Marié de Jager Attorneys

Protection of Personal Information Policy

POPIA

Created Date: 17 March 2026

Review Period: Annually

Review Date: 17 March 2027

CONTENT:

PURPOSE

The purpose of this policy is to ensure compliance with the Protection of Personal Information Act 4 of 2013 (POPIA), safeguarding personal information in line with the Constitutional right to privacy. This policy aims to regulate the lawful processing of personal information within the firm by setting minimum threshold requirements, balancing privacy rights with access to information, and protecting key interests such as the free flow of information. In addition, it provides for the monitoring of compliance and the reporting of breaches to the Information Regulator.

POLICY STATEMENT

The firm is committed to safeguarding the privacy of its employees, clients, and website visitors. The firm takes the maintenance and protection of privacy and confidentiality very seriously, including but not limited to, commercial information, personal information, and intellectual property.

DEFINITIONS

Biometrics means any technique of personal identification that is based on physical, physiological, or behavioural characterisation, including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

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.

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.

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

Constitution means the Constitution of the Republic of South Africa, 1996.

Data subject means the person to whom personal information relates.

Day means business days, unless otherwise indicated.

Deidentify in relation to personal information of a data subject, means to delete any information that:

- Identifies the data subject;

- Can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
- Can be linked by a reasonably foreseeable method to other information that identifies the data subject.

Direct marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply any goods or services to the data subject; or
- Requesting the data subject to make a donation of any kind for any reason.

Electronic communication means any text, voice, sound, or image message sent over an electronic communications network that is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Employee means any director, partner, associate, manager or employee in the employ of the firm, including consultants

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.

Firm means Marié de Jager Attorneys.

Head means the proprietor, managing partner, or managing director of the firm, being the senior attorney in charge of the firm.

Information officer in relation to a private body, means the head of a private body as contemplated in section 1 read with section 55 of the Act. This shall include a deputy information officer appointed in terms of section 56 of the 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.

Person means a natural or juristic person.

Personal information means information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to:

- Information relating to race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth.

- Information relating to the education, medical, financial, criminal, or employment history of the person.
- Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person.
- The biometric information of the person.
- The personal opinions, views, or preferences of the person.
- Correspondence sent by the person that is implicitly or explicitly private or confidential.
- The views or opinions of another individual about the person.
- The name of the person if it appears with other personal information 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:

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use.
- Dissemination by means of transmission, distribution, or making available in any other form.
- 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.

Record means any recorded information:

- Regardless of form or medium, including:
  - Writing on any material.
  - Information produced, recorded, or stored electronically.
  - Labels, markings, or other writings identifying or describing anything.
  - Books, maps, plans, graphs, or drawings.
  - Photographs, films, negatives, tapes, or other visual images.
- In the possession or under the control of a responsible party.
- Whether or not it was created by a responsible party.
- Regardless of when it came into existence.

Regulator means the Information Regulator established in terms of section 39 of the Act.

Re-identify in relation to personal information of a data subject, means to resurrect any information that has been de-identified.

Responsible party means a public or private body or any other person which determines the purpose of and means for processing personal information.

Restriction means to withhold from circulation, use, or publication any personal information but not delete or destroy such information.

Special personal information means personal information that is more sensitive in nature and is subject to stricter processing conditions under POPIA. Based on the provision you provided, it includes:

- Religious or philosophical beliefs
- Race or ethnic origin
- Trade union membership
- Political persuasion
- Health or sex life
- Biometric information
- Criminal behaviour, specifically:
  The alleged commission of an offence by the data subject
  Legal proceedings related to such offence or the outcome of those proceedings

This type of information may not be processed unless specific exceptions under section 27 apply.

Unique identifier means any identifier assigned to a data subject that uniquely identifies that data subject in relation to a responsible party.

RESPONSIBILITY AND ACCOUNTABILITY

1. The head, together with its appointed information officer retain the accountability to ensure that the firm remains compliant with the provisions of this policy.

