PROFILE RISK MANAGERS CC

POPI ACT COMPLIANCE POLICY

Table of Contents

1. GOVERNING PRINCIPLES

PROFILE RISK MANAGERS CC (PRM) is committed to the prescriptive provisions of the POPI Act. This commitment includes a guarantee of protecting the personal information of its customers. individuals protected by this policy includes insureds, former insureds, applicants, claimants and other individuals involved in a claim. The manner of this protection is set out in more detail hereunder.

The business is further regulated by the Financial Sector Conduct Authority and subscribe to the principles ensconced in the FAIS Act and the General Code of Conduct. Section 3 of the Code prescribes the confidentiality and integrity measures relating to client and insurer information. The Long- and Short-term Insurance Acts, through binding Policyholder Protection Rules, prescribe information security and information dissemination measures. The business is fully compliant with these prescriptive requirements and exact strict adherence thereto.

The Information Officer [IO] of the business is Coral-Anne Oosthuizen and must ensure this policy is executed by the business as well as monitor continued compliance with the POPI Act. Appointment as IO is made in terms of an appointment letter, clearly setting out the duties and responsibilities of the person.

This Policy is further supplemented by the following policies:

- The FAIS Policy Manual [specifically the Code of Conduct];
- The Treating Customers Fairly Policy; and
- The IT Governance Policy.

2. SCOPE

This Policy must be adhered to by all employees, directors, officers, and other staff of the brokerage and all third parties who Process the Personal Information of PRM's data subjects on behalf of the organisation as part of any functions or duties which they carry out (whether contractual or otherwise) for PRM as authorised third parties.

This Policy is applicable to the processing of all Personal Information throughout the information life cycle, from the point of first collection of Personal Information until the time that such information is destroyed.

3. POPI ACT LEGAL FRAMEWORK

A. DEFINITIONS

CONCEPT	EXPLANATION
Personal information	Any data processed by private and public bodies. Refer Section B for types of personal information.
Responsible party	Person domiciled in SA that processes personal information (can be alone or in conjunction with another person).
Data subject	Personal information of a juristic person (such as divulged in a tender) or of an identifiable living individual (personal details such as identity numbers, telephone numbers, etc.)
Processing	Automated or non-automated processing is included. Included in definition is collection, recording, organising, updating, storing, modification, retrieving, consulting, use, dissemination, transmission, distribution, making available, merging, linking, blocking, erasing or destructing.
Information that may be processed	Refer Sections C and D.

De-identify	Deleting information that identifies a data subject, can be manipulated to identify a data subject, can be used to link other data of a data subject.
Re-identify	Resurrecting information that has been de-identified that can identify a subject or can be used to identify a data subject or link data of a data subject.
Unique identifier	The manner of identifying a specific data subject – by the assignment of a unique identifier to that subject.
Public record	Any record that is in the public domain and under control of a public body, such as CIPC records of company directors.
Record	Any recorded information in the following format: • Writing on any material • Recorded or stored on tape-recorded, computer, etc. • Labels or markings that accompanies anything • Books, plans, maps, graphs and drawings • Photographs, film, negatives or tapes that can be reproduced
Restriction	Any personal information that is retained in a filing system and that is withheld from circulation but not destroyed or deleted (such as details of former employees).
Special personal information (S 26)	Information that may not be processed that includes: • details of a person's religious & philosophical beliefs, • race & ethnicity, • trade union membership or political affiliation, • health, sex life, biometric information, • criminal behaviour.
Information officer	Internal person responsible for data management as per Section 1 of PAIA (CEO or delegated person).
Special personal information that may be processed (S 27)	Special information may be processed: • with consent of the subject, • where it is necessary in law, • required in terms of international public law, • relevant for statistical or research reasons (conditions), • information was made available by the subject.
Information regulator	Person responsible for ensuring that the Act is executed. Currently not appointed. Refer Section 39 for detail.
Promotion of Access to Information Act (PAIA)	The instrument through which access to information is gained or requested. Businesses are required to develop a PAIA information manual by 31 December 2015.
Legislation requiring collation and processing of personal information	FAIS, FICA, Basic Conditions of Employment Act, Unemployment Insurance Act, Income Tax Act, Consumer Protection Act, National Credit Act, Electronic Communications & Transactions Act, Companies & Intellectual Property Commission, Short-term Insurance Act, Long-term Insurance Act, Pension Funds Act, Medical Schemes Act, etc.

