PRIVACY POLICY

Document Number:	8/9/P
Approved By:	Board of Directors
Approval Date:	June 2021
Next Review Cycle:	June 2024
Version:	1
Type:	Governance
Policy Owner:	Executive Manager: Business Change & Technology
Board Oversight:	Social and Ethics Committee

Contents

1. INTRODUCTION

The Protection of Personal Information Act 4 of 2013 (POPIA) introduced certain conditions to establish minimum requirements for the processing of personal information.
This policy is intended to create a framework of governance towards a sustainable privacy compliance culture within Sasria.

2. PURPOSE OF THE POLICY

To maintain the confidentiality, access to and availability of information about our customers, employees, and any other individuals Sasria will undertake business with and ensure compliance with POPIA and regulations.

The purpose of this policy is to:

2.1. Provide the basis for the implementation of the provisions of the POPIA by all Sasria employees.

2.2. Drive the commitment towards a sustained a management and promotion of data privacy culture by regulating the way personal information of Sasria clients may be processed.

3. SCOPE OF THE POLICY

Policy is applicable to all employees of Sasria.
Defined terms in this Policy are capitalized and defined, see Definition Section below.

4. DEFINITIONS

biometrics'' means a technique of personal identification that is based on physical, physiological, or behavioral characterization 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.

‘‘**data subject**’’ means the person to whom personal information relates.

‘‘**de-identify**’’, in relation to personal information of a data subject, means to delete anyinformation that—
identifies the data subject.
can be used or manipulated by a reasonably foreseeable method to identify the datasubject; or
can be linked by a reasonably foreseeable method to other information that identifies the data subject,
and ‘‘**de-identified**’’ has a corresponding meaning.

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

‘‘filing system’’ means any structured set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

‘‘information officer’’ of, or in relation to, a—
public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or
private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act.

‘‘operator’’ means a person who processes personal information for a responsible party interms of a contract or mandate, without coming under the direct authority of that party.

‘‘person’’ means a natural person or a juristic person.

‘‘personal information’’ means information relating to an identifiable, living, natural person,and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person.
(b) information relating to the education or the medical, financial, criminal or employmenthistory of the person.

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person.
(d) the biometric information of the person.
(e) the personal opinions, views, or preferences of the person.
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
(g) the views or opinions of another individual about the person; and
(h) the name of the person if it appears with other personal information relating to the personor if the disclosure of the name itself would reveal information about the person.

''private body'' means—

(a) a natural person who carries or has carried on any trade, business, or profession, but only in such capacity.
(b) a partnership which carries or has carried on any trade, business, or profession; or
(c) any former or existing juristic person but excludes a public body.

''processing'' means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating ormodification, retrieval, alteration, consultation, or use.
(b) dissemination by means of transmission, distribution or making available in any otherform; or
(c) merging, linking, as well as restriction, degradation, erasure, or destruction of information.

'Promotion of Access to Information Act'' means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

''public body'' means—

(a) any department of state or administration in the national or provincial sphere ofgovernment or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

- exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
- exercising a public power or performing a public function in terms of any legislation.

‘‘public record’’ means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether it was created by that public body.

‘‘record’’ means any recorded information—

(a) regardless of form or medium, including any of the following:

- Writing on any material.
- information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded, or stored.

‘‘Regulator’’ means the Information Regulator established in terms of section 39.

‘‘re-identify’’, in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

a. identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
b. can be linked by a reasonably foreseeable method to other information that identifies thedata subject, and

‘‘**re-identified**’’ has a corresponding meaning.

‘‘responsible party’’ means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

‘‘restriction’’ means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

‘‘unique identifier’’ means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to.