2. Every employee will be responsible for observing and complying with the provisions of this policy.

3. Every employee will be responsible to report any activity that constitutes non-compliance with the policy.

INFORMATION OFFICER

The information officer is:

Name:
Email:
Tel:

4. Duties of the information officer include:

4.1. Monitoring compliance with this policy.

4.2. Enforcing compliance with this policy.

4.3. Developing, implementing and enforcing any additional procedures, standards and processes, as he or she may deem necessary and appropriate, to effectuate this policy.

4.4. Working with and engaging with the Information Regulator as may be required.

4.5. Assigning duties to the deputy information officer/s.

PURPOSES OF PERSONAL INFORMATION

5. The firm will collect data for the purposes below (as required):

5.1. Billing and invoicing for legal services provided.

5.2. Client communication and updates (progress reports, case updates, requesting further information, etc.)

5.3. Client identification and verification as required in terms of the Financial Intelligence Centre Act 38 of 2001.

5.4. Compliance with regulatory and legal obligations (tax related requirements, legal filings, etc.)

5.5. Conducting legal research and case preparation.

5.6. Employment-related purposes (HR records, payroll, etc.)

5.7. Ensuring security and confidentiality of client information.

5.8. Handling complaints or disputes.

5.9. Handling requests for access to personal information.

5.10. Maintaining records of legal transactions and agreements.

5.11. Management of client trust accounts.

5.12. Managing client matters (legal advice, litigation, contract drafting, drafting Wills and other legal documents, etc.)

5.13. Managing relationships with external service providers (sheriffs, advocates, experts, consultants, court staff, etc.)

5.14. Marketing and business development, subject to consent (newsletters, client engagement, etc.)

5.15. Our services are not directed at or designed for children. However, we may need to process a child's personal information when providing legal services in certain private matters. This will only occur where required for the specific legal service and always on behalf of the parent or guardian. If the reason for needing a child's personal information is unclear, please contact our information officer for further clarification.

5.16. When it is necessary for us to process your special personal information, we will do so as part of our standard business operations, for a legitimate and lawful purpose, and in compliance with all applicable legal requirements, including POPIA.

PROCESSING OF PERSONAL INFORMATION

For the purposes stated above, the firm may collect and process personal information in various way, including but not limited to:

5.17. **Billing and Invoicing**
Personal and case-related data is processed to generate invoices, track payment status, and manage client accounts.

5.18. **Communication**
Client information is processed to communicate with clients about case progress, court dates, meetings, and billing. This may involve email, phone calls, letters, or secure portals.

5.19. **Data Analysis**
Information is analysed to assess legal matters, prepare for cases, draft documents, or provide legal advice/ services. This includes reviewing client histories, legal documents, and applicable laws.

5.20. **Data Collection**

Information collected through various means, such as client intake forms, email correspondence, phone calls, meetings, and documents provided by clients.

5.21. **Data Sharing**

Information may be shared with external parties such as courts, opposing counsel, experts, or government agencies to further a case, comply with legal obligations, or obtain required documentation.

5.22. **Data Storage**

Collected information is stored securely, usually in our electronic databases (back up servers, shared network drives within the firm, and local hard drives), practice management software, or physical files.

5.23. **Document Preparation**

Client information is used to draft legal documents such as contracts, pleadings, agreements, and other transactional documents. Personal and case details are processed to create accurate legal content.

5.24. **Record Keeping**

Records of client data, legal documents, and communication are maintained for compliance with legal, regulatory, and professional standards. **In terms of Financial Intelligence Centre Act, client information is retained for 5 years, whereas the Legal Practice Council requires client information to be retained for 7 years.**

After expiry of the mandatory record keeping period above, the records shall be destroyed.

Public records shall be disposed of in the ordinary manner, but all financial records, and/ or records that are confidential in nature shall be shredded or destroyed in an equivalent fashion as directed by the industry standards at the time.

5.25. **Security**

The firm has implemented data protection measures, including encryption, access controls, and audits to secure sensitive client information from unauthorised access, theft, or loss.

PROCESSING SPECIAL PERSONAL INFORMATION

6. The firm may process special personal information under the following circumstances:

6.1. With the data subject's consent – when explicit consent has been given for the processing of such information.

6.2. To establish, exercise or defend legal rights – when necessary for litigation, legal advice, or compliance with legal obligations.

