POPIA & PAIA POLICY

1. Introduction and Overview

This policy explains how we obtain, use and disclose your personal information, in accordance with the requirements of the Protection of Personal Information Act 4 of 2013 ("POPIA"). At Smuts & Co we are committed to protecting your privacy and to ensure that your personal information is collected and used properly, lawfully and transparently.

1.1 Who are we?

Smuts & Co Inc.
Registration Number 2013/008787/07
Tel: 021 824 2020

22B Church Street
Durbanville, 7550
Email: info@smutsco.co.za

1.2 What information do we collect?

If you make use our legal services, personal data will be required to fulfil the requirements of the mandate between you our client and the Company.

We collect the following personal information (if applicable to your specific legal requirements):

- Name
- Identification Number
- Telephone contact details
- Email address
- Physical address
- Marital status
- Financial/Banking Details
- Confidential Correspondence
- Tax Number/Vat Number

We collect and process your personal information mainly to contact you for the purposes of conducting business with you and to deliver legal services to you in terms of our mandate and to keep you informed of current matters and legislation that could be of relevance to you.

1.3 What we do not collect

- We do not collect or process personal data for any other purposes than what is outlined in this policy or instructed by the data subject (our client)
- We do not collect or process personal data from minors
- We do not collect or process any sensitive special personal data such as:
    - political opinions
    - religious or philosophical beliefs
    - trade-union membership
    - genetic or biometric data
    - health-related data
    - data concerning sex life

1.4 Responsibilities

In compliance with POPIA, Smuts & Co Inc. has the following roles and responsibilities:

- We are the responsible party (or operator) regarding your (our client's) personal information, such as email addresses, phone numbers, billing details, and other personal information required in order to provide legal services to you in terms of our mandate.
- We take adequate measures to ensure that your personal information is handled and stored safely and destroyed when necessary.

1.5 How do we look after your personal data?

We limit the amount of personal data collected only to what is necessary for the purpose, as described above. We restrict, secure and control all of our information against unauthorised access, damage, loss or destruction, whether physical or electronic.

We retain personal data only for as long as is required by law, hard copies for 7 years and 10 years for electronic records. If we retain your personal data for historical or statistical purposes, we ensure that the personal data cannot be used further. While in our possession, together with your assistance, we try to maintain the accuracy of your personal data.

2. Privacy Principles

We abide by the following POPIA principles when collecting, recording, storing, and destroying personal information:

2.1 Accountability and Security Safeguards

As your legal partner, management of your data is critical to us and a responsibility we take seriously. We have measures in place to ensure data is kept safe.

2.2 Processing Limitation

All personal information will be processed in a fair and lawful manner, will be specific to the purpose in terms of our mandate and/or with the consent of the data subject (ie. Yourself).

We will not contact/solicit you unless you have given permission to do so, or you have previously been a client with Smuts & Co and/or have engaged in direct contact with us in the past 18 months.

Consent must be voluntary, specific and informed and preferably given in writing. The person giving consent must have the capacity to consent and what is consented to must be expressed in plain language. You are entitled to withdraw your consent at any stage.

Data can be processed without consent in the following circumstances:

- To fulfil a legal obligation;
- For historical, statistical or research purposes in the public interest;
- If the information has been deliberately made public by the data subject, such as on social media;
- If the Information Regulator has authorized it;
- If it is done as part of performing a contract which involves an adult data subject; or
- To protect a legitimate interest of an adult data subject or third party to whom the PI was supplied.

2.3 Purpose Specification

Personal Information will only be processed for specific, defined and legitimate reasons. The reason for collecting information must fit in with the purpose.

2.4 Further Processing Limitation

Personal Information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Further processing is therefore limited to the original purpose.

2.5 Information Quality

We prefer to collect information directly from you (our client) where you provide us with your personal details and additional data as required for the specific purpose of our mandate. Where this is not possible, measures will be taken to verify such personal information with you.

In terms of Section 24 of POPIA and Regulation 3, a data subject may request for their personal information to be corrected/deleted in the prescribed form, unless the request is unlawful or unreasonable.

