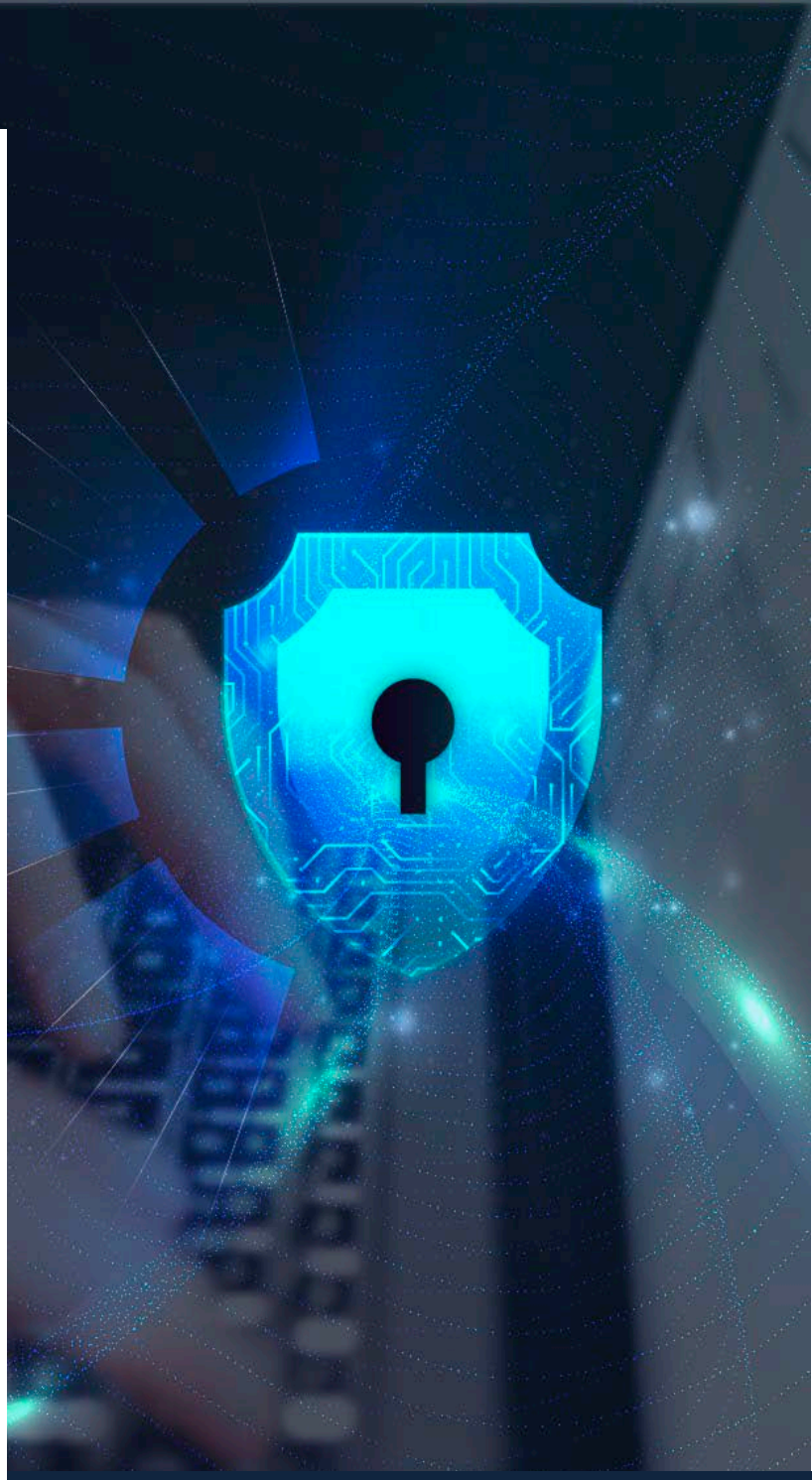
POPIA Data Plan



Protocol Risk Managers (Pty) Ltd

Protocol Risk Managers is a registered financial services provider - FSP 49614

All material © Protocol Risk Managers (Pty) Ltd

Table of Contents

Protocol Risk Managers is a registered financial services provider - FSP 49614

POPIA Data Plan

What does Personal Information mean?