6.3. To comply with international public law obligations – if processing is required under international legal standards.

6.4. For public interest research, statistics or history – when the purpose serves the public interest, consent is impractical, and safeguards are in place.

6.5. When the data subject has made the information public – voluntarily and knowingly.

6.6. If authorised by the regulator – where the regulator grants permission based on public interest and adequate safeguards.

Additional authorisations apply for specific categories (when required):

6.7. Religious or philosophical beliefs – we do not collect information about your religious of philosophical beliefs, where such information is required for the execution of our mandate, we will advise you and seek consent.

6.8. Race or ethnic origin – for identification when essential, or to advance legitimate interests under the law.

6.9. Trade union membership – as required for the execution of our mandate, particularly in relation to labour law matters.

6.10. Political persuasion – we do not collect information about your political beliefs and persuasions, but we may collect information about political affiliations to the extent that it may affect the execution of our mandate.

6.11. Health or sex life – when necessary for the purposes of executing our lawful mandate, especially when it relates to family law matters.

6.12. Criminal behaviour or biometric information – when necessary for the purposes of executing our mandate, especially when it relates to criminal law matters, on information required for the purposes of human resources records.

6.13. The firm may process children's personal information under these conditions:

6.13.1. With prior consent from a competent person – typically a parent or legal guardian.

6.13.2. To establish, exercise or defend legal rights – in legal proceedings or advisory services involving children.

6.13.3. To comply with international public law obligations – where necessary under international law.

6.13.4. For public interest research, statistics or history – where consent is impractical, provided safeguards protect the child's privacy.

6.13.5. Where the child, with competent person's consent, made the information public – the child has willingly disclosed the information.

6.13.6. Additionally, the Information Regulator may authorise such processing if it serves the public interest and adequate safeguards are in place. The firm will provide transparency, allow parental oversight, avoid over-collection, and implement protective measures to ensure the integrity and confidentiality of the child's data.

DISCLOSURE

7. The firm may disclose personal information to a third party under specific lawful circumstances. These include where:

7.1. The data subject has given voluntary, specific, and informed consent.

7.2. The disclosure is necessary to conclude or perform a contract to which the data subject is a party; or where required by law, regulation, or a court order.

7.3. When necessary to protect the legitimate interests of the data subject, the firm, or a third party, provided these do not override the data subject's rights.

7.4. It is required for the performance of a public duty or where the data subject has deliberately made the information public.

7.5. In the case of cross-border disclosures, information may be transferred if the recipient is subject to laws or agreements offering similar protection to POPIA, or if the data subject consents.

COLLECTION, USE, PROTECTION AND DISCLOSURE OF PERSONAL AND/ OR CONFIDENTIAL INFORMATION (AN OVERVIEW)

Collected from	Type of data collected	Application of information	Protection	Disclosure
Prospective employees	Personal and demographic information (mode: CVs; application forms; interviews)	Consideration of prospective employees; Building of prospective employee data base.	Prospective employees are asked whether the firm may retain their information. All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person).	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the prospective employee.
Employees	Personal and demographic information (mode: employee information forms; employee discussions and correspondence)	General employee administration; payroll processing; employee related statistics and reports.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person).	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the employee.

Prospective clients	Limited personal and demographic information (mode: website submission forms; consultations etc.)	To establish contact with prospective clients and/ or to assess client needs; elected correspondence.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person). Secured website with SSL security certificate. Users can unsubscribe from electronic communication where applicable.	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the prospective client.
Clients	Personal and demographic information (mode: mandate; FICA data collection documents; consultations; documentary evidence; correspondence; website etc.)	Case management; billing of clients; correspondence with clients, etc.	All information is stored on password protected computers, or in lockable cabinets behind a lockable door (when not under direct control of the responsible person). Secured website with SSL security certificate. Users can unsubscribe from electronic communication. Password protected login	Where legally required to do so; when in public interest; when in the best interests of the firm; with consent of the client.

			interface + Encryption.	

