POPI Manual

STREET SMART FINANCIAL SERVICES (PTY) LTD

Herein referred to as the FSP

1. Background to data protection compliance

POPI refers to South Africa's **Protection of Personal Information Act 4 of 2013,** which seeks to regulate the Processing of Personal Information.

2. Aim of the Act

The Protection of Personal Information act will significantly impact on the way in which businesses including Financial Services Providers (FSP'S) collect, store, process and disseminate information from and to clients and employees. The legislation promotes the protection of personal information processed by public and private bodies and aims to introduce certain information on protection principles to establish minimum requirements for the processing of personal information.

The view 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

3. Personal information

Personal information broadly means any information relating to an identifiable, living natural person or juristic person (Companies, Close Corporations or Trusts) and includes, but is not limited to:

- **Contact details:** email addresses, telephone numbers, physical and business addresses
- **Demographic information:** age, sex, race, birth date, ethnicity etc.
- **History:** employment, financial, educational, criminal, medical history
- **Opinions** of and about the person
- **Records of Advice:** financial advice relating to a specific client
- **Banking details of clients**
- **Any form of Private or Confidential correspondence**

4. Processing

Processing means anything done with the personal information, including collection, usage, storage, dissemination, modification or destruction (whether such processing is automated or not)

5. Obligations and Responsibilities of the FSP

The obligations and responsibilities of the FSP are as follows:-

- to collect information that is needed for the specific purpose of rendering financial intermediary services and advice
- to apply reasonable security measures to protect personal information obtained
- to ensure all information obtained is relevant and up to date
- to hold as much as you need, and only for as long as you need it
- to allow the subject of the information to see it upon request

6. Data protection compliance in terms of the Act

POPI promotes transparency with regard to what information is collected and how it is to be processed. This openness is likely to increase the **client's confidence** in the FSP.

7. Application of the POPI Act

Accountability for compliance lies with a **Responsible Party**, meaning 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.

Generally the **Responsible Person** must be a resident in South Africa or the processing should occur within South Africa. (subject to certain exclusions as per Section 3 Act 4 of 2013).

There are cases where POPI does not apply.

8. Exclusions

(Section 4 of Act 4 of 2013)

- Purely household or personal activity
- Sufficiently de-identified information
- Some state functions including criminal prosecutions, national security etc.
- Journalism under a code of ethics
- Judiciary functions etc…

9. Database protection measures

The following measures will be taken by the FSP to improve the overall **reliability of its databases**.

Database protection measures adopted by the FSP:

- Capturing only minimum required data provided
- Ensuring accuracy of all information within the FSP
- Removing data that is no longer required by the FSP

Compliance demands identifying Personal Information and taking reasonable measures to protect the data integrity of our client/s. This will likely **reduce the risk of data breaches** and the associated public relations and legal consequences for the FSP.

10. Consequences of non-compliance

Non-compliance with the POPI Act could expose the **Responsible Party** of the FSP to a **penalty** of a **fine and/or imprisonment of up to 12 months.** In certain cases the penalty for non-compliance could be a **fine and/or imprisonment of up to 10 years.** (as per Section 99 of Act 4 of 2013)

11. Contents of the Act

The Act is sectioned into 12 Chapters as defined as follows:-

Chapter 1	Definitions and Purpose
Chapter 2	Application, Provisions and Exclusions • The wide ambit of the Act necessitates certain exclusions as far as its application is concerned
Chapter 3	Conditions for lawful processing of personal information • This chapter contains 8 (eight) information protection principles: ▪ Accountability ▪ Processing limitation ▪ Purpose specification ▪ Further processing limitation ▪ Information quality ▪ Openness ▪ Security safeguards ▪ Data subject participation
Chapter 4	Exemption from information protection principles
Chapter 5	Supervision • This chapter deals with the Information Protection Regulator and Information Protection Officers
Chapter 6	Notification and Prior Investigation
Chapter 7	Codes of Conduct
Chapter 8	Rights of data subjects regards unsolicited electronic communications and automated decision making
Chapter 9	Trans-border information flows
Chapter 10	Enforcement
Chapter 11	Offences and Penalties
Chapter 12	General Provisions

12. Data compliance: Internal controls checklist

The following internal controls have been implemented and adopted by the FSP in order to support the FSP to accomplish specific goals or objectives.

The **4 (four) key components** considered by the FSP when evaluating internal controls for data security are:

- **Ownership**
- **Risk Alignment**

- **Monitoring and Testing**
- **Control Limitations**

OWNERSHIP

One of the central components of control strength is ensuring there is clear ownership. There must be a clear indication as to who within the FSP is responsible for the control.

The true owner of the control has the knowledge of:

- the true underlying risk
- the purpose and design of the control
- how the control is monitored and tested
- The ability to determine whether the control is effective.

RISK ALIGNMENT

The danger with many internal controls is that they are created to report a "perceived" risk without a real analysis of the inherent threat. Without a clear understanding of both the real threat and its potential impact, it is impossible to design the appropriate control.

Internal controls do not eliminate risk; they only bring it within acceptable tolerance levels. There is always a component of risk, despite the presence of a control.

Risk alignment measures taken by the FSP:

- Continuous risk assessment
- identification of the expected level of risk
- Ensuring that control is effective
- Creating potential risk scenarios to improve effectiveness

MONITORING AND TESTING

One of the most misunderstood areas in all of internal control management, and perhaps one of the most critical, is that of monitoring and testing.

Control *monitoring* involves understanding who is overseeing a control on a day-to-day basis to ensure its being used.

The key individuals are responsible for:

- spot-checks to be conducted (in compliance with clean desk policies)
- certain types of management reports that may identify control gaps
- monitoring risk areas of non-compliance constantly and informally

Control *testing* involves a deliberate process of testing. A given control to ensure its being utilized as intended and is typically done periodically.

CONTROL LIMITATIONS

Staff members need to access data to perform their job functions, the data is inherently exposed. The FSP needs to be aware of what risks are being mitigated through internal controls and what risks still exist.

Control limitations involves

- Discussions with staff members surrounding risk mitigating with key individual will be conducted on a regular basis.

The central theme that runs through this internal controls checklist is that internal controls need to be carefully understood, evaluated and monitored if they are going to truly accomplish what the FSP intend for them, and, taking a deliberate and thoughtful approach to strengthening and regularly reviewing the internal controls is critical to ensuring compliance with legal and regulatory guidelines.