, alleged or suspected non-compliance with the POPI Act. Disciplinary hearings could ensue, and the staff member be held responsible for non-compliance which could result in dismissal.

13. QUERIES - CONTACT DETAILS OF THE REPSONSIBLE PARTY AND INFORMTION REGULATOR

13.1 If you have any queries about this Policy or privacy practices, wish to withdraw consent or exercise any of your rights in terms of the POPI Act, please contact us at the numbers/addresses listed on our website or contact us on our office landline on 011 664 8188. You may also email the Head Information Officer at: barne@ddrinc.co.za or the Deputy at brenda@ddrinc.co.za.

15.1 Should you wish to lay a complaint at the Information Regulator the details are:
Address : 54 Maxwell Dr, Woodmead, Sandton, 2191
Phone: 010 023 5200
E-mail: enquiries@inforegulator.org.za
Website : https://inforegulator.org.za/

Last review and Update: AUGUST 2025