2.6 Openness

Care will be taken to notify the data subject of the collection of information. All data collected will be available to you upon reasonable request.

2.7 Data Subject Participation: Access & Information Request

In terms of Section 11(3) of POPIA and Regulation 2, a data subject may at any time object to the processing of his/her/its personal information in the prescribed form, subject to exceptions as contained in POPIA.

The promotion of Access to Information Act, 2000 (PAIA) gives third parties the right to approach private bodies and the government to request information held by them, which is required in the exercise and/or protection of any rights.
Our **Information Officer** is: Natasha Davidtz (Director)

Our **Deputy Information Officer** is: Bianca Little (Office Manager)

Refer to the PAIA Manual attached as Annexure A for the procedure and other requirements that a request must meet as prescribed by PAIA.

- Information requests can be sent to: info@smutsco.co.za
- Requests for personal information will be handled in accordance with POPIA.
- Any concerns, complaints or questions you may have pertaining to our above- stated policies can be emailed to info@smutsco.co.za

2.8 Security Safeguards

All personal information collected is protected against loss and unauthorized access. We employ the following physical safety measures within our office:

- Gated front-door access.
- Receptionist to identify/welcome visitors.
- Landlord's CCTV camera at perimeter gate

In general, you will be assigned a secretary (paralegal) and a professional (attorney) who will have access to your data. These employees are moderated by their employment contracts and the gravity of their access rights is re-enforced during induction. Staff members can only access client data if they have permission to do so. All staff, service providers and consultants are subject to a formal contract in line with the principles of POPIA.

Staff are also trained regularly and have immediate access to the following policies:

- Company Policy (general operating procedures)
- POPIA & PAIA Policy

Staff who retire, transfer from a department, resign etc. are removed immediately from mailing lists and access control lists. New staff are carefully trained before being allowed to access confidential or personal files.

We have an up-to-date Company Policy which incorporates the use of any office technology and software (e.g. telephone, mobile phone, email, internet, intranet, and remote access, etc.) by our staff. This policy is understood and signed by each user of such technology. Breach of this policy will lead to serious disciplinary consequences for staff. Our security procedures are reviewed & updated by management regularly.

3. Policies and Controls for unauthorised Access to Client Information

3.1 Paper records

- Paper records and files containing personal data are handled in such a way as to restrict access to only those persons with business reasons to access them.
- The Company shreds all discarded paper records that contain confidential information. Other secure disposal methods are in place and properly used for confidential material not on paper.
- Facsimile technology (fax machine) is not used for transmitting documents containing personal data.

3.2 Laptops and Other Mobile Storage Devices

- All laptops, cellphones and other devices capable of storing data are password protected
- Passwords used to access PCs, applications, databases, etc. are of sufficient strength to deter password cracking or guessing attacks
- Passwords are created for employees via our technical administrators, this ensures that passwords are securely managed and comply with best practices
- Personal, private, sensitive, or confidential data are not stored on portable devices
- When out of the office, laptops are kept secure at all times
- When replacing or selling laptops, hard drives are formatted
- PCs are logged off or locked when left unattended for any period of time
- Where possible, staff are restricted from saving files to the local disk as users are instructed to only save files to their allocated network drive
- Staff ensure that callers to the office or other unauthorized persons are unable to view personal or sensitive information, whether held on paper documents or information displayed on PC monitors

3.3 Data Transmissions

Data transfers only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation. In general, we do not employ manual data transfers using removable physical media (e.g. memory sticks, CDs, tapes, etc.). However, in the event it is necessary, any such encrypted media will be accompanied by a member of our technical specialists and secured from any and all threats to ensure usage will not cause security breach or damage to data.

3.4 Monitoring

Audit trails are used where technically possible, to capture instances of inappropriate access (whether internal or external), addition, deletion, or editing of data. Access to files containing personal data is monitored by supervisors on an ongoing basis. Staff are aware that this is being done. IT systems are in place to support this supervision.