5. RELATIONSHIP WITH OTHER POLICIES

This policy must be read in conjunction with:
Records Management Policy
Records Retention Procedures
Information Technology and Security Policy
The Usage Policy

6. REGULATORY FRAMEWORK

The regulatory framework for the Privacy Policy is provided by:

- Constitution of the Republic of South Africa, 1996
- Protection of Personal Information Act, No. 4 of 2013
- Promotion of Access to Information Act, No. 2 of 2000
- Electronic Communications and Transactions Act, No. 25 of 2002
- National Archives and Records Services of South Africa Act, No. 43 of 1996
- Legal Deposits Act, No. 54 of 1997
- Public Finance Management Act, No. 1 of 1999
- Promotion of Administrative Justice Act, No. 3 of 2000
- Consumer Protection Act, No. 68 of 2008
- Basic Conditions of Employment Act, No. 75 of 1997
- Employment Equity Act, No. 55 of 1998
- Labour Relations Act, No. 66 of 1995
- Unemployment Insurance Act, No. 63 of 2002
- ISO 15489-1:2001, clause 6.2.

7. ROLES AND RESPONSIBILITIES

The Information Officer and/or Deputy Information Officer/s are responsible for:

(a) advise the data controller or data processor on data processing requirements provided under POPIA.
(b) ensure on behalf of the data controller or data processor that POPIA is complied with.
(c) facilitate capacity building of Sasria employees involved in data processing operations.
(d) provide advice on data protection impact assessment; and
(e) co-operate with the Information Regulator and any other authority on matters relating to data protection.
(f) need to ensure that-

i. a compliance framework is developed, implemented, monitored, and maintained.

ii. a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

iii. a manual is developed, monitored, maintained, and made available as prescribed in sections 14 and 51 of PAIA, as amended.

iv. internal measures are developed together with adequate systems to process requests for information or access thereto.

v. internal awareness sessions are conducted regarding the provisions of POPIA, regulations made in terms of POPIA, codes of conduct, or information obtained from the Regulator; and

vi. upon request by any person, copies of the manual are provided to that person upon the payment of a fee to be determined by the Regulator from time to time.

vii. All Privacy incidents must be reported to the Records Manager by the Deputy Information Officers

8. PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

8.1. Personal information must be processed in a lawful manner that does not infringe on the right to privacy of data subjects. Transfer of personal information across Sasria departments must be lawful and in line with relevant legislation.

8.2. Personal information in the custody of Sasria must always be protected.

8.3. All personal information breaches must be managed in a manner that achieves deterrence and prevents reoccurrence of breaches.

8.4. Complaints concerning management of personal information must be dealt with in accordance with the policy on complaints and the Act.

8.5. Privacy risk assessments must be conducted to ensure proper security safeguards are implemented.

8.6. Develop strategy and plan to mitigate the operational risk which potentially will affect safekeeping of the personal data of clients.

8.7. A standard for processing personal information as defined must be followed.

9. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The following conditions for processing of personal information will be adhered to by Sasria:

9.1. Accountability

Sasria is accountable for ensuring implementation of measures that give effect to Sasria data privacy principles and conditions of lawful processing of personal information.

9.2. Processing limitation

Sasria must implement limits to the collection of personal information. Any personal information collected must be obtained by lawful and fair means and, with the knowledge and consent of the data subjects.

9.3. Further processing limitation

Sasria must ensure that personal information is not processed for a secondary, incompatible purpose, unless that processing is compatible with the original purpose.

9.4. Purpose specification

Sasria must ensure that there is a specific and legitimate business purpose for the processing of personal information. The information is only to be used for a specified purpose.

9.5. Information quality and Accuracy

Sasria must ensure that personal information is accurate, complete, and up to date throughout the information lifecycle. Provision should be made for data subjects to be able access and correct their information.

9.6. Openness

Sasria must ensure that data subjects are informed of the purposes for which personal information is processed by Sasria.

9.7. Security

Sasria must implement security safeguards to ensure the confidentiality, integrity, and availability of personal information to the data subject. Personal information is to be kept secure to mitigate security incidents that result in unauthorised use of the information.

9.8. Collection directly from data subject

Personal information must be collected directly from data subject except where collection of the information from another source would not prejudice a legitimate interest of the data subject. Sasria

must provide data subjects with mechanisms to access, update, correct or delete their personal information.

10. RIGHTS OF THE INDIVIDUAL

Sasria must ensure that the right of the data subjects to privacy is respected throughout the information life cycle.

11. PROCESSING

11.1. Processing is not limited to electronic Personal Information but includes paper-based records. In addition, Processing encompasses an array of activities including the collection, storage, use, display, transfer, archiving, modifying, maintaining and destruction of Personal Information. Personal information must be processed in a lawful manner that does not infringe on the right to privacy of data subjects.