Personal Information is defined as: information relating to an identifiable, living natural/juristic person, including, but not limited to—

- 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;
- information relating to the education or the 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 of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- 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.

What does Special Personal Information mean?

In certain instances, consent to process Special Personal Information may be required from you either by Protocol Risk Managers or by an authorised third party. Special Personal Information can be highly sensitive in nature and therefore a higher degree of protection is given to such information under POPIA. Special Personal Information is a person's Personal Information that concerns their religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health, sex life, biometric information or criminal behaviour. Such information, if needed, will be requested of you at the time it is necessary for the policy to perform. If you withhold such information, performance of the policy may be delayed or may not be possible.

Why we collect your Personal Information?

As an Underwriting Manager, we may collect your Personal Information for the following reasons, some of which are mandatory:

- process policy applications;
- administering your policy;
- underwriting purposes;
- to meet our obligations under an agreement with you
- to provide you with access to our products and services, including but not limited to analysis, advice or intermediary services in relation to your policy;
- monitor and analyse your conduct relating to the policy for fraud, compliance and other risk-related purposes;
- develop new products and services;
- to help us improve our offerings to you;
- to confirm and verify your identity or to verify that you are an authorised user for security purposes;
- for the detection and prevention of fraud, crime, money laundering or other malpractice;
- to conduct market or customer satisfaction research or for statistical analysis;
- for audit and record keeping purposes;
- in connection with legal proceedings;
- to comply with legal and regulatory requirements or industry codes to which we subscribe or which apply to us, or when it is otherwise allowed by law.

The information we collect will depend on the purpose for which it is processed. We will only collect information that Protocol Risk Managers requires for the purposes it deems to be in your interest. In some instances, we will inform you of what information you are required to provide us and what information is optional.

Information will primarily be collected directly from you; however, we may also collect and/or verify information about you, potentially electronically, from other sources, with or without your knowledge. We may collect such information about you from contracted parties or publicly available sources such as electoral rolls, court judgements, bankruptcy or repossessions, credit rating agencies and verification agencies.

Website usage information is collected using "cookies" which allows us to collect standard internet visitor usage information.

Do we disclose your Personal Information?

Your Personal Information will be kept confidential, however, under certain circumstances, to ensure the purpose of collection is met, we may lawfully disclose it to the following third parties:

- Service providers;
- Subcontractors;
- Agents;
- Reinsurers;
- Insurance associations or other insurers;
- Statutory authorities;
- Protocol Risk Managers- personnel;
- Court of Law;
- Governmental bodies;
- The regulator.

We may also disclose your Personal Information, where we are required to disclose in terms of law or industry codes or where we believe it is necessary to protect our rights. The third parties above may sometimes be located outside the Republic of South Africa.

We have agreements and security measures in place to ensure that all third parties to whom your Personal Information is disclosed comply with the terms and provisions of the POPIA. We ensure that third parties fully understand the duties and obligations they become encumbered with in retaining the privacy and integrity of your Personal Information.

How we protect your Personal Information?

In terms of the law, we are obliged to implement measures and strategies to ensure protection of your Personal Information, whereby, unauthorised access and use is deterred. Our security policies and procedures, which are reviewed on an ongoing basis include the following:

- Physical security;
- Computer and network security;
- Access to Personal Information;
- Secure communications;
- Security in contracting out activities or functions;

- Retention and disposal of information;
- Acceptable usage of Personal Information;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

How to access your Personal Information?

You may contact Protocol Risk Managers or your Broker to enquire what Personal Information we hold for you. We will make the information available to you once we are reasonably satisfied that you have confirmed your identity to us.

How to correct your Personal Information?

You may update, correct, amend or delete your Personal Information at any time. We will take reasonable steps to confirm your identity before making changes to Personal Information.