3.5 We also take the below precautions:

- Privileges are allocated on a need-to-use basis, and only after authorization
- Staff access rights are reviewed at regular intervals
- Staff are advised on how to select and maintain secure strong passwords. Domain account passwords are regularly updated and encrypted.
- Additional phone number confirmation security for all authorized users. This additional security measure ensures that no unauthorized users/hackers can breach access without secure verification.
- Staff and sub-contractors are made aware of the security requirements and procedures for protecting unattended equipment
- Minimum amount of personal information (PI) necessary for a specific & lawful purpose is collected
- Process as little information as possible (principle of minimality)
- Ensure the accuracy of the procession of the PI
- Retain the PI for the minimum time possible
- Ensure that PI is safely stored and that is controlled
- Train staff in their obligations concerning the processing of PI
- Destroy all PI that is no longer required in a lawful manner
- Off-site server replication for secure data backup and retention is employed. The server is located within a secure data center with access control and complete backup power and connectivity solutions in place.

3.6 Reports & Incidents

We have a breach management plan to follow should an incident occur. There are five elements involved:

- Identification and Classification
- Containment and Recovery
- Risk Assessment
- Notification of Breach
- Evaluation and Response

3.6.1 Identification and Classification

Although we do everything technologically possible to ensure data security, we have also put procedures in place that will allow any staff member to report an information security incident. Staff are aware they should immediately report such an incident to the Information Officer and/or Deputy Information Officer. This allows for early recognition of the incident so that it can be dealt with in the most appropriate manner. The report is then reviewed by the Information Officer to confirm if a breach has actually occurred.

3.6.2 Containment and Recovery

This step limits the scope and impact of the breach of data protection procedures. If a breach occurs, the Information Officer and/or Deputy Information Officer:

- Investigate the breach and ensure that the appropriate resources are made available for the investigation.
- Establish who in the organisation needs to be made aware of the breach and begins the containment exercise.
- Establish whether there is anything that can be done to recover losses and limit the damage the breach can cause.

3.6.3 Risk Assessment

In assessing the risk arising from a data security breach, the Information Officer and Deputy Information Officer will consider what the potential adverse consequences for individuals would be, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be.

3.6.4 Notification of Breaches

If inappropriate release/loss of personal data occurs it is reported immediately internally, and, if appropriate in the circumstances, to the persons whose data it is. When notifying individuals, we shall consider using the most appropriate medium to do so.

3.6.5 Evaluation and Response

Subsequent to any information security breach a thorough review of the incident will occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

4 Systems, applications and software

4.1 Email software

We make use of Microsoft Office 365 Hosted Exchange Enterprise Server as our email platform. Microsoft uses 'encryption in transit' for all data, which means that your data is protected against eavesdropping.

4.2 Bulk email application via Succeed Group

We make use of a GDPR and POPIA compliant bulk mail platform with dedicated secure data centers via our service provider, Succeed Group. The following measures apply to the platform used for bulk email distribution. The product has been designed to prevent and withstand attacks common to web-based applications. The application makes use of industry-standard safeguards to stand up to the following types of attacks:

- **SQL Injection Attacks -** Data filtering and escape mechanisms prevent attack via SQL malware scripts.
- **Cross-site Scripting Attacks -** All input is validated and type cast to ensure input data is valid. Additionally, all queries run on the database use bound parameters (a method of escaping input) or MySQL escaped strings to prevent SQL injections.
- **File System Monitoring -** Attackers commonly target the file system on an application server. To counter these attacks we have mechanisms in place that monitor for any unauthorised file system changes. If any change is detected, the application is shut down and we are alerted to the problem so that we can investigate the issue.
- **Session Management -** We use PHP session management. It is a robust, trusted mechanism. Furthermore, we namespace and segregate all session data.

Recipients of bulk email communication have had to express a legitimate interest and have either:

- Opted in to receive newsletters, or
- Established a clear business relationship or interest by being a customer or
- Previously received regular opt-out communication or
- Engaged with bulk email communication in the past 18 months.

4.3 Intelligent Business Email

We make use of first-class email Signature and Marketing software via our service provider, Succeed Group.

