

https://dspace.org/

Data Governance in the AI Era: Analysing the Effectiveness of Information Regulator in Implementing POPIA

Goitsione, Obopeng

2025
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/49195
Goitsione, Obopeng . (2025). Data Governance in the AI Era: Analysing the Effectiveness of Information Regulator in Implementing POPIA [Masters dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. v

Downloaded from a DSpace repository. https://dspace.org/

Data Governance in the AI Era: Analysing the Effectiveness of Information Regulator in Implementing POPIA

Student Name: Obopeng Goitsione

Supervisor: Ashraf Patel

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2025

ABSTRACT

With the Fourth Industrial Revolution (4IR) accelerating digital transformation, emerging technologies such as Artificial Intelligence (AI) pose complex challenges to data protection and regulation enforcement. This study assesses the effectiveness of South African Information Regulator (IR) in enforcing the Protection of Personal Information Act (POPIA) in the dynamic changing data economy driven by 4IR technologies.

Utilising a qualitative research approach through interviewing industry participants and the review of regulatory frameworks, supported by the review of existing literature, the study concludes that while South Africa's Protection of Personal Information Act (POPIA) represents a crucial step towards strengthening data protection, its enforcement faces significant challenges, including regulatory inefficiencies, inadequate penalties to deter non-compliance, and the rapid evolution of emerging technologies outpacing existing legal frameworks. The Information Regulator's limited capacity, coupled with insufficient public awareness about data privacy risks and challenges relating to IR accessibility at predominately rural area, further undermines effective oversight and compliance.

Key recommendations include enhancing regulatory enforcement through stricter penalties and clearer breach reporting obligations, strengthening the regulator's capacity with additional funding and resources, and working in collaboration with other sister regulators in developing AI-specific guidelines to address emerging risks. Moreover, increasing public education on data privacy and embedding data protection practices across sectors are essential for fostering a culture of compliance and safeguarding personal information in the digital era.

KEYWORDS

Information society, data economy, 4IR, artificial intelligence, generative AI, data governance, data management, regulations, data protection, data privacy, data security, evolution, POPIA, information regulator

DECLARATION

I, Obopeng Goitsione, declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Obopeng Goitsione Signature: 

Signed at: Centurion

On the 29th day of March 2025

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervisor, Mr. Ashraf Patel. Thank you for your guidance and encouragement throughout this journey. Your invaluable coaching and support helped me navigate every challenge along the way.

I am also deeply thankful to my family, especially my wife Kego Goitsione, for providing a strong support system that allowed me to focus on my studies. Your unwavering encouragement, willingness to offer resources, and readiness to shoulder some of my responsibilities made this achievement possible. Thank you so much my Skattebol.

To my two beautiful daughters, Laone and Tshwanelo, and my son, Kanelo; although you may not have fully understood my absence during this period, your innocent joy and presence provided me with immense strength and motivation throughout this journey.

To my father and mother, Rre Kobua and MaKobua, and all my siblings; thank you for your messages of encouragement during this journey. You remain my pillar of strength.

To all my extended family, friends and colleagues who continued to check up on me, giving me strength and messages of support; I am deeply grateful. Special thanks to Kabelo Goitseone for your unwavering support, words of encouragement and believing in me. You kept me going my brother, kealeboga, Kobua.

To all the participants who took the time to participate in the interviews. This study would not have been possible without your valuable contribution.

TABLE OF CONTENTS

LIST OF TABLES ..... **viii**

LIST OF FIGURES ..... **ix**

LIST OF ACRONYMS ..... **x**

1. CHAPTER 1: INTRODUCTION **1**

1.1 STATEMENT OF PURPOSE 1
1.2 BACKGROUND OF THE STUDY 1
1.3 RESEARCH PROBLEM 6
1.4 RESEARCH QUESTIONS 10
1.5 RESEARCH PROPOSITIONS 10
1.6 SIGNIFICANCE OF THE STUDY 10
1.7 DEFINITION OF TERMS 11
1.8 ASSUMPTIONS 13
1.9 DELIMITATIONS OF THE STUDY 13
1.10 CHAPTER OUTLINE 14

2. CHAPTER 2: LITERATURE REVIEW **16**

2.1 INTRODUCTION 16
2.2 INFORMATION SOCIETY THEORY 16
2.3 PUBLIC INTEREST THEORY OF REGULATION 20
2.4 DATA GOVERNANCE FRAMEWORK (ORGANISATIONAL) 24
2.5 PRIOR STUDIES – LITERATURE REVIEW 29
2.6 ANALYTICAL FRAMEWORK 34
2.6.1 CONCEPTUAL FRAMEWORK 35
2.7 CONCLUSION 37

3. CHAPTER 3: RESEARCH METHODOLOGY **38**

3.1 INTRODUCTION 38
3.1.1 ONTOLOGY AND EPISTEMOLOGY 38
3.2 RESEARCH APPROACH 39
3.3 RESEARCH DESIGN 40

3.4 Research Strategy 41
3.5 Data Collection Methods 42
3.6 Population and Sample 42
3.7 Data analysis and interpretation 43
3.8 Research Instrument 44
3.9 Validity and Reliability 45
3.9.1 Credibility 45
3.9.2 Transferability 45
3.9.3 Dependability 46
3.9.4 Confirmability 46
3.10 Limitations of the study 46
3.11 Ethical Considerations 47
3.12 Conclusion 47

4. CHAPTER 4: PRESENTATION OF DATA 48

4.1 Introduction 48
4.2 Demographics Data 48
4.3 Analysis Process 52
4.4 Presentation of findings 52
4.4.1 Theme 1: Handling of POPIA infringement cases 59
4.4.2 Theme 2: Effectiveness of POPIA Enforcement by the Information Regulator 61
4.4.3 Theme 3: POPIA provisions adequacy in evolving technologies 63
4.4.4 Theme 4: Emerging Risks from AI and Generative Technologies 64
4.4.5 Theme 5: Compliance Requirements and Challenges in Data Protection 66
4.4.6 Theme 6: Consumer Protection and Public Awareness in the Data Economy 68
4.4.7 Theme 7: Oversight and Compliance 72
4.4.8 Theme 8: Stakeholder engagement and collaboration 73

