Ground Floor, Coral House,
20 Peter Place,
Lyme Park, Sandton
PO Box 803,
Cramerview, 2060
Tel +27 (0) 11 463 0105
Fax +27 (0) 11 463 0249

Sigma Risk Solutions ("The Company")
Data and Protection of Personal Information Policy

11/11/2013
15/01/2015
02/07/2021

1. Introduction and purpose

The Company may process personal information on behalf of its clients, who are registered insurers. Accordingly, the Company uses information technology systems which record and store data and personal information in relation to all insurance policies. For certain products (for example motor claims), the Company may process personal information and communicate with data subjects. All information is however received directly form the data subjects and used for purposes of claims and subsequent reporting.

The Company processes personal information of its own employees, and in this regard acts as a responsible party. The Company is also an accountable institution in terms of the Financial Intelligence Centre Act. Accordingly, it is required to identify all clients, and will as a result hold personal information relating to both juristic and natural persons, as a responsible party.

This policy is adopted in line with the Protection of Personal Information Act, 2013. The Company recognizes each individual's right to privacy as well as the competing right of access to information and the importance of effective transfer of information, and accordingly undertakes to safeguard all personal information and adopt appropriate IT safeguards.

The Company has also appointed and Information Officer and Deputy Information Officers as prescribed by the Information Regulator.

2. Implementation date

This Policy shall take effect on adoption by the Board of Directors, and shall be reviewed thereafter on an annual basis.

3. Definitions

Act	means the Protection of Personal Information Act, 2013;
Data	means all information stored relating to clients and policies that is not personal information
Data Subjects	means the person to whom the personal information relates

De-identify	in relation to personal information of a data subject, means to delete any information that— *(a)* identifies the data subject; *(b)* can be used or manipulated by a reasonably foreseeable method to identify the data subject; or *(c)* can be linked by a reasonably foreseeable method to other information that identifies the data subject;
FAIS	means the Financial Advisory and Intermediaries Act, 2002
FICA	means the Financial Intelligence Centre Act, 2001.
Information Officer	of, or in relation to, a— (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;
Legitimate Purpose	in respect of personal information processed by the Company as an operator, means the legitimate purpose as defined by the applicable responsible party who authorises the Company to process personal information as an operator; In respect of personal information processed by the Company as a Responsible party as an employer, means for all purposes relating to an individual's employment with the Company, including the employment contract, terms and conditions of employment, termination of the employment contract and including the processing of personal information for audit, storage and back up purposes; In respect of personal information processed by the Company in terms of its FICA obligations, the legitimate purpose of processing personal information is in order to identify and verify clients and including the processing of personal information for audit, storage and back up purposes.
Operator	means a personal who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party
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, colour, 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 employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular 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 person 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— *(a)* the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; *(b)* dissemination by means of transmission, distribution or making available in any other form; or *(c)* merging, linking, as well as blocking, degradation, erasure or destruction of information.
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.

4. Policy

The Company uses its own IT systems and maintains these systems according to its IT Governance Policy.

The Company ensures that all data and personal information is stored and accessed on IT systems which guarantee confidentiality, integrity, availability of functioning of the system and authenticity of system information.

Based on these IT governance principles, The Company sets its data and protection of personal information policy, which is applied to all personal information which is entered onto a record and filed, and all other data which is stored and kept by the Company.

4.1. Data

The Company stores data and data assets, through its own IT systems. Data is a valuable asset of the Company, and must be protected and kept secure.

All data is in electronic format. Data includes Company data and all client data across all lines of business, including email addresses, fax and telephone numbers. Data also includes information assets, which includes documents, files and information saved on file servers, databases and application systems. The medium that data resides on (including paper, hard-disks, removable disks, network based storage technologies and storage area networks) also form part of this policy and require application of the same principles.