Key elements for which your personal data may be collected are:

- To enable us to deliver our services to you in the capacity of Controller or Processor
- Where you have consented to doing so and only for the purpose for which they are collected
- Where it is in our legitimate interests to do so

4.4 Monthly Newsletter

We aim direct marketing to our database that has opted in as required in terms of POPIA and/or to our existing clients being clients who use our business for legal services as and when necessary. All newsletters sent out after 1 July 2021 will provide an "opt-in" selection for clients to make a voluntary, specific and informed choice of whether they want to receive our monthly newsletter.

4.5 Secure Login

We take every possible precaution to ensure that only authorised parties can log into our unique service-related applications.

5 Cross-Border flows of Personal Information

Section 72 of POPIA provides that Personal Information may only be transferred out of the Republic of South Africa in the following circumstances:

- If the recipient country can offer such data an "adequate level" of protection. This means that its data privacy lawsmust be substantially like the Conditions for Lawful Processing as contained in POPI; or
- If the data subject consents to the transfer of their Personal Information; or
- If the transfer is necessary for the performance of a contractual obligation between the data subject and the Responsible Party; or
- If the transfer is necessary for the performance of a contractual obligation between the Responsible Party and athird party, in the interests of the data subject; or
- If the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject, and if it were, the data subject, would likely provide such consent.

The Company does not do any Cross-Border transfers of any Personal Information relating to employees, clients, companies, or organization unless specifically requested thereto by the data subject which the data subject's consent.

6 Changes to this Policy

If we make any material changes, we will update same on our website. Your continued use of our services following the update means that you accept Smuts & Co's updated POPIA & PAIA Policy.

Annexure A

PAIA MANUAL

1. Introduction

This manual was prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 and to address requirements of the Protection of Personal Information Act, 2013, as per the Privacy Policy to which this manual is attached.

Nature of Business

Smuts & Co is a law firm providing legal services, hereinafter referred to as "the Company".

Contact details

Smuts & Co Inc.
Registration Number 2013/008787/07
Tel: 021 824 2020

22B Church Street
Durbanville, 7550
Email: info@smutsco.co.za

2. Who can make a PAIA request?

Records held by the Company may be accessed on request only once the requirements for access have been met. A requester is any person making a request for access to a record of the Company and in this regard, the Act distinguishes between two types of requesters:

- **Personal Requester:** is a requester who is seeking access to a record containing personal information about the requester. The Company will provide the requested information, or give access to any record about the requester's personal information, subject to the provisions of the Act and applicable law. The prescribed fee for reproduction of the information requested will be charged by the Company.
- **Other Requester:** is a requester (other than a personal requester) entitled to request access to information pertaining to third parties. However, the Company is not obliged to grant access prior to the requester fulfilling the requirements for access in terms of the Act. The prescribed fee for reproduction of the information requested will be charged by the Company.

3. Request Procedure to be followed

A requester must comply with all the procedural requirements contained in the Act relating to a request for access to a record. A requester must complete the request form enclosed herewith in Appendix 1 and submit it together with proof of payment of a request fee (if applicable) to the information officer at the physical address or email address as stated above. The request form must be completed with sufficient information to enable the information officer to identify the following:

- the record/s requested
- the identity of the requester
- what form of access is required
- the postal address or email of the requester

A requester must state that he/she requires the information to exercise or protect a right and clearly set out what the nature of the right is, so to be exercised or protected. The requester must also provide an explanation of why the requested record is required for the exercise or protection of that right.

The Company will process a request within 30 days, unless the requestor has stated special reasons which would satisfy the information officer that circumstances dictate that this period not be complied with.

The requester shall be informed in writing whether access has been granted or denied. If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of the information officer.

4. Decision

The Company will decide whether to grant or decline a request and will give notice with reasons (if required) to that effect. The 30 day period within which the Company has to decide whether to grant or refuse a request, may be extended for a further period of not more than 30 days if the request is for a large quantity of information, or the request requires a search for information that has been backed up and stored offsite and the information cannot reasonably be obtained within the original 30 day period. The information officer will notify the requester in writing should an extension be necessary.