5. CHAPTER 5: DISCUSSION 76

5.1 Introduction 76
5.2 Discussion of findings related to Proposition 1 78
5.2.1 Enforcement Gaps and Delayed Processes 78
5.2.2 Insufficient Deterrence Through Penalties 79
5.2.3 Regulatory and Procedural Shortcomings 80
5.2.4 Exploitation of Legal Loopholes 80
5.2.5 Successes by the Information Regulator 81
5.3 Discussion of findings related to Proposition 2 82
5.3.1 Resource and Capacity Constraints 82
5.3.2 Communication Gaps 83
5.3.3 Lack of Adequate Guidance Notes 84
5.4 Discussion of findings related to Proposition 3 86
5.5 Discussion of findings related to Proposition 4 88

5.5.1 TELE-MARKETING CHALLENGES 89
5.5.2 ORGANISATIONAL VULNERABILITIES AND RISK MANAGEMENT 89
5.5.3 DATA BREACHES 90
5.6 CONCLUSION 90

6. CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS 91

6.1 INTRODUCTION 91
6.2 CONCLUSIONS PER RESEARCH QUESTIONS 91
6.2.1 CONCLUSIONS RELATING TO RESEARCH QUESTION 1 91
6.2.2 CONCLUSIONS RELATING TO RESEARCH QUESTION 2 92
6.2.3 CONCLUSIONS RELATING TO RESEARCH QUESTION 3 93
6.2.4 CONCLUSIONS RELATING TO RESEARCH QUESTION 4 94
6.3 RECOMMENDATIONS 95
6.4 SUGGESTIONS FOR FURTHER RESEARCH 98

References 99

Appendix A 114

Appendix B 121

LIST OF TABLES

Table 1. Selected Data Breach Incidents in South Africa. Source: Multiple Sources 8

Table 2. Key Terms/Concepts Definitions and Sources 11

Table 3 Breakdown of Participants Demographics..... 50

Table 4. Mapped Research Questions, Propositions, Themes, Codes and Verbatim ... 55

LIST OF FIGURES

Figure 1. Information Regulator of South Africa Organogram. Source: (Information Regulator, 2024) 4

Figure 2. AI Market Size in South Africa. Source: (Statista, 2024) 5

Figure 3. The Data Economy Conceptual Model. Source**:** (Sestino et al., 2023) 19

Figure 4. Expanded Data Lifecycle 25

Figure 5. The DAMA Wheel Framework. Source: (DAMA International, 2017) 26

Figure 6. The DAMA Wheel Framework Evolved. Source: (DAMA International, 2017) 27

Figure 7. Data Governance, data lifecycle management & AI relationship illustration.. 28

Figure 8. Awareness of the Regulator Survey. Source: (HSRC, 2023) 33

Figure 9. Research Conceptual Framework. Adapted from (Ndemo & Mkalama, 2023) 37

Figure 10. Word Cloud: Study Frequently used words. Source: Atlas.ti Data Analysis 53

Figure 11. Study Participants Contribution. Source: Atlas.ti Data Analysis 54

Figure 12. IR Infringement Case and Complain Step-by-Step High-level Process..... 79

LIST OF ACRONYMS

4IR	The Fourth Industrial Revolution
AI	Artificial Intelligence
AU	African Union
BCG	Boston Consulting Group
CDO	Chief Data Officer
DAMA	Data Management Association International
DBE	Department of Basic Education
DCAM	Data Management Capability Assessment Model
DCDT	Department of Communication and Digital Technologies
DE	Data Economy
DG	Data Governance
DGI	Data Governance Institute
DHET	Department of Higher Education and Training
DMBOK	Data Management Body of Knowledge
DoJCD	Department of Justice and Constitutional Development
DPC	Data Protection Commission
ECTA	Electronic Communication and Transactions Act
EU	European Union
FPB	Film and Publication Board
GCIS	Government Communication Information System
GDPR	General Data Protection Regulation
HSRC	Human Sciences Research Council
ICASA	Independent Communication Authority of South Africa
ICO	Information Commissioner's Office
ICT	Information Communication Technology
ICTG	Information Communication Technology Governance
IEC	Independent Electoral Commission
IoT	Internet of Things

IR	Information Regulator of South Africa
IS	Information Society
KPI	Key Performance Indicator
MICT	Media, Information and Communication Technologies
ML	Machine Learning
NCC	National Consumer Commission
NLP	Natural Language Processing
NPO	Non-Profit Organisation
PAIA	Promotion of Access to Information Act
POPIA	Protection of Personal Information Act
RSA	Republic of South Africa
SAFPS	Southern African Fraud Prevention Services
SLR	Systematic Literature Review
SMEs	Small and Medium Enterprises
UK	United Kingdom

1. CHAPTER 1: INTRODUCTION

1.1 Statement of purpose

This qualitative study aimed to assess the role and effectiveness of South Africa's Information Regulator (IR) in enforcing the Protection of Personal Information Act (POPIA) within the evolving data economy. The research focused on how effectively the Information Regulator (IR) ensures organisational compliance with data protection, privacy and consumer rights outlined in POPIA, particularly in the context of rapid advancements in Fourth Industrial Revolution (4IR) technologies. Special attention was given to the impact and challenges associated with the Artificial Intelligence (AI) technologies.

1.2 Background of the study

As Digital Technology advances, it fundamentally changes the global economies and technological landscapes. These changes are characterised by the development of innovative methods of production, exchange and consumption, the advent of new economic participants and the increasing complexities in global economic governance. At the core of these transformations is the advancement of Information Society (IS), where the ability to create and accumulate, transmit, preserve, manipulate and interpret data has become pivotal to the emergence of new business models and actors (Sestino, Kahlawi, & De Mauro, 2023).

The concept Information Society is defined as a society where Information and Communication Technologies (ICTs) play a central role in driving economic, social, and cultural activities, enabling the transmission, storage, and dissemination of information (Tunacan & Hatipoğlu, 2021). It is a shift towards The Knowledge Economy where society (individuals, organisations and government) produce, spread and consume information are paramount. Webster and Robins (2013) argue that digital technologies play a crucial

role in enabling real-time communication, knowledge sharing, and fostering global interconnectedness (Webster & Robins, 2013). The World Bank defines the Knowledge Economy as an economy whose knowledge, information and intellectual capital are main drivers of the creation, distribution and use of wealth. It emphasises the contribution of human capital, innovation, and technological change in economic growth and development (Chen & Dahlman, 2006).

Evolution of the Information Society has birthed the Data Economy (DE), a profitable system that taps into every stage of the data lifecycle ranging from capture, storage to analysis and monetisation. It is an expanding phenomenon in many industries fuelled by technological advances and breakthroughs and digital transformation spikes. The waves of the DE are long-lasting and seep into beyond consumer behaviour and business operations, and even policymaking and implementation of the same.