B. PROTECTED INFORMATION

TYPE OF INFORMATION	DESCRIPTION
Private details	Race, gender, sex, pregnancy, marital status, nationality, ethnicity, social origin, colour, sexual orientation, physical health, mental health, disability, religion, conscience, belief, culture, language, birth
History of a person	Employment, medical, financial, criminal

Numbers and addresses	E-mail address, telephone number, address, telephone number, any other identifying number
Biometric information	Blood type, fingerprints or other such identifying information
Outlook	Views, opinions or preferences
Correspondence	Explicitly private or confidential correspondence or further correspondence that reveal origin of original correspondence
Views	Views and opinions of a person about another person
Names	The names and surname of a person

C. EXCLUSIONS TO PROCESSING OF PERSONAL INFORMATION

TYPE OF INFORMATION	**EXAMPLE**
Personal or household activity	Social Networking
De-identified information	Information that cannot be re-identified.
Processing by the state	National security, defence or public safety. Criminal offences, prosecution or execution of sentences.
Processing for journalistic purposes	News reporting
Processing by cabinet	
Court exercising judicial functions	
Exemptions in terms of Section 34	

D. LAWFUL PROCESSING CONDITIONS (INFORMATION PROTECTION PRINCIPLES)

PROTECTION PRINCIPLE	**DESCRIPTION**
Accountability	Responsible party must comply with principles
Processing limitation	Process data in a lawful and reasonable manner
	Process the minimum of information (specific purpose, adequate, relevant, not excessive)
	Consent & justification (subject may object under certain circumstances, if an objection is received you may not process information any further)
	Direct collection from subject (Exceptions: public record, necessary for national security or enforcement of laws, not reasonably practicable, etc.)
Purpose specification	Specify the purpose that the information will be used for (lawful, specific, defined, related to a function of the responsible party)
	Data subject must be informed of the purpose
	Data may not be retained for longer than needed
Further processing	Must be in line with original purpose of collection
	Exception: statistical, historical or research purposes
Quality of information	Must take reasonable practicable steps to ensure that information is complete, up to date, accurate and not misleading
Openness	If processing of information is planned, the Regulator and data subject must be notified
Security safeguards	Take reasonable and appropriate technical and organisational measures to prevent loss or unauthorised use of information. Identify internal and external risks and establish safeguards. Employ technology such as access control or encryption.
	When processed by an operator: may only be done with knowledge of responsible party. A duty of confidentiality exists.

	Notification of security compromises: regulator and data subject must be informed if data was accessed or acquired by an unauthorised person
Data subject participation (rights of data subjects)	Data subject has the right to access the information through PAIA.
	Right to request whether or not information is held.
	Right to be informed to whom the data was disclosed.
	May request a description of the information.
	Right to request the correction or deletion of data that is inaccurate, irrelevant, out of date or obtained unlawfully.

4. COLLECTING, USING, AND DISCLOSING CUSTOMER (PERSONAL) INFORMATION

The business will collect, use, and disclose personal information in order to provide customers with the insurance protection that they requested or, in the case of a claimant, to provide such claimant with the compensation to which he or she is entitled to under his/her policy.

In order to achieve this goal, the business will use personal information for the purposes of:

- establishing and maintaining communications with the customer;
- obtaining information from the customer as to his/her/its needs and requirements;
- approach various insurers with the customer's information in order to obtain quotes;
- underwriting risks on a prudent basis;
- investigating and paying claims;
- detecting and preventing fraud;
- offering and providing products and services to meet customer needs;
- compiling statistics and reporting as required or authorised by legislation.

Although care is taken to provide a complete list of the functions that the business will perform in carrying out its mandate as contained in the contract with any client, the above list may not be exhaustive and it is accepted by the client that the authorisation to utilise personal information is extended to any ancillary activity reasonably proximate to advisory and intermediary services provided in the insurance context, as long as it is to the benefit of the client and within the parametres of the contract entered into between the client and the business.

Given the nature of the insurance industry in general, consent to use information so collated may not need to be repeated for implied use where the use and disclosure of personal information is necessary to supply clients with the services required or implied in terms of the insurance contract and any other agreement entered between the client and the company.

The company may also disclose personal information to businesses that provide goods and services to insurance companies and their customers, such as claims adjusters, appraisers, panel-beaters and other workshops. Such service providers will only be privy to the information necessary for executing the services required. Any disclosure of personal information to any of the aforementioned service providers will be made strictly on the basis that the recipient of the information will maintain the confidentiality of the information.

Any customer may withdraw consent subject to legal or contractual obligations and on reasonable notice. Withdrawal of consent may limit the company's ability to provide a client with the requested product or service. If a customer wants to withdraw his/her consent, the Information Officer must first be contacted in order to be advised of the implications of such withdrawal.

5. PROTECTING CLIENT PRIVACY

The privacy and confidentiality of information that any customer or prospective customer share with the company is fundamental to operating the business. It is company policy to safeguard all personal information with appropriate security measures. Personal information is kept in strict confidence. The company maintains physical, electronic and procedural safeguards to protect information from unauthorised access.

The company performed a complete Information Risk Assessment to ensure its internal and external risks are addressed. The business regularly reviews its policies and practices, monitors computer networks, test the strength of information security measures as well as monitor compliance with applicable legislation.