5. Grounds for refusal of access to records in terms of PAIA

The following are the grounds on which the Company may refuse a request for access in accordance with Chapter 4 of PAIA:

- Mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of personal information would be unreasonable.
- Mandatory protection of the commercial information of a third party, if the records contain:
    a) Trade secrets of that third party
    b) Financial, commercial, scientific, or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or
    c) Information disclosed in confidence by a third party to the Company, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition
- Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.
- Mandatory protection of the safety of individuals and the protection of property.
- Mandatory protection of records that would be regarded as privileged in legal proceedings.
- Protection of the commercial information of the Company, which may include:
    a) Trade secrets
    b) Financial/commercial, scientific, or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of the Company.
    c) Information which, if disclosed, could put the Company at a disadvantage in contractual or other negotiations or prejudice the Company in commercial competition; and/or

6. Remedies available to the requester upon refusal of a request for access of PAIA

In accordance with sections 56(3)(c) and 78 of PAIA, a requestor may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

7. Fees

The Act provides for two types of fees:

- **A request fee:** which will be a standard fee of R50. This fee is exempt if requesting access to your own personal information
- **An access fee:** to be calculated according to the reproduction costs, search and preparation time and cost, including postal costs where applicable.

When a request is received by the information officer of the Company, the information officer shall by notice require the requester (other than a personal requester) to pay the prescribed request fee before further processing of the request can take place. If a search for the information is necessary and the preparation and disclosure of the information for disclosure requires more time than prescribed in the regulations for this purpose, the information officer shall notify the requester to pay as a deposit if the request is granted.

The information officer shall withhold information until the requester has paid the fee/s indicated. If a deposit has been paid in respect of a request for access which is refused, then the information officer shall repay the deposit to the requester.

8. Changes to this Policy

Any changes to this policy will be updated on our website. Your continued use of our services following the update means that you accept Smuts & Co's updated POPIA & PAIA Policy.

Request for access to the record of Private Body

(Section 53(1) of the Promotion of Access to Information Act, 2 of 2000 (Regulation 10)

A. Particulars of a Private Body

The Head:

B. Particulars of Person Requesting access to the Record

a) The particulars of the person who requests access to the record must be given below.
b) The address and/or email in the Republic of South Africa to which the information is to be sent must be given.
c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full Names and Surname:

Identity Number:

Postal Address:

Fax Number:

Telephone Number: E-Mail Address:

Capacity in which request is made, when made on behalf of another person:

C. Particulars of Person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full Names and Surname:

Identity Number:

D. Particulars of Record

a) Provide full particulars of the record to which access is requested, including the reference number if that is known toyou, to enable the record to be located.
b) If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requestermust sign all the additional folios.

1. Description of record or relevant part of the record:
2. Reference number, if available:
3. Any further particulars of record:

E. Fees

a) A request for access to a record, other than a record containing personal information about yourself, will beprocessed only after a request fee has been paid.
b) You will be notified of the amount required to be paid as the request fee.
c) The fee payable for access to a record depends on the form in which access is required and the reasonable timerequired to search for and prepare a record.
d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.

Reason for exemption from payment of fees:

F. Form of Access to Record

If you are prevented by a disability to read, view, or listen to the record in the form of access provided for in 1 to 4 hereunder, state your disability and indicate in which form the record is required.

Disability:

Form in which Record is required:

Mark the appropriate box with an X.

NOTES:

(a) Compliance with your request in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the Record is in written or printed form					
	Copy of Record*		Inspection of Record		
2. If record consists of visual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):*					
	View the Images		Copy of the Images*		Transcription of the Images*
3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack (audio cassette, CD, DVD, or digital audio format)		Transcription of soundtrack* (written or printed document)		
4. If record is held on computer or in an electronic or machine-readable form:					
	Printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (CD, DVD, or digital audio format)
*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.					

A. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign allthe additional folios.

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

B. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved/denied. If you wish to be informed in another manner, please specify that manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at_____this_____day_____of 20_____

_____

Signature of Requester/Person on whose behalf request is made