The arrival of 4IR as elaborated by Klaus Schwab in the (World Economic Forum, 2016) and followed by his book titled "The Fourth Industrial Revolution" introduces us to disruptive technologies such as Artificial Intelligence (AI), Advanced Data Analytics, Robotics, the Internet of Things (IoT), Automation and Cloud Computing, just to name a few (Schwab, 2016). These technologies transform industries and drive the DE by providing the way for data collection, processing and utilisation in an efficient way, creating innovation, economic growth and change in society. Such research study only focused on some selective 4IR technologies, i.e., AI and Generative AI.

Critical to harnessing the value of the Data Economy is effective Data Governance (DG), which entails implementing robust data management practices. Data Governance ensures availability, usability, integrity and security, including data protection, privacy and consumer rights and effective risk management controls against any data-related risks (Chen, et al., 2023). The principles of DG align with national and international regulations such as South Africa's Protection of Personal Information Act (POPIA) and the EU General Data Protection Regulation (GDPR), which aims to safeguard consumer data and regulate its dissemination.

The Protection of Personal Information Act (POPIA), which is the equivalent of the EU General Data Protection Regulation (GDPR), was written in 2003 and enacted in 2013, with enforcement beginning fully from July 1, 2021. Protection of Personal Information Act (commonly known as the POPI Act or POPIA) is a South African act that governs the legal processing and processing of personal information. The act is applicable to any organisation or business including individual that are incorporated in and trade with information or records of information pertaining to personal information in the Republic of South Africa (RSA). The act requires the minimum requisite or requirements (principles) to be met for the protection and effective handling of personal information. Personal Information refers to any information which can successfully identify an individual (Swales, 2022).

The Information Regulator of South Africa (IR)

The South African Information Regulator (IR) is an independent regulatory body mandated to protect personal information, enforce compliance with data protection laws, and promote access to information (Information Regulator, 2022). It oversees the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA), with roles including handling complaints, conducting investigations, raising public awareness, monitoring compliance, and issuing guidelines. The IR consists of a chairperson and four ordinary members, two of whom are appointed by the President upon the National Assembly's recommendation. Its decisions are binding unless overturned by a South African court (Information Regulator, 2024).

The organisational structure of the Information Regulator of South Africa as depicted in Figure 1 below is designed to support its dual mandate under POPIA and PAIA. Led by a Chairperson and Members, operational functions are overseen by the Chief Executive Officer. The structure comprises six core divisions POPIA, PAIA, Education and Communication (EDUCOM), Legal Services, Corporate Services, and Financial Management, along with a Provincial Coordination Sub-Division and internal audit functions.

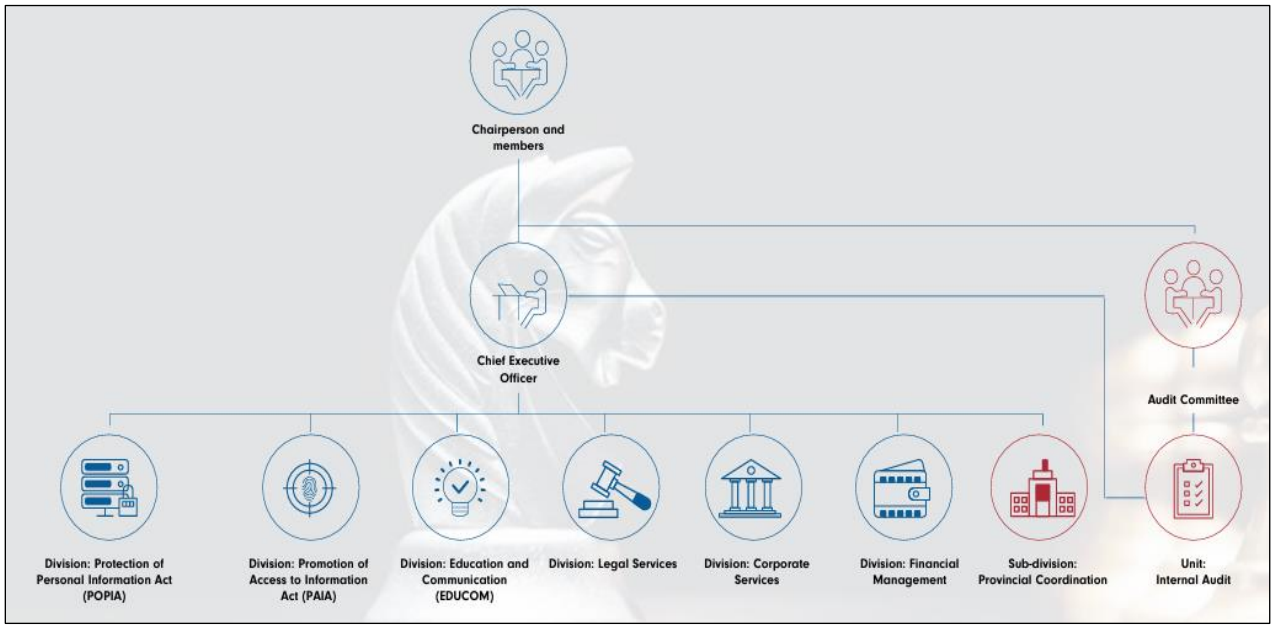


Figure 1. Information Regulator Organogram. Source: (Information Regulator RSA, 2023)

Artificial Intelligence Market in South Africa

The projected AI adoption growth in South Africa Statista Market Insights (2024) analysis shows significant expected growth, it is estimated that the growth of the AI market size in South Africa will be worth over US$4.00bn by 2030. This is a significant growth from the previously projected market reach of US$0.90bn in 2024 (Statista, 2024). Formulating effective governance policies requires addressing associated risks and balancing AI's potential through a collaborative approach involving multinational stakeholders. Figure 2 depicts the expected market growth (Statista, 2024).