RIGHTS OF DATA SUBJECTS

8. The rights of data subjects under POPIA include the right to:

8.1. Be notified when personal information is collected or accessed by an unauthorised person.

In the event of a breach, the firm will promptly notify the Information Regulator and affected data subjects. Notifications will be issued in writing via mail, email, website, media, or as directed by the Information Regulator. The notice will outline the nature of the breach, corrective actions taken, recommended protective measures, and, if known, the identity of the unauthorised party. If necessary, the firm will publicly disclose the breach to ensure data subjects are informed and protected, always prioritising transparency and compliance with regulatory requirements.

8.2. Establish whether a responsible party holds personal information and request access.

A former, prospective, or existing client (data subject), upon proving their identity, may request confirmation, free of charge, on whether the firm holds their personal information. They may also request access to that information, including details of third-party access, within a reasonable time, format, and fee structure. The firm will provide a fee estimate and may request a deposit. The data subject must be informed of their right to request correction. Access may be refused if valid grounds under the Promotion of Access to Information Act apply, but non-exempt information will still be disclosed.

8.3. Request correction, destruction, or deletion of personal information.

A data subject may request the correction or deletion of their personal information if it is inaccurate, outdated, irrelevant, or unlawfully obtained, or request its destruction if the firm is no longer authorised to retain it. Upon request, the firm will act promptly by correcting, deleting, or justifying the information, or noting the unresolved dispute. If changes affect past or future decisions, affected third parties will be informed where practicable/ applicable. The firm will also notify you of the action taken in response to the request. The above may be requested by completing and submitting **form 2** to the information officer.

8.4. Object to the processing of personal information on reasonable grounds.

8.5. Object to the processing of personal information for direct marketing purposes.

8.6. Not have personal information processed for direct marketing via unsolicited electronic communications.

A data subject has the right to object to the processing of their personal information on reasonable grounds relating to their specific situation.
This objection applies when processing is based on the firm's or a third party's legitimate interests, or when used for purposes like direct marketing. The objection must be made in the prescribed manner. Once an objection is lodged, the firm will no longer process the information unless legislation permits it, or compelling legitimate grounds can be demonstrated that override the interests, rights, and freedoms of the data subject.
It must be understood that an objection to processing of certain information may result in the firm being unable to execute its mandate, which may result in termination of the mandate by the responsible attorney.
The above may be requested by completing and submitting **form 1**, to the information officer.

8.7. Not be subject to decisions based solely on automated processing of personal information.

A data subject may not be subject to decisions with legal or significant effects based solely on automated processing, such as profiling for work performance, creditworthiness, or health. Exceptions apply if the decision is linked to a contract and protects the data subject's interests, or if governed by law or a code of conduct with safeguards. In such cases, the firm will allow the data subject to make representations and provide enough information on the logic behind the automated decision to enable an informed response.

8.8. Submit complaints to the Information Regulator.

Any person may submit a written complaint to the Information Regulator, in the prescribed manner and form, if they believe their personal information has been interfered with or unlawfully processed. Additionally, a responsible party or data subject may lodge a complaint if aggrieved by an adjudicator's decision under section 63(3). The Regulator must provide reasonable assistance to individuals who require help in submitting their complaint.
For more information on how to lodge a complaint with the Regulator, please visit their website on https://inforegulator.org.za/complaints/.

8.9. Institute civil proceedings for interference with the protection of personal information.

A data subject, or the Information Regulator on their behalf, may institute civil action for damages against a responsible party for breach of POPIA, regardless of intent or negligence. Defences include *vis major*, Plaintiff's consent or fault, impracticality, or exemption by the Information Regulator. Courts may award compensation for patrimonial and non-patrimonial loss, aggravated damages, interest, and legal costs. If the Information Regulator brings the action, awarded amounts are deposited into a trust, with expenses deducted and the remainder distributed to the

data subject. Undistributed funds after three years revert to the Information Regulator. All court orders must be published. Settlements require court approval.