The company will restrict access to personal information to those employees identified to access the client's information to provide the contracted products and services to the client. Employees are bound by a Confidentiality Policy and various Confidentiality Undertakings.

Apart from cases of disclosure as set out in Section 3 above, the company will not make any personal information available without obtaining the express prior written consent of the client.

Personal information is retained only as long as it is needed. It may also be retained to meet any legal, regulatory or tax requirement. **Annexure A to the IT Governance Policy** contains a list of the legal prescripts in various applicable legislation as to retention of information periods.

6. PROCESSING OF PERSONAL INFORMATION BY THIRD PARTIES

Personal Information will only be provided to authorised third parties where consent is obtained from data subjects or in furtherance of a business need or in compliance with a legal obligation. The extent of the consent required will be determined in consultation with the Information Officer.

Where necessary or appropriate, agreements with authorised third parties to whom the company may disclose personal information must be concluded to ensure that they process any personal pnformation in accordance with the provisions of this Policy and the relevant laws.

Authorised third parties must immediately inform the business of any actual or suspected security breach or compromise to personal information in its possession. The authorised third parties may be required to notify the affected data subject(s) and the Information Regulator.

7. ACCESSING PERSONAL INFORMATION

Any requests for amendment of information or for details of personal information held by the company must be made to the Information Officer at (e-mail address).

Any consumer has the right to submit a written request to access personal information that is in possession of the business and make corrections to it. The company will amend personal information that is verified to be inaccurate or incomplete. The company will respond to any such request within 30 days or advise the requester if additional time is required to respond to the request.

Personal information not readily available to a consumer/client may be requested through the Promotion of Access to Information Act process. Requesters should consult the business' PAIA Manual, available on the website www.profilerisk.co.za // available by request in writing from the Information Officer.

There may be situations in which the company is legally prohibited from allowing consumers access to personal information.

8. CROSS BORDER DATA TRANSFERS

The company can send or transfer Personal Information of Data Subjects to authorised third parties beyond the borders of the countries in which personal information is collected in order to achieve the purpose for which the personal information was collected and Processed, including for processing and storage by authorised third parties, if the applicable data subject(s) has consented to such cross-border transfer.

Where no consent has been obtained, the cross-border transfer must meet one of the following conditions:

- The recipient must be subject to existing legislation in his /her/its country or to binding corporate rules or to a binding agreement that enforces and upholds Personal Information protection measures which are acceptable to the business;
- The transfer must be necessary for the conclusion and/or performance of a contract between the business and the Data Subject;
- The transfer must be necessary for the conclusion or performance of a contract entered, in the interest of the Data Subject, between the company and the relevant group company or the authorised third party; and
- The transfer must be to the benefit of the data subject and must take place in circumstances under which it is not reasonably possible to obtain the data subject's consent and where it is reasonably possible to obtain such consent; the data subject would be likely to give it.

The processing of Personal Information in a foreign jurisdiction may be subject to the laws of the country in which it is held, and may be subject to disclosure to the Governments, Courts of law, Enforcement or Regulatory Agencies of such other country, pursuant to the laws of such country.

9. INVESTIGATING AND REPORTING DATA BREACHES

The business has taken reasonable steps to protect the integrity of personal information of clients and other persons, as prescribed in the Act. Despite taking these measures there is no guarantee information of a client or the integrity of the IT infrastructure of the company cannot be compromised. In the instance a data breach takes place or the personal information of a data subject falls into the hands of an unauthorised third party, the company must take immediate remedial action.

Remedial action includes the following steps:

- Any employee becoming aware there was a data breach or personal information divulged to an unauthorised third party, must immediately report the event to the Information Officer or, where appointed, the Deputy Information Officer.
- The IO (or DIO) must investigate the event or manage/oversee the investigation of the event.
- The data subject(s) whose information was compromised, must be informed as prescribed in Section 22 of the Act.
- Where an insurer's information was compromised, the insurer must be informed of the breach within 2 days of the IO (or DIO) becoming aware of the event.
- The breach must be contained and remedial action, appropriate to the circumstances, must be taken in order to either retrieve the information, destroy it or retrieve it.
- A root cause analysis must be performed to take appropriate remedial steps to ensure the event doesn't recur.

- Remedial steps, including assigning responsibility and, where applicable, disciplinary or appropriate action (against internal and/or external parties) must be taken.
- Where it is indicated the IO (or DIO) must report the matter to the Information Regulator (IR). This report must be submitted to the IR within a reasonable time after the event came to the attention of the business, but not longer than 2 weeks after becoming so aware thereof.

10. RESPONSIBILITY

The members are responsible for developing this Policy. Senior management is responsible for ensuring that this Policy is accepted and implemented throughout the organisation.

11. REVIEW

This Policy will be reviewed on an annual basis or when appropriate (changes in law).