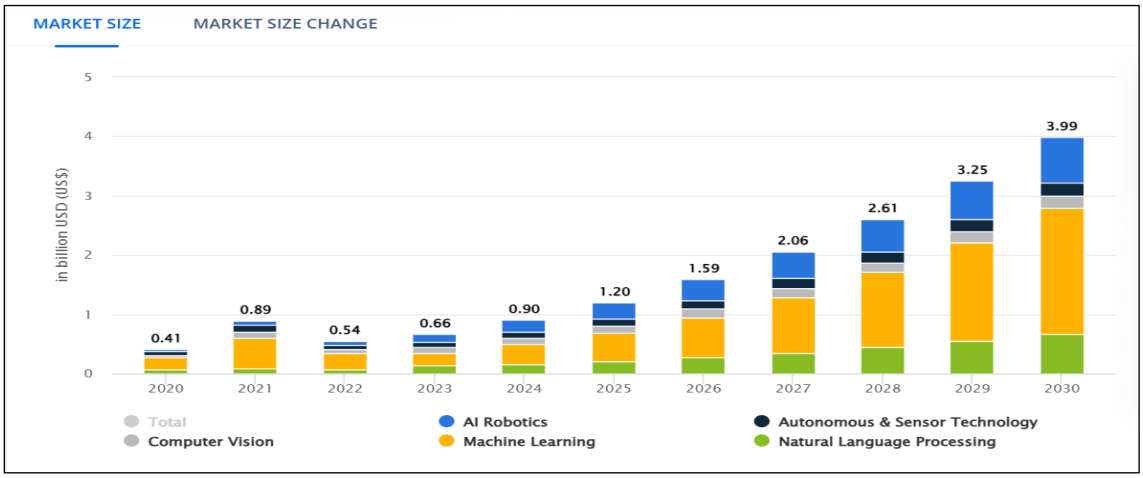


Figure 2. AI Market Size in South Africa. Source: (Statista, 2024)

Emerging Technologies Challenges

Poor security protocols have exposed many firms to cyber-attacks, and a large share of data breaches (CIPIT, 2023). Besides the foregoing, the expansion of AI technologies has also been accompanied by an intensified impact on the exploitation of data-related activities. This is largely being felt in terms of false information which has been growing exponentially in the cyber world. Cyberbullying is another hateful trend perpetuated by the dissemination of AI technologies (OECD, 2021).

An increase in illegal use of personal data, identity theft, or impersonating identities is another dire trend in South Africa. Southern African Fraud Prevention Services (SAFPS), a Non-Profit Organisation (NPO) concerned with fraud prevention released a 2023 report that a growing incidence of identity theft is alarming (SAFPS, 2024). Consumer data is being compiled and used by many organisations without acquiring the same from consumers with visible consent. Target marketing is the most frequent use of their information. This has led to an overwhelming amount of unsolicited marketing with customers being inundated with unwanted promotional materials and ads (OECD, 2021).

These widespread data exploitation practices enabled and amplified by AI create an increasingly complex enforcement landscape for South Africa's Information Regulator (IR). AI systems often operate in a black-box, evolving algorithms that make data processing and decision-making difficult to interpret or audit. This presents a significant

challenge for the IR, whose mandate requires proactive monitoring and enforcement under the Protection of Personal Information Act (POPIA). Furthermore, the pace at which AI technologies are advancing far exceeds the regulator's current ability to adapt legislation, issue timely guidance, or establish adequate safeguards. As a result, enforcement remains largely reactive, leaving gaps in oversight and creating opportunities for non-compliance and abuse. This regulatory lag reinforces the urgent need to assess and strengthen the IR's role in governing AI-related data practices.

1.3 Research Problem

With the rapid adoption and evolution of AI technologies, there is a growing concern about data privacy, data protection and ethical use of data which affects consumer rights. Despite the potential benefits of AI technologies, their vast adoption and growth have led to an increase in risk exposure to data breaches, consumer vulnerabilities and unauthorised use of personal data.

Whilst the Protection of Personal Information Act (POPIA) offers a much-needed legislative framework for information protection in South Africa, the enforcement role falls primarily with the Information Regulator (IR). Yet, a review of the IR's recent annual reports indicates a noticeable gap; the risks and regulatory challenges posed by Artificial Intelligence (AI) technologies are not meaningfully addressed. This omission is particularly concerning with the exponential growth of AI applications in finance, healthcare, marketing, and law enforcement, all of which involve the processing of personal data on a mass scale. This not only heightens the risks of failure to comply with POPIA in AI-driven ecosystems but also exposes individuals to automatic decision-making, algorithmic bias, and inscrutable data processing. This qualitative study aimed to assess the role and effectiveness of the South African Information Regulator in enforcing the POPIA amid the challenges posed by emerging Fourth Industrial Revolution (4IR) technologies, particularly AI.

Reported Data Breaches

Numerous reported incidents relating to data breaches and cybersecurity attacks driven by AI capabilities have been recorded. In 2022, TransUnion, a global credit bureau, experienced multiple breaches, including one involving a ransom demand of R224 million linked to the exposure of approximately 54 million identity records. A separate breach by its U.S. counterpart compromised over 22 million individuals, revealing the cross-border implications of data security lapses. The exposed data included sensitive personally identifiable information (PII), such as names, addresses, and financial records (TransUnion, 2022).

Also in 2022, Dischem was affected by a brute-force cyberattack on a third-party service provider, leading to the compromise of data for approximately 3.6 million customers. This incident attracted the attention of the IR, who signalled a potential penalty of R10 million, highlighting the regulatory risks of weak third-party data governance (ITWeb, 2022). In 2020, Experian South Africa suffered a breach that impacted approximately 24 million individuals and 793,000 businesses. The incident, reported by the South African Banking Risk Information Centre (SABRIC), raised significant concerns about data handling within the financial sector. In 2021, Postbank, a division of the South African Post Office, experienced a cyberattack involving the fraudulent crediting and withdrawal of funds from grant beneficiary accounts, resulting in an estimated financial loss of R90 million (RSA Government, 2022).

These incidents highlight not only increasing threats to data privacy but also reveal the limited preparedness of the Information Regulator in managing such rapidly evolving risks. Unlike conventional threats, AI systems introduce complex, opaque, and adaptive mechanisms that make it difficult to trace or predict breaches in advance. This poses a regulatory dilemma, as AI technologies evolve faster than regulatory responses, a widening gap emerges between enforcement capacity and real-world risk, making compliance both more critical and more difficult to enforce.

