# PROTECTION OF PERSONAL INFORMATION POLICY

**A SANSOM ATTORNEYS INC.**
**(hereinafter referred to as the "Firm")**

**DATE OF COMPILATION: 21/07/2026**

**DATE OF REVISION: 21/07/2026**

**Version: 01**

**TABLE OF CONTENTS** **PAGE**

## 1. PREAMBLE

Chapter 3 of the Protection of Personal Information Act 4 of 2013 (POPIA) provides for the minimum conditions for the lawful processing of personal information by a responsible party. The Firm requires personal information relating to natural persons and juristic persons in order to carry out its legal, professional, administrative, employment, and operational functions. The manner in which such information is processed, stored, used, retained, and disclosed is determined by the Firm in accordance with applicable legislation and professional obligations. The Firm acknowledges its obligations in terms of POPIA, the Promotion of Access to Information Act 2 of 2000 (PAIA), the Legal Practice Act 28 of 2014, the Financial Intelligence Centre Act 38 of 2001 (FICA), and all other legislation applicable to the lawful processing, confidentiality, retention, and protection of personal information. The Firm recognises that legal professional privilege and attorney-client confidentiality remain paramount in all processing activities undertaken by the Firm. Accordingly, all processing of personal information by the Firm shall be undertaken in a lawful, reasonable, confidential, and secure manner consistent with the rights of data subjects and the professional obligations applicable to legal practitioners. The Firm undertakes to ensure that personal information processed by it is processed lawfully, fairly, and transparently; collected for specific, explicitly defined, and lawful purposes; adequate, relevant, and not excessive in relation to the purpose for which it is processed; accurate and kept up to date where reasonably practicable; retained only for as long as necessary; and protected by appropriate technical and organisational security safeguards against unauthorised access, loss, damage, destruction, or unlawful disclosure.

## 2. SCOPE AND APPLICATION

This Policy applies to all directors, attorneys, candidate attorneys, consultants, employees, temporary staff, contractors, operators, service providers, and any other persons acting on behalf of or under the instruction of the Firm who process personal information in the course and scope of their duties. This Policy applies to all personal information processed by the Firm in both physical and electronic form, including information relating to clients, employees, service providers, counsel, correspondent attorneys, litigants, witnesses, website users, and any other third parties whose information may be processed by the Firm. Compliance with this Policy is mandatory and forms part of the governance and compliance obligations of all persons associated with the Firm.

## 3. DEFINITIONS

For purposes of this Policy, unless the context indicates otherwise, the following terms shall bear the meanings assigned to them under POPIA:

**“Data Subject”** means the person to whom personal information relates.

**“Information Officer”** means the head of the private body or any duly authorised person designated in terms of POPIA and PAIA.

**“Operator”** means a person or entity which processes personal information for the Firm in terms of a contract or mandate without coming under the direct authority of the Firm.

**“Personal Information”** means information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person.

**"Processing"** means any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, retrieval, dissemination, use, distribution, destruction, or deletion.

**"Record"** means any recorded information regardless of form or medium.

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

**"Security Compromise"** means any unauthorised access to, acquisition of, disclosure of, loss of, or damage to personal information.

**"Special Personal Information"** means personal information relating to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information, criminal behaviour, or information concerning children.

**4. INFORMATION OFFICER DETAILS**

The head of the Firm acts as the Information Officer in accordance with POPIA and PAIA and is responsible for overseeing the implementation, monitoring, and enforcement of this Policy and all applicable data protection obligations. The Information Officer may designate Deputy Information Officers or authorised representatives to assist with the administration of POPIA and PAIA compliance obligations where necessary.

The Information Officer's details are as follows:

| CONTACT DETAILS | |
|---|---|
| Name of Business | A Sansom Attorneys Inc. |
| Designated contact person | Alechia Sansom (Information Officer) |
| Physical address | 26 Plataan Street, Vredekloof, Brackenfell, 7560 |
| Telephone number | 074 507 0786 |
| Email address | alechia@asansomattorneys.co.za |

**5. DATA SUBJECT RIGHTS**

Data subjects have the right to be notified that their personal information is being collected by the Firm and, where required by law, to be notified in the event of a security compromise affecting their personal information. Data subjects have the right to establish whether the Firm holds personal information relating to them and to request access to such information in accordance with applicable legislation and the Firm's PAIA Manual. Data subjects may request the correction, deletion, destruction, or updating of personal information that is inaccurate, irrelevant, excessive, incomplete, misleading, out of date, or unlawfully obtained. Data subjects may object to the processing of their personal information on reasonable grounds relating to their particular situation, subject to any legal obligations, legitimate interests, legal proceedings, or professional obligations applicable to the Firm.

Data subjects have the right to object to the processing of personal information for purposes of direct marketing by means of unsolicited electronic communications. Data subjects may lodge complaints with the Information Regulator in relation to any alleged infringement of their rights under POPIA. The exercise of certain rights by data subjects may be limited where records are protected by legal professional privilege, confidentiality obligations, legal proceedings, statutory obligations, or any lawful grounds for refusal recognised under applicable legislation.