POPIA DATA BREACH POLICY AND RESPONSE PLAN

Introduction

Under the Protection of Personal Information Act (POPIA) certain personal data breaches must be notified to the Information Regulator (IR) and affected data subjects need to be told too.

The purpose of this policy is to outline the internal breach reporting procedure of Protocol Risk Managers. (hereafter "FSP") and our internal and external response plan and it should be read in conjunction with our data protection policy.

What constitutes a personal data breach?

A personal data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

A breach is therefore a type of security incident and there are three different types of breach that may occur:

1. **Confidentiality breach** – an accidental or unauthorised disclosure of, or access to, personal data.
2. **Availability breach** – an accidental or unauthorised loss of access to, or destruction of, personal data.
3. **Integrity breach** – an accidental or unauthorised alteration of personal data.

A breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

A personal data breach would, for example, include:

- Personal data being disclosed to an unauthorised person, e.g. an email containing personal data being sent to the wrong person.
- An unauthorised person accessing personal data, e.g. an employee's personnel file being inappropriately accessed by another member of staff due to a lack of appropriate internal controls.

- a temporary or permanent loss of access to personal data, e.g. where a client's or customer's personal data is unavailable for a certain period of time due to a system shut down, power, hardware or software failure, infection
- by ransomware or viruses or denial of service attack, where personal data has been deleted either accidentally due to human error or by an unauthorised person or where the decryption key for securely encrypted data has been lost.

Notification to the Information Regulator

Not all personal data breaches have to be notified to the Information Regulator. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Company on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example,
it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the Information Regulator without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. (Amend as appropriate) If our report is submitted late, it must also set out the reasons for our delay. The notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- the name and contact details of the Company's CEO
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

Protocol Risk Managers is a registered financial services provider - FSP 49614

Awareness of the breach occurs when one has a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach.

Communication to affected data subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Company also needs to communicate the breach to the affected data subjects without undue delay, i.e. as soon as possible. In clear and plain language, we must provide them with:

- a description of the nature of the breach
- the name and contact details of the Company's CEO
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

We will also endeavour to provide data subjects with practical advice on how they can themselves limit the damage,
e.g. cancelling their credit cards or resetting their passwords.
We will contact data subjects individually, by e-mail, unless that would involve the Company in disproportionate effort, such as where their contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website. www.protocoluma.co.za

However, we do not need to report the breach to data subjects if:

- we have implemented appropriate technical and organisational protection measures, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- we have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.

Assessing "risk" and "high risk"

In assessing whether a personal data breach results in a risk or high risk to the rights and freedoms of data subjects,
the Company will take into account the following criteria:

- the type of breach

Protocol Risk Managers is a registered financial services provider - FSP 49614

- the nature, sensitivity and volume of personal data affected
- ease of identification of data subjects – properly encrypted data is unlikely to result in a risk if the decryption key was not compromised in the breach
- the severity of the consequences for data subjects
- any special characteristics of the data subject
- the number of affected data subjects
- special characteristics of the Company.

Data breach register

The Company will maintain a register of all personal data breaches, regardless of whether or not they are notifiable to the Information Regulator. The register will include a record of:

- the facts relating to the breach, including the cause of the breach, what happened and what personal data were affected
- the effects of the breach
- the remedial action we have taken.

Data breach reporting procedure

If you know or suspect that a personal data breach has occurred, you must immediately both advise your line manager and contact the Company's Managing Director. You must ensure you retain any evidence you have in relation to the breach and you must provide a written statement setting out any relevant information relating to the actual or

- suspected personal data breach, including:
- your name, department and contact details
- the date of the actual or suspected breach
- the date of your discovery of the actual or suspected breach
- the date of your statement
- a summary of the facts relating to the actual or suspected breach, including the types and amount of personal data involved
- what you believe to be the cause of the actual or suspected breach
- whether the actual or suspected breach is ongoing
- who you believe may be affected by the actual or suspected breach.