Table 1. Selected Data Breach Incidents in South Africa. Source: Multiple Sources

Organisation /Sector	Incident Description	Year	No. Affected Customers	Estimated Revenue Impact
TransUnion	In 2022, TransUnion, a major credit reporting agency, experienced a data breach. During this incident, unauthorised individuals gained access to sensitive personal information stored in TransUnion's databases. The breach exposed details such as names, addresses, Social Security numbers and financial data of affected individuals (TransUnion, 2022). In 2022, TransUnion (USA) reported a data breach exposure affecting more than 22 million, with personally identifiable information at risk and possible impact on government agencies (TransUnion USA, 2022).	2022 2022	Over 5 million consumer data and Businesses: 600k 4TB data – 54m identity information. Over 22 million identities	R224m – ransom demand
Dischem	In 2022, a third-party service provider (Grapevine) for Dis-Chem experienced a brute-force attack carried out by a	2022	3.6m customers	R10m Information

	cybercriminal. In a brute force attack, the hacker systematically tries various combinations of characters to crack a password until the correct combination is discovered (ITWeb, 2022).			Regulator potential penalty
Experian South Africa	Experian South Africa, a credit reporting company, suffered a data breach in August 2020. Approximately, 24 million South Africans and 793,749 business entities were impacted. The breach involved a fraudster posing as a client and requesting access to Experian's services. The fraudster was able to extract personal and business information, such as names, ID numbers and bank account details (SABRIC, 2020).	2020	24m personal information 793k business entities - SABRIC	
Post Office/Post bank	In 2021, Postbank fell victim to a cybercrime attack, resulting in an estimated financial loss of R90 million. The fraudulent scheme involved illegally crediting grant beneficiary accounts with substantial sums and subsequently withdrawing the funds from these accounts (RSA Government, 2022).	2021		Approximately R90m

1.4 Research Questions

The following research questions were developed to guide the research discussions and assist in understanding the impact of each of the research components:

1. How have POPIA and related data privacy infringement cases been dealt with in South Africa?
2. How effective is the Information Regulator in enforcing POPIA regulations?
3. How effective are POPIA provisions in governing the risks emanating from AI technologies and mitigate data privacy issues?
4. What are the challenges emanating from Generative-AI concerning data privacy, protection, and consumer rights in South Africa?

1.5 Research Propositions

- Data privacy infringement cases in South Africa have been managed ineffectively.
- The South African Information Regulator is not fully effective in enforcing compliance requirements of the POPI Act.
- The current POPIA provisions are inadequate to fully address the rapidly evolving risks and challenges associated with AI technologies on data privacy.
- South African consumers face increasing exposure to risks associated with Generative-AI and are vulnerable to data breaches and misuse.

1.6 Significance of the study

The advent of the Fourth Industrial Revolution (4IR) and the exponential growth of Artificial Intelligence (AI) technologies have transformed the Data Privacy and Protection and risk management environment. The growth of these technologies' capabilities, particularly Generative AI and Machine Learning has witnessed an

unprecedented data explosion in the volume, variety and velocity of data created and processed and thus new risks and complexities to data protection and privacy.

This research work is of paramount significance in the above regard. It answers the imperative call to understand how data protection and privacy, are being managed. The research aimed at acquiring insightful understanding of the challenges that the Information Regulator is encountering in enforcing application of data protection policies for guarding personal information and upholding POPIA principles.

Furthermore, the research will contribute to academic literature, as well as ongoing debates and policy-making processes concerning data regulation and governance.

1.7 Definition of terms

Table 2. Key Terms/Concepts Definitions and Sources

Term	Definition
Data Economy	"The Data Economy is the global digital ecosystem in which the producers and consumers of data - businesses and individuals and government and municipal agencies gather, organise and share accumulated data from a wide variety of sources (MIT Technology Review, 2021)". "Data Economy refers to a correlated set of activities aimed at the process of extracting value and valorising different data, using varied but integrated processes of generation, collection, processing, analysis, automation and exploitation of data made possible by digital technologies (Sestino et al., 2023)".

Data Governance	Establishes accountability, policies, and decision rights to ensure data is managed properly vital for compliance, risk management, and organizational alignment (DAMA International, 2017).
Information Society	Information society is the society which is at a step of development of the modern civilization which is characterized by increase in a role of information and knowledge in life of society; increase of a share of information and communication technologies, information products and services in gross domestic product; creation of the global information infrastructure providing information exchange of people, their access to information and satisfaction of their social and personal requirements (Grishin, Boichenko, & Lukinova, 2020).
4IR	“Industry 4.0, the Fourth Industrial Revolution and 4IR all refer to the current era of connectivity, advanced analytics, automation and advanced manufacturing technology that has been transforming global business for years. This wave of change in the manufacturing sector began in the mid-2010s and holds significant potential for operations and the future of production (Mckinsey & Company, 2022)”.
Artificial Intelligence	“Artificial Intelligence (AI) is a set of methods or automated entities that together build, optimize and apply a model so that the system can, for a given set of predefined tasks, compute predictions, recommendations, or decisions (NLP) (ISO, 2022)”.

Generative-AI	"Generative AI refers to AI systems whose primary function is to generate content and provide new possibilities for users (Gmiterek & Kotuła, 2025)". "Generative AI is a subset of AI that includes large language models (LLMs) capable of generating text, images, code, and sound (Toner, 2023)".

1.8 Assumptions

The following assumptions have been made regarding the research study:

- The respondents had sufficient knowledge and understanding of the topic to provide meaningful responses.
- The respondents were presumed to provide open and honest feedback and to articulate any discomfort with the questions posed.
- The responses given by interviewees were interpreted accurately and without bias.

1.9 Delimitations of the study

- The study focused on the enforcement of POPIA by the South African Information Regulator, with a particular emphasis on risks associated with emerging technologies.
- While the study examined data protection and privacy issues, it did not delve deeply into other aspects of data governance, such as data quality, data integration, or data architecture.
- The study employs a comparative analysis approach by referencing other established data protection regulations, such as the General Data Protection Regulation (GDPR) of the European Union, for benchmarking purposes.

- A qualitative research method was employed due to its strength in providing in-depth insights into the research topic and addressing the research questions.
- Participants were selected based on their expertise in the study area and their involvement in data regulations and compliance practices.

1.10 Chapter Outline

Chapter 1	This chapter introduces the context of the data economy, underpinned by data governance, advancements in digital technology (highlighting both risks and opportunities) and its associated regulations and compliance. It provides a comprehensive background to the research problem, formulates the research questions, and explains the rationale behind the study.
Chapter 2	This chapter delves into a thorough review of existing studies, published reports and regulations that revolve around the key focus concepts and dimensions. It formulates the research propositions and covers the key theoretical frameworks and conceptual model that underpin this study.
Chapter 3	This chapter outlines the methodology followed for conducting the research study. It details the strategies for data collection, sampling, data analysis and presentation, research instrument, research limitation and all ethical undertaking of the study.
Chapter 4	This chapter present the findings derived from the data collection process in a detailed and structured manner.

Chapter 5	This chapter discussed and analysed the data findings, extracting valuable insights and interpretations from these findings.
Chapter 6	The final chapter summarised the study findings and their implications. It also provided thoughtful recommendations for future consideration, based on the insights derived from the study.

2. CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In this chapter, a detailed review of the currently available literature relevant to this study is conducted. The chapter begins with performing an analysis of the selected theoretical frameworks pertinent to this study. This is followed by a review of prior literatures focusing on the governance of data at the organisational micro level and the role of the Information Regulator in ensuring effective policy implementation and adherence to enforcement.

The following theories and framework are instrumental in providing a robust foundation for the research and the concepts that support theoretical constructs upon which this study is grounded:

- Information Society Theory
- The Theory of Regulation (Public Interest)
- Data Governance Framework (Organisational Level)

2.2 Information Society Theory

The Information Society theory has been in existence since the 1970s (Webster, 1995, 2006). It was during this time that the foundations of this idea were laid as the world began recognising the increasing importance of information in economic and social processes. Scholars such as Prof. Manual Castells have written extensively on the idea and his rationale is explored further in this section. Castells (1997) defines the Information Society as a society where the creation, processing and transmission of information become the principal sources of economic activity and power. He points out the shift from industrial economies to knowledge-based economies where ICTs play a significant role. This is characterised by the worldwide spread of digital technologies and the domination of information processing in economic, political and cultural processes (Castells, 1997). Castells (2010) further introduced the concept of

the Network Society in his book titled "*The Information Age: Economy, Society and Culture – Volume I: The Rise of the Network Society*", emphasising the transformative impact of networked communication technologies on social relationships and Organisational forms. He argues that Networks are not simply technical structures but social ones that enhance new patterns of interaction, cooperation and collective action. Networked individuals and organisations operate in a decentralised manner, characterised by flexible connections rather than rigid hierarchies (Castells, 2010).

The concept evolved throughout the 1980s, however, it was not until the 1990s that it significantly took off and gained widespread recognition. This was due to the advent of digital technologies, which revolutionised the way information was created, stored, processed and disseminated (Gunter et al., 2009; Hiranya, 2017).

At its core, the Information Society encapsulates a shift towards a knowledge-based economy, where information becomes a crucial asset driving innovation, productivity and global connectivity (Toivanen, 2012). Some view it as a society where ICT enables the creation, distribution and manipulation of information and has become the most significant economic and cultural activity (Lnenicka & Komarkova, 2019). Webster (2006) defines the Information Society using 5 key components - Technology, Economic, Occupational, Spatial and Cultural, each with distinguished factors, but related on a foundational level by their interconnectedness and influence (Webster, 1995, 2006).

Technology focuses on the role of Information and Communication Technologies (ICTs) in the Information Society. It is centred around innovations and encompasses the rapid evolution and integration of technologies and network infrastructures, essential for communication, data storage and knowledge dissemination. This includes the adoption of digital platforms, the use of internet-based communication facilities and the use of mobile devices.

For the Economic component, Webster (2006) further argues that the Information Society thrives on producing, distributing, and consuming information as a primary economic resource. Occupational, Information Society introduces new professions

and skill sets, highlighting the changes in work and employment. Spatial, includes the phenomenon of globalisation, the rise of global communication and connectivity. This brings about virtual collaborations and remote work environments, transforming how businesses operate, and societies interact. Culturally, the Information Society fosters cultural diversity and identities through digital platforms, challenging traditional norms and enabling global cultural exchanges (Webster, 1995, 2006).

The Information Society Theory and the Data Economy concept are closely intertwined due to their shared focus on the transformative effects of ICTs on society, economics and culture. Both concepts highlight the need for robust policies and governance frameworks to manage the ethical, legal and regulatory challenges posed by the widespread use of ICTs and data. This includes issues related to privacy, security, intellectual property rights and access to digital resources (Castells & Cardoso, 2006).

The Data Economy concept was first introduced in connection with digital economic space worldwide. It gained prominence in recent years due to the increasing significance and impact of digital technology on businesses and society (Sestino et al., 2023).

The debates on the need to regulate the proliferation of digital information still forms part of key discussions globally. In the recently published article from G20 discussions on the Digital Economy in Brazil, Manuel Castells highlighted the need to regulate the network to cap the spread of misinformation and other social ills (G20 Brazil, 2024). Figure 3 below depicts the Data Economy ecosystem and its relationship with other significant components relevant to this research study.

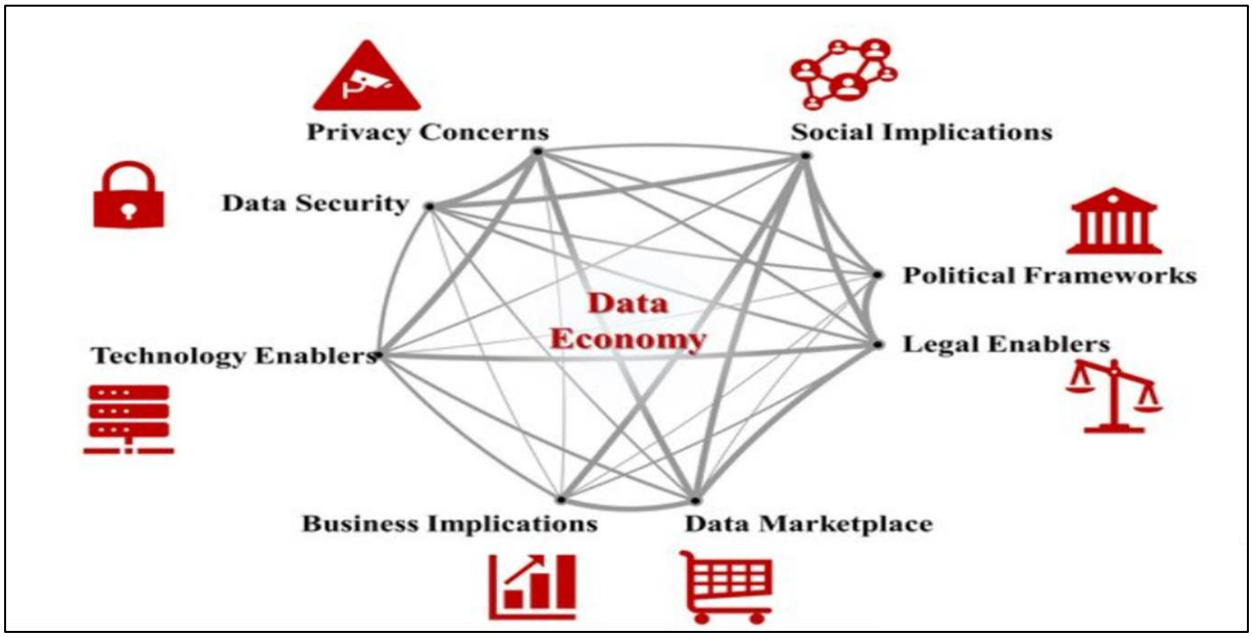


Figure 3. The Data Economy Conceptual Model. Source**:** (Sestino et al., 2023)

In the context of South Africa, considering its social standing, notable challenges to technological advancement that society must navigate include full public participation and disparities in access to ICTs deepening existing inequalities, perpetuating marginalisation among vulnerable populations (World Bank, 2022). Simultaneously, the proliferation of digital surveillance and extensive data collection raises profound concerns regarding privacy rights and civil liberties. Moreover, the ethical dimensions of these technologies, encompassing challenges such as algorithmic bias and the spread of misinformation, underscore the urgent need for rigorous oversight and regulatory frameworks to safeguard societal values and ensure equitable participation in the digital age.