Data is generated by the Company, but in respect of client data, data is exchanged between outsourcing parties and binder holders of the client. A number of different parties therefore have access to this data, and the Company can only implement control measures in respect of data received, data in its possession and under its control.

The Company is satisfied that its clients contract only with outsourcing parties which comply with sound IT governance principles and accordingly is satisfied that all data received from other parties is of a good quality.

It is the Company's policy to ensure that data is handled in a secure manner, so as not to compromise the integrity or confidentiality of the data. The Company ensures that data is accurate and of a good quality according to the principles set out in the Company's IT Governance Policy.

4.2. Personal Information

As operator, the Company may process personal information of policyholders (or prospective policyholders), the purpose of which is solely related to insurance policies, and in accordance with the legitimate purpose which is established by the Company's clients (the respective Responsible Parties).

It is the Company's policy not to receive personal information from any third party. Where this occurs, the Information Officer shall be notified so that the information can be de-identified. However, should it become necessary, or unavoidable that personal information be received and processed by the Company, the principles in this policy shall be applied accordingly.

As a responsible party, the Company processes personal information of employees (or prospective employees), the purpose of which relates solely to employment contracts and terms and conditions and employment at the Company. In addition, the Company may process personal information in as a responsible party for FICA purposes, where such processing is in line with the legitimate purpose.

Personal information may need to be further processed from time to time. Where this is required, other than for the legitimate purposes for which the information was initially obtained, the data subject shall be notified of such and their further consent obtained. The Company does not use personal information for marketing, comparative or public purposes. No decision regarding a data subject shall be taken solely on automated processing of personal information.

The Company shall secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures, as defined in the Company's IT Governance Policy.

The Company ensures the following:

- Processing must be lawful and done in a reasonable manner which does not infringe the privacy of the data subject;
- Consent must be obtained before any personal information of a data subject is collected, processed (or further processed) or recorded (this is specified in contracts where the Company deals with other Responsible parties);
- Personal information may only be processed and further processed for the legitimate purpose for which it was obtained;
- Where applicable, the Company must communicate the specific and explicitly defined purpose for processing the personal information, otherwise this duty rests on the responsible party;
- The responsible party must ensure that certain disclosures are made to the data subject, including but not limited to:

    - A right of access to the information;
    - A right to rectify the personal information;
    - A right to request that the information no longer be processed;
    - Details of the responsible party and any operators;
    - Which personal information is required;
    - Which laws require the collection of such information;
    - The location and existence of an incident management process.

- Personal information must be protected by the Company which requires a proper and functioning IT security system in accordance with the Company's IT Governance Policy;
- Personal information must be collected only from the data subject him/herself personally and from no other source, however, once collected from the data subject it may be transferred between operators acting for the same responsible party, as long as this does not amount to trans-border flow, which must then comply with paragraph 3.3 below. This is ensured by the responsible party;

- Where the Company transfers personal information to a third party for whichever purpose, the consent of the data subject must first be obtained, this includes where personal information is transferred for storage and back up purposes.

The Company shall take reasonably practical steps to ensure personal information processed is:

- complete, accurate & not misleading;
- updated where necessary;
- verified to ensure accuracy.

Where the Company may act as operator, it shall only transfer and exchange personal information and (and in all other instances) data with the responsible party and with other operators of the responsible party, as authorised per service level agreement.

4.3 Trans-border Information flows

The Company shall not transfer any personal information of a data subject to a third party which is situated in a foreign country, unless:

- the recipient of the information is subject to a law or binding corporate rules or binding agreement which upholds the principles for reasonable processing of the information, as according to the Act and this policy, and includes provisions which protects the further transfer of such information from the recipient to another third party in a foreign country; or
- the data subject further consents to the transfer of information, which is relevant to the insurance contract; or
- the transfer is necessary for the performance of a contract between the data subject and the responsible party or for implementation of pre contractual measures in response to the data subjects request; or
- the transfer is necessary for the performance of a contract in the interest of the data subject between a third party and the responsible party, the transfer is for the benefit of the data subject and it is not reasonably practical to obtain the consent of the data subject, who would likely consent if it were reasonably practical to obtain his consent.