Protocol Risk Managers is a registered financial services provider - FSP 49614

You must then follow the further advice of the Managing Director. You must never attempt to investigate the actual or suspected breach yourself and you must not attempt to notify affected data subjects. The Company will investigate and assess the actual or suspected personal data breach in accordance with the response plan set out below and the data breach team will determine who should be notified and how.

Response plan

The Company's Managing Director will assemble a team to investigate, manage and respond to the personal data breach. They will lead this team and the other members will consist of nominated senior members of the management team.

- The data breach team will then:
- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the Company's data breach register.
- Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected data subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Protocol Risk Managers is a registered financial services provider - FSP 49614

Response plan template

Data breach team

Data breach team lead: Jan Labuschagne Managing Director
Other members of data breach team: Brett Gunter Claims Manager, Monique Bester HR, Accounts and Payroll

Background

- Name and department of person notifying actual or suspected breach:
- Date of actual or suspected breach:
- Date of discovery of actual or suspected breach:
- Date of internal notification of actual or suspected breach.

Preliminary assessment

- Summary of the facts relating to the actual or suspected breach, including the types of personal data involved:
- Categories and approximate number of affected data subjects:
- Categories and approximate number of affected records:
- How sensitive is the personal data?
- Cause of the actual or suspected breach:
- Any other relevant information or comments.

Containment and recovery

- Is the actual or suspected breach ongoing?
- What steps can be taken to contain the breach, i.e. to stop or minimise further loss, destruction or unauthorised disclosure?
- What steps can be taken to recover any lost personal data?
- Does the breach need to be reported to the police, for example if there is evidence of theft?
- Does any professional regulator or trade body need to be notified of the

Protocol Risk Managers is a registered financial services provider - FSP 49614

breach?

- Does the breach need to be reported to any relevant insurers, e.g. professional indemnity?

Detailed assessment

- What types of personal data are involved, and does the breach involve any special categories of personal data or personal data relating to criminal convictions and offences?
- Who is affected by the breach?
- What are the likely consequences of the breach for affected data subjects?
- Where personal data has been lost or stolen, are any protections in place such as encryption?
- What has happened to the personal data?
- What uses could a third party make of the personal data?
- Are there any other personal data breaches?
- Has the breach been recorded in the data breach register?
- Any other relevant information or comments:

Notifying the INFORMATION REGULATOR

- What is the type of breach?
- What is the nature of the personal data affected?
- What is the potential harm to data subjects?
- What is the sensitivity of the personal data affected?
- What is the volume of personal data affected?
- How easy is it to identify data subjects from the personal data?
- What is the number of affected data subjects?
- Any other relevant information or comments:
- Taking the above into account, is there a legal obligation to notify the Information Regulator?

Notifying affected data subjects

- Is there a legal or contractual obligation to notify affected data subjects?
- If there is no legal or contractual obligation, should affected data subjects be

Protocol Risk Managers is a registered financial services provider - FSP 49614

notified anyway? Consider whether it will help them to know or whether there is a danger of over-notifying.

- What is the best way to notify affected data subjects?
- Do any data subjects, or categories of data subjects, need to be treated with care because of their special characteristics?
- What additional information should be provided to data subjects about what they can do to limit the damage?
- How should affected data subjects contact the Company for further information or advice and how will we manage such responses?
- How will we keep a record of who has been notified?
- Any other relevant information or comments:
- Is there any legal or contractual requirement to notify any other parties?

Response

- What security measures were in place when the breach occurred?
- What further measures have been, or are to be, put in place to address the breach and mitigate its possible adverse effects?
- Please also outline the timetable for any measures that have not yet been taken.
- What further technical or organisational measures are to be put in place to prevent the breach happening again?
- Does further staff training on data protection awareness need to be conducted?
- Is it necessary to conduct a privacy risk assessment?
- Any other comments:

Approval of response plan Name: Jan Labuschagne Job title: Managing Director Date: 14 June 2022

Signature:

Protocol Risk Managers is a registered financial services provider - FSP 49614