South Africa's King IV Code, which provides a practical and principle-based approach to good corporate governance, highlights compliance as integral to sustainable business practices, aligning organisational goals with societal expectations (IODSA, 2016). These frameworks should include clear procedures and policies for the storage, collection, processing, and dissemination of data. They need to include provisions for

the individual to have control of their data such as the ability to access, correct or delete their data.

A study by Fritz-Morgenthal et al. (2022), emphasises the growing complexity of financial models, from simple rules-based to sophisticated AI and Machine Learning (ML) models. It highlights the need for a risk-based governance framework to manage these models, which is crucial as financial institutions increasingly rely on AI for decision-making processes (Fritz-Morgenthal, Hein, & Papenbrock, 2022). As the adoption of AI technologies becomes increasingly prevalent in financial services, the management of personal and confidential information takes on heightened importance (Oyewole, Oguejiofor, Eneh, Akpuokwe, & Bakare, 2024).

2.3 Public Interest Theory of Regulation

The Regulation Theory emerged in the 1970s as a method of analysis on how the state regulates economic affairs and governs capitalist economies. Drawing from French economist Michel Aglietta (1976), Regulation Theory counteracts the axioms of standard neoclassical economics in emphasising the centrality of institutions, government action, and social practices in attaining economic growth and stability. It became especially relevant for its analysis of the development of capitalist economies, particularly in light of the economic crises and structural shifts that defined the late 20th century (Aglietta, 1976).

Morgan and Yeung (2007) defines theory of regulation as a collection of propositions or assumptions that attempt to explain the origin of regulations, identify the participants who play a role in their development and describe the usual dynamics of interaction among these regulatory entities (Morgan & Yeung, 2007).

The Public Interest Theory of Regulation began during the late 19th and early 20th centuries in response to increasing monopoly power and the necessity for government action to safeguard the public interest. Stigler (1971) contends that regulation which is shaped by the interests of the industries regulated, not by the public interest alone, might be captured by the industries that they regulate. This notion of regulatory capture

has been in question about the effectiveness and purity of regulatory processes (Stigler, 1971).

Steven P. Croley's book, Regulation and Public Interests: The Possibility of Good Regulatory Government (2008), thoroughly explores the principles of effective regulatory governance. It delves into how regulation intersects with public interests, highlighting the potential for achieving good regulatory governance. Croley (2008) argues that "good regulatory government" is characterised by its capacity to balance regulatory efficiency with responsiveness to public needs. He stresses the importance of a regulatory system that is not only efficient but also democratically legitimate and publicly acceptable (Croley, 2008).

Croley's vision of good regulatory government is in sync with contemporary regulatory theory that emphasises efficiency and accountability. The challenge, however, lies in the practical implementation of such a balance. Croley believes that regulatory agencies should utilise informed professionals so that regulations will be based on good scientific and technical data. He also believes that openness and accountability are the foundation of good regulatory governance. Croley also argues that good regulation not only requires technical expertise but also the engagement of a variety of public voices to ensure that regulations reflect wider societal interests and values (Croley, 2008). Transparency and accountability are universally regarded as core components of good governance. Studies by other scholars note that transparent regulatory processes can increase public trust and compliance (Schillemans & Bovens, 2019).

Hantke-Domas (2003) critically evaluates the public interest theory of regulation and challenges its theoretical soundness and usefulness in practice. He examines the theory’s claim that regulation serves the public interest and contrasts it with alternative perspectives, such as the capture theory. Hantke-Domas argues that the theory assumes a level of goodwill and rationality by regulators that fail to account for the dynamics of regulatory environments, including political and economic stress.

The Theory of Regulation profoundly impacts policy implementation by framing how regulations are designed, enforced and evaluated. Policy implementation scholars, like (Pressman and Wildavsky, 1984), emphasise the pivotal role of regulatory agencies in translating legislative mandates into practical actions. This involves balancing regulatory objectives with operational constraints and stakeholder interests (Pressman & Wildavsky, 1984).

While the public interest theory establishes an idealised framework that proposes that laws are passed in the public interest, empirical evidence tends to portray a more complex situation. The POPI Act of South Africa, for instance, is a regulatory framework that is intended to protect people's personal data and privacy, in the public interest. However, the success of and rigorous adherence to POPIA have been undermined by challenges such as inconsistent adherence among organisations, which led to concerns being expressed.

Section 5 of the POPIA Act, which is titled "Rights of Data Subjects," gives a legal framework for handling personal information. It mandates that personal information must be processed lawfully and ethically, thereby safeguarding the right to privacy of data subjects. This framework contains several significant rights, including the right to be informed about the collection of personal information, the right of access and rectification of personal information, and the right to object to the processing of personal information (POPIA, 2019).

Constitutional Right

The South African Bill of Rights, as inscribed in the Constitution of the Republic of South Africa, is a pillar of South African democracy. It confirms the democratic pillars of human dignity, equality and freedom and it obliges the legislature, the executive, the judiciary, and all state organs under the force of law binding upon all the laws. It contains rights like equality, life, freedom of expression, political rights and others (RSA Constitution, 1996).

In its preamble, the Protection of Personal Information Act of 2013 recognises section 14 of the Constitution of the Republic of South Africa of 1996, which declares that everyone has the right to privacy, this includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. It further asserts that “The State” must respect, protect, promote and fulfil the rights in the Bill of Rights (RSA Government Gazette, 2013). The POPI Act and the South African Bill of Rights are closely connected, as both strive to safeguard and uphold individuals' fundamental rights, the right to privacy.

POPIA gives expression to the right by creating an environment in the law where information that is personal can be processed in a manner that respects the right to privacy. POPIA and the South African Bill of Rights substantially work together in protecting people's rights, particularly in processing their personal information. They ensure that such processes are conducted in a manner that respects and upholds the inherent rights of all people in South Africa.