**6. LAWFUL BASIS FOR PROCESSING**

The Firm processes personal information only where permitted by POPIA and where a lawful basis for such processing exists. Personal information may be processed where the data subject has consented to the processing; where processing is necessary to conclude or perform a contract; where processing complies with a legal obligation imposed on the Firm; where processing protects a legitimate interest of the data subject; where processing is necessary for pursuing the legitimate interests of the Firm or a third party; where processing is necessary for the establishment, exercise, or defence of a legal right; or where processing is necessary for the administration of justice, legal proceedings, or legal advisory services. The Firm will process only such personal information as is reasonably necessary and relevant for the purpose for which it is processed.

**7. PURPOSE OF PROCESSING PERSONAL INFORMATION**

The Firm processes personal information for purposes related to the rendering of legal services, litigation, dispute resolution, debt recovery, conveyancing, employment matters, labour matters, regulatory compliance, legal advisory services, trust account administration, client relationship management, procurement, accounting, taxation, recruitment, payroll administration, operational management, and compliance with legal and professional obligations. The Firm may also process personal information for purposes related to FICA compliance, verification of identity, risk management, fraud prevention, internal administration, security management, information technology support, and the exercise or protection of legal rights. The Firm undertakes not to process personal information for any purpose that is incompatible with the original purpose for which the information was collected unless such processing is permitted by law.

**8. CATEGORIES OF DATA SUBJECTS**

The Firm may process personal information relating to various categories of data subjects, including clients, prospective clients, employees, candidate attorneys, consultants, directors, service providers, suppliers, advocates, correspondent attorneys, litigants, witnesses, debtors, creditors, website users, and any other third parties whose information is processed in the ordinary course of business. The personal information processed by the Firm may include names, identity numbers, registration numbers, contact details, addresses, financial information, banking details, tax information, employment information, legal records, litigation records, compliance documentation, electronic communications, and any other information necessary for lawful business and professional purposes.

**9. PROCESSING OF SPECIAL PERSONAL INFORMATION**

The Firm may process special personal information where such processing is permitted under POPIA and necessary for lawful purposes. Special personal information may be processed where the data subject has consented to such processing; where processing is necessary for the establishment, exercise, or defence of a legal right; where processing is necessary for legal proceedings; where processing is required by law; where the information has deliberately been made public by the data subject; or where processing is otherwise permitted under POPIA. The Firm acknowledges that, due to the nature of legal services rendered, it may process special personal information relating to criminal conduct, health information, children, employment matters, financial conduct, disciplinary proceedings, and other confidential legal matters. The Firm undertakes to implement appropriate safeguards and confidentiality measures in relation to all special personal information processed by it.

**10. SHARING PERSONAL INFORMATION**

The Firm may share personal information with third parties where such disclosure is necessary for lawful business, professional, regulatory, operational, or legal purposes. Personal information may be shared with advocates, correspondent attorneys, service providers, operators, courts, tribunals, regulatory authorities, law enforcement authorities, banks, insurers, auditors, information technology providers, cloud service providers, debt collection agents, consultants, and any other persons where disclosure is necessary for the performance of professional services, compliance with legal obligations, or the protection of lawful interests. The Firm will take reasonable steps to ensure that recipients of personal information implement appropriate technical and organisational safeguards to protect such information and maintain confidentiality.

**11. OPERATORS AND THIRD-PARTY SERVICE PROVIDERS**

Where the Firm appoints operators or third-party service providers to process personal information on its behalf, the Firm will ensure that appropriate written agreements are concluded with such parties in accordance with POPIA. Operators and service providers processing personal information on behalf of the Firm shall be required to process such information only in accordance with the Firm's instructions, maintain appropriate security safeguards, implement confidentiality obligations, and comply with all applicable legal requirements relating to the protection of personal information. The Firm may conduct reasonable due diligence measures in relation to operators and service providers to ensure compliance with applicable security and confidentiality standards.

**12. CROSS-BORDER FLOW OF PERSONAL INFORMATION**

The Firm may transfer personal information to recipients located outside the Republic of South Africa where such transfer is necessary for lawful business, operational, legal, technological, or professional purposes. Cross-border transfers may occur through the use of cloud storage platforms, electronic communication systems, software applications, information technology infrastructure, international service providers, or legal and professional engagements involving foreign jurisdictions. The Firm will take reasonable steps to ensure that any cross-border transfer of personal information complies with section 72 of POPIA and that the recipient is subject to laws, agreements, binding corporate rules, or other safeguards providing an adequate level of protection substantially similar to that provided under

POPIA. Where required by law, the Firm will obtain consent from the data subject or rely on another lawful basis recognised under POPIA before transferring personal information across borders.

**13. DESCRIPTION OF SECURITY MEASURES**

The Firm implements appropriate technical and organisational measures to protect the confidentiality, integrity, and availability of personal information in its possession or under its control. Physical records are stored in secure facilities with access restricted to authorised persons only. Electronic records and systems are protected through user authentication measures, password controls, encryption technologies, anti-malware systems, firewalls, access restrictions, secure backups, and other appropriate cybersecurity safeguards. The Firm may implement multi-factor authentication, endpoint protection, audit logging, secure disposal procedures, email security protocols, role-based access controls, and monitoring measures where appropriate to reduce foreseeable internal and external security risks. All employees, contractors, and operators are required to maintain the confidentiality of personal information and comply with the Firm's security procedures and confidentiality obligations. The Information Officer may conduct periodic risk assessments, security reviews, and compliance evaluations to identify and address foreseeable security risks.