5. Retention of Records

Personal information and data shall be recorded and kept for only so long as is necessary to achieve the legitimate purpose. Should the need for the records become unnecessary, the records shall be kept for a further period of five years, in order to comply with the Company's obligations in terms of FAIS, and a further two years, (in respect of accounting records and annual financial statements) in order to comply with the requirements of the Companies Act, 2008 and thereafter destroyed or de-identified according to the Company's IT Governance Policy. Where the records relate to personal information where the Company acts as a responsible party in terms of employee information, the records are not subject to FAIS, and therefore shall only be kept for a period of three years after termination of the employment contract, which allows an employee sufficient time to request copies of such records. After this period, records shall be de-identified and destroyed according to the Company's IT Governance Policy. In terms of personal information processed by the Company as a responsible party in terms of the Company's FICA obligations, records shall be kept for a period of five years after the legitimate purpose becomes irrelevant, in terms of FICA record keeping obligations.

The Company shall ensure that all records of personal information, which is not retained for historical, statistical or research purposes, is either deleted or de-identified, after the required period for retention has lapsed. Where personal information is retained for historical, statistical or research purposes, additional safeguards shall be implemented in respect of confidentiality and security of information.

Records are kept according to the time frames specified in the Company's Document Retention Policy.

6. Back ups

The Company shall back up all electronic data and personal information according to its IT Governance Policy.

7. Safety and Security, privacy and confidentiality of data and personal information

The Company ensures that the integrity of the personal information is secure by having appropriate and reasonable technical and organisational measures to prevent:

i. Loss, damage or unauthorised destruction of personal information;
ii. unlawful access to or processing of information by:

- Identifying all reasonably foreseeable internal and external risks to personal information and data under its control;
- Establish and maintain appropriate safeguards against the risks identified;
- Regularly verify that the safeguards are effectively implemented;
- Ensure that the safeguards are continuously updated in response to new risks or deficiencies in previously implemented safeguards;
- Physical records shall only be accessible by authorised personnel and will be kept in a secure location.

8. Access to Information

As operator, the Company does not deal with data subjects directly. Should a data subject request access to information, the Company shall refer the data subject to the relevant person of the responsible party, who is authorised to make the relevant disclosures to the data subject.

As a responsible party, the Company shall make all personal information available to data subjects, according to the procedure and format set out in its Promotion of Access to Information Manual.

9. Incident Management Strategy

The Company shall adopt an incident management strategy to deal with any security breaches, which sets out the following:

- Notification procedures where personal information of a data subject has been compromised;
- Manner of notification;
- Details of breach;
- Actual information which has been compromised;
- Identity of person responsible for the breach;
- What remedies are available to the data subject whose information has been breached.

10. Responsibility

The Company shall appoint an Information officer (A Wethmar). The Information security officer shall:

- Encourage compliance with information protection principles in terms of the Act and this Policy;
- Be accountable for information quality;
- Liaise with the information security officer of the responsible party where required;
- Monitor information security standards within each area of the business.

11. Procedural Documents and related Policies

- Responsible Practice Policy: IT, Data and POPI
- Disaster Recovery Policy

- Claims Filing Policy
- Record Management Procedure Promotion of Access to Information Manual
-

12. Contact Details

Sigma has appointed the following Information officer and Deputy Information Officer, who are responsible for overseeing the Company's POPI strategy and general adherence to this Policy:

- Information Officer:
  Mr. Andrew Wethmar
  Contact: Andrew.wethmar@sigmarisk.co.za

- Deputy Information Officers:

  - Mr. Jadyrien Subrayen
    jadyrien.subrayen@sigmarisk.co.za

  - Mr. Morné Steenkamp
    morne.steenkamp@sigmarisk.co.za