11.2. Prior- Authorisation must be obtained from the Information Regulator before any processing by a department if the intention is to:

a. Process any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other responsible parties.
b. Process criminal behavior or unlawful or objectionable conduct of data subject on behalf of third Parties.
c. Transfer of special personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information, or
d. Process information for purposes of credit reporting.

12. CREATION AND COLLECTION

12.1. Personal information must be collected directly from a data subject. Where the data subject is a Sasria policyholder, personal information of the data subject may be collected from an Agent Company / Intermediary which administers insurance business on behalf of Sasria, as such collection does not prejudice a legitimate interest of the data subject.

12.2. The information steering committee must assess the indirect collection procedures and determine the lawfulness, where personal information is not directly collected from the data

subject or derived from the public domain.

12.3. Personal information must only be processed by Sasria in the followingcircumstances:

12.3.1. The data subject concerned has provided informed consent.

12.3.2. Processing is necessary for conducting or performing the function of Sasria.

12.3.3. Processing complies with an obligation imposed by law on Sasria.

12.3.4. Processing protects the legitimate interests of a data subject.

12.3.5. Processing is necessary for pursuing the legitimate interests of Sasria or a third party to whom the information was supplied.

12.4. Service providers must manage personal information in terms of the agreement signedwith Sasria.

12.4.1. Data subjects must be given the opportunity to object to the collection of personal information by Sasria unless lawful grounds exist for such collection.

12.4.2. Where collection of a data subject's personal information is through an Agent Company, Intermediary or any other third party, Sasria must ensure that such parties are contractually bound to comply with POPIA.

13. SPECIAL PERSONAL INFORMATION

A register of all special personal information processed must be maintained by the relevant Departments.

14. PRIVACY NOTICES

14.1. A privacy notice must be available to data subjects upon or before the collection oftheir personal information by Sasria.

14.2. A privacy notice must be displayed and available on all Sasria's online applications and manual forms that are used to collect personal information.

14.3. The privacy notice must be drafted and updated by Information and Records Management in consultation with relevant Departments.

15. USE AND MAINTENANCE OF PERSONAL INFORMATION

Personal information must be used and maintained in line with POPIA requirements.

16. ACCESS TO PERSONAL INFORMATION

All access to personal information requests must be done in accordance with the Sasria's PAIA manual which is available on the website.

17. RETENTION AND STORAGE OF PERSONAL INFORMATION

Retention and storage of personal information will be undertaken in line with Saria's retention policy. Personal information will not be retained for no longer than necessary to fulfil the stated purposes unless a law or regulation specifically requires otherwise.

18. CROSS-BORDER TRANSFER OF PERSONAL INFORMATION

18.1. Sasria's employees must inform and submit a request to the relevant Deputy Information Officer prior to the transfer of personal information across borders.

18.2. The Deputy Information officer must assess all requests to transfer personal information across bordersand determine whether such transfer would be lawful in terms of the POPIA.

18.3. Where the transfer is assessed to be lawful in terms of the Sasria's legislative and regulatory obligations, personal information may be shared across borders.

19. COMPLAINTS MANAGEMENT

All complaints related to processing of personal information must be managed in accordance with the policy and procedures on complaints.

20. BUSINESS CHANGES

Key privacy controls must be implemented to ensure the privacy principles are upheld whenever there is a business change which requires Sasria to process personal information.

21. MONITORING

Compliance and Internal Audit within Sasria shall oversee the application of the Privacy Policy and related policies, principles, and procedures.

22. NON-COMPLIANCE AND CORRECTIVE ACTION

Information officer must report any breaches to data subject and the Regulator in terms of the Act. Non-compliance with this policy will be dealt with in line with the Sasria Disciplinary Policy.

23. TRAINING AND AWARENESS

23.1. All Sasria employees must be aware of Sasria's commitment to ensuring the lawful processing and protection of personal information.

23.2. Regular training of all relevant employees in respect of the processing of personal information.

23.3. Regular training and awareness must be conducted to ensure lawful processing ofpersonal information.