**14. ACCESS CONTROL AND REMOTE WORKING**

The Firm implements role-based access controls to ensure that access to personal information is limited to authorised persons who require such access for legitimate business or professional purposes. Employees and authorised users accessing Firm systems remotely are required to use approved devices, comply with password and authentication requirements, maintain the confidentiality of all information accessed remotely, and take reasonable steps to prevent unauthorised access to Firm systems and records. The use of personal devices, public networks, removable storage devices, or unauthorised software for processing personal information may be restricted or prohibited where necessary to protect the security and confidentiality of information.

**15. RETENTION AND DESTRUCTION OF RECORDS**

The Firm retains personal information only for as long as reasonably necessary to fulfil the purpose for which the information was collected and processed unless a longer retention period is required or permitted by law. The Firm may retain records for purposes relating to legal proceedings, prescription periods, professional indemnity requirements, regulatory compliance, taxation, employment obligations, FICA obligations, accounting obligations, operational requirements, or lawful business purposes. Where personal information is no longer required, the Firm will take reasonable steps to securely destroy, delete, or de-identify such information in a manner that prevents unauthorised access or reconstruction. The destruction of records shall be conducted in accordance with applicable legal, regulatory, and professional obligations.

## 16. SECURITY COMPROMISES AND INCIDENT REPORTING

Any actual or suspected unauthorised access to, disclosure of, loss of, theft of, or damage to personal information must immediately be reported to the Information Officer. The Firm will investigate all reported incidents and take reasonable steps to contain, assess, and mitigate the effects of any security compromise. Where required by law, the Firm will notify the Information Regulator and affected data subjects of any security compromise in accordance with section 22 of POPIA. The Firm may maintain records of security incidents, investigations, remedial measures, and notifications for governance and compliance purposes.

## 17. EMPLOYEE RESPONSIBILITIES

All employees, directors, consultants, candidate attorneys, contractors, and representatives of the Firm are required to process personal information lawfully, confidentially, and in accordance with this Policy. Employees and authorised persons must access personal information strictly on a need-to-know basis and may not disclose personal information to unauthorised persons. All persons processing personal information on behalf of the Firm are required to protect passwords and access credentials, securely store records, comply with security procedures, report suspected security incidents, and uphold legal professional privilege and confidentiality obligations. Any breach of this Policy or failure to comply with applicable data protection obligations may result in disciplinary action, termination of employment or engagement, civil liability, criminal sanctions, or any other lawful remedial action available to the Firm.

## 18. TRAINING AND COMPLIANCE MONITORING

The Firm may conduct POPIA awareness initiatives, compliance training, monitoring activities, audits, and risk assessments to promote compliance with applicable data protection obligations and this Policy. Employees and authorised persons may be required to participate in training and compliance initiatives relating to confidentiality, information security, cybersecurity awareness, records management, and lawful processing practices. The Information Officer may review compliance measures periodically and recommend amendments or improvements to governance and security practices where necessary.

## 19. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION

In accordance with section 11(3) of POPIA and the applicable Regulations, a data subject may object, on reasonable grounds relating to their particular situation, to the processing of their personal information by the Firm. A data subject may also object at any time to the processing of personal information for purposes of direct marketing by means of unsolicited electronic communications. Any objection to processing must be submitted to the Information Officer in the prescribed form and manner. Upon receipt of a valid objection, the Firm will consider the objection and take appropriate steps in accordance with POPIA, subject to any lawful basis for continued processing, including legal obligations, legal proceedings, professional obligations, or the establishment, exercise, or defence of legal rights.

## 20. REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION

In accordance with section 24 of POPIA and the applicable Regulations, a data subject may request the correction, deletion, destruction, or updating of personal information that is inaccurate, irrelevant, excessive, incomplete, misleading, out of date, or unlawfully obtained. A data subject may further request the destruction or deletion of records that the Firm is no longer authorised to retain. Any request for correction or deletion must be submitted to the Information Officer in the prescribed form and manner. The Firm may take reasonable steps to verify the identity of the requesting person before implementing any requested correction, deletion, or destruction of records. Where reasonably practicable, the Firm may notify third parties to whom the information has previously been disclosed of any material correction or deletion. The Firm reserves the right to refuse requests where retention or processing is required by law, legal proceedings, professional obligations, legal professional privilege, or any lawful basis recognised under POPIA.

## 21. GOVERNANCE AND REVIEW

The Information Officer is responsible for overseeing the implementation, administration, and monitoring of compliance with this Policy. This Policy may be reviewed, amended, or updated from time to time to ensure alignment with legislative developments, regulatory requirements, operational practices, technological changes, and evolving data protection risks. All amendments to this Policy shall become effective upon approval by the Firm.

**Issued by**

**Alechia Sansom – Information Officer**
**Director**