GENERAL GUIDING PRINCIPLES

9. The firm is guided by the following 8 conditions/ guiding principles for the lawful processing of personal information:

9.1. **Accountability**

The firm will take full responsibility for ensuring that all personal information is processed lawfully and in accordance with POPIA. This includes putting policies, procedures, and training in place to monitor and enforce compliance throughout the information lifecycle.

9.2. **Processing limitation**

We will only process personal information lawfully and for legitimate purposes. Processing will be minimal, relevant, and limited to what is necessary. Consent will always be obtained where required, and data will be collected directly from the data subjects unless otherwise justified.

9.3. **Purpose specification**

All personal information collected will be for a specific, explicitly defined, and lawful purposes. Records will not be kept longer than necessary unless required by law or for lawful retention. Retention and destruction practices will be clearly documented and enforced.

9.4. **Further processing limitation**

Further use of personal information will be compatible with the original purpose for which it was collected. If not, new justification or consent will be sought. We will evaluate compatibility based on the relationship between the purposes, the nature of the information, and its consequences.

9.5. **Information quality**

Personal information must be complete, accurate, and kept up to date. The firm will take reasonable steps to ensure the integrity of data at the time of collection and during use, especially when decisions are made based on that information.

9.6. **Openness**

We will maintain documented processing activities and inform data subjects when collecting their personal information. Notification will include the purpose, source (if not direct), recipients, and the subject's rights, ensuring transparency and informed participation.

9.7. **Security safeguards**

The firm has implemented appropriate technical and organisational measures to secure personal information against loss, unauthorised access, or damage. Contracts with operators will ensure compliance, and we will notify affected parties and the Information Regulator of any security compromise.

9.8. **Data subject participation**

Data subjects have the right to access their personal information and request correction or deletion where appropriate. Requests will be handled fairly, efficiently, and in the prescribed manner, ensuring transparency, responsiveness, and respect for data subject rights.

STAFF TRAINING

9.9. All employees will be provided with a copy of this policy upon engagement, alternatively employment, and this policy will be prominently available at the firm's offices, and/ or on each employee's computer; save were in the latter instance the policy may also be availed on the firm's local intranet or network (if applicable).

9.10. All employees will receive in-service training, as applicable to their job function, in respect of the application of this policy.

9.11. Structured training will be provided when there are changes in the regulatory framework and at least every 2 years. Unstructured training will provided as required to ensure compliance with this policy and to ensure awareness of the protection of personal information.

9.12. Any amendments to this policy will be brought to the attention of each employee by distributing a copy thereof to the aforesaid persons and by prominently pointing out the material changes.

REFERENCES

Destroying Records – the legal effect, Michalson L https://www.michalsons.com/blog/destroying-records-the-legal-effect/1093 (accessed November 2018).

Financial Intelligence Centre Act 38 of 2001.

Information Regulator (South Africa) https://inforegulator.org.za/ (accessed: March 2025).

Protection of Information Act 84 of 1982.

Protection of Personal Information Act 4 of 2013, and regulations.

Rules made under section 95(1) of the Legal Practice Act 28 of 2014.

FORM 1: OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.

2. If the space provided for in this Form is inadequate, submit information as an Annexure *to this Form and sign each page.*

3. Complete as is applicable.

A DETAILS OF DATA SUBJECT	
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Email address:	
B DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Email address:	
C REASONS FOR OBJECTION IN TERMS OF SECTION 11 (1) (*d*)	
(*Please provide detailed reasons for the objection*) **– attach more pages if required**	

Signed on ___ of _____.

_____

Signature of data subject/designated person

FORM 2: REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.

2. If the space provided for in this Form is inadequate, submit information as an Annexure *to this Form and sign each page.*

3. Complete as is applicable.

Mark with "X":

	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 DATA SUBJECT	
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Email address:	
B DETAILS OF RESPONSIBLE PARTY	
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
Contact number(s):	
Email address:	
C INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED	
Attach more pages if required	

D REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*a*) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24 (1) (*b*) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN
(*Please provide detailed reasons for the request***) – attach more pages if required**

Signed on ___ of _____.

_____

Signature of data subject/designated person