POPIA aims to safeguard personal data from theft, misuse and malicious activities, uphold the constitutional right to privacy and facilitate international trade by ensuring adequate data protection. The Act applies to any processing of personal information by entities in South Africa or abroad using means to process in South Africa. It covers both public and private entities and extends to the workplace, considering job applicants and current and former employees as "data subjects".

Drahos and Krygier (2017) argue that good regulation is concerned with robust institutional arrangements for coordination and coherence among different stakeholders. This can be applied to data protection regulation like POPIA, which stipulates institutional responsibility and governance arrangements to attain data protection compliance. The authors highlight the role of networks in the regulation process, referring to how interactions between stakeholders influence the regulation process. This is applicable in data protection laws, where cooperation among regulators-businesses-data subjects is necessary for effective implementation and enforcement (Drahos & Krygier, 2017).

The scholars further argue for adaptive regulatory approaches that balance flexibility with restriction, crucial in addressing evolving technological landscapes. This is pertinent to AI policies, where regulatory frameworks must adapt to the rapid advancements in artificial intelligence while ensuring ethical standards and data privacy protections. From a global perspective and harmonisation, they also highlight the interconnected nature of regulatory frameworks globally, advocating for international cooperation and harmonisation. This perspective aligns with GDPR's extraterritorial scope and efforts to harmonise data protection standards across the EU. To strengthen POPIA, this study aims to look at how POPIA can leverage other similar matured globally renowned policies (Drahos & Krygier, 2017).

2.4 Data Governance Framework (Organisational)

In the modern era of technological advancement, the ability and velocity of data acquisition and utilisation have escalated exponentially. The framework helps organisations develop comprehensive data governance strategies that align with their business objectives and regulatory requirements (DAMA International, 2017).

Numerous institutions have developed various Data Governance Frameworks to address the complex challenges organisations face in managing data effectively. Popular frameworks include The Data Management Association International-Data Management Body of Knowledge (DAMA-DMBoK), Data Governance Institute (DGI) Framework, and The Data Management Capability Assessment Model (DCAM) Framework. This study focused on DAMA-DMBoK Framework. DAMA is a global non-profit organisation established in 1980 dedicated to advancing excellence in data and information management by formulating standardised methodologies, principles, and terminologies within the field (DAMA International, 2017).

Ndemo et al. (2023) argues that implementing a robust data governance strategy requires a thorough understanding of the process involved in translating data into information and policy measures (Ndemo, Ndung’u, Odhiambo, & Shimeles, 2023). Eryurek et al. (2021) emphasise the need for a holistic approach to implementing a

data governance framework, considering all stages of the data lifecycle, from data consumption to inventory, data usage and eventual deletion (Eryurek, et al., 2021).

Expanded data management lifecycle is depicted in Figure 4. Governing the use of data is essential, as it enables organisations and customers to establish trust implement control measures and treat their data as key business assets. This is further highlighted in The King IV Code on Corporate Governance (a globally renowned framework on principles, standards and guide on corporate governance and ethical leadership), the importance of effectively implementing regulations and policies within organisations to ensure ethical conduct, transparency and accountability (IODSA, 2016).

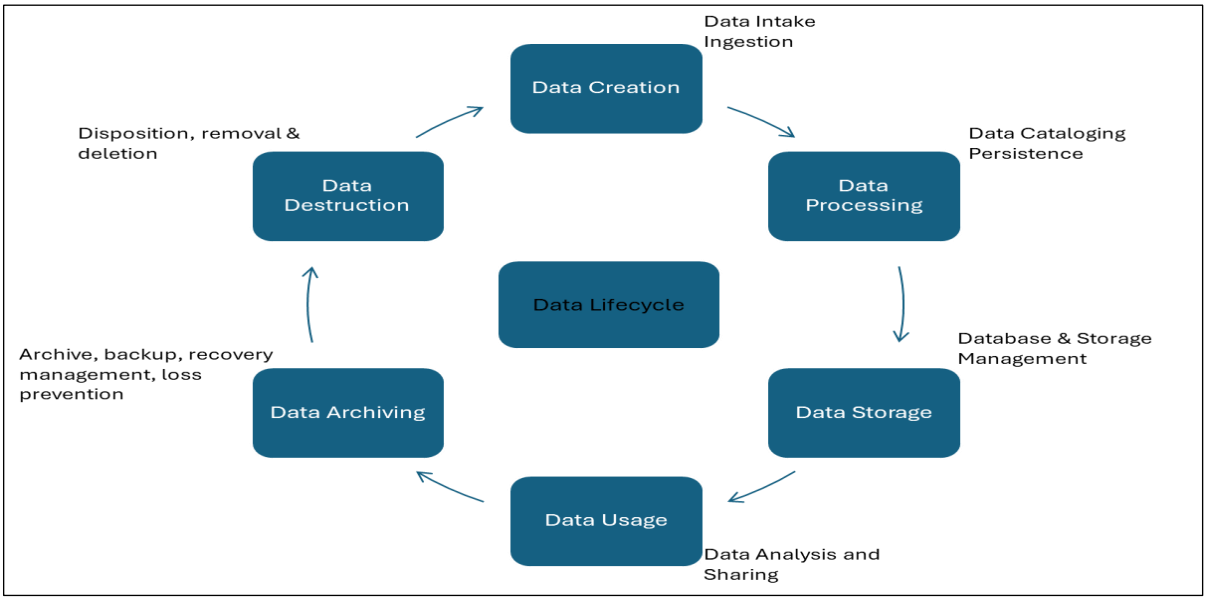


Figure 4. Expanded Data Lifecycle

DAMA Framework (Organisational Level)

DAMA published Data Management Body of Knowledge (DMBOK2), which outlines various frameworks developed by industry experts (Ruslan, Alby, & Lubis, 2023). These frameworks provide concepts that organisations could adopt and apply depending on various factors and companies' circumstances such as levels of data management maturity, operating model, the size of the organisation and its strategic vision (DAMA International, 2017).

The DAMA Wheel, a well-known and widely used framework, outlines 11 Data Management Knowledge Areas, including Data Architecture, Data Modeling and Design, Data Storage and Operations, Data Security, Data Integration and Interoperability, Document and Content Management, Reference and Master Data, Data Warehousing and Business Intelligence, Metadata Management, and Data Quality Management. As shown in Figure 5, these knowledge areas are depicted in a wheel, with Data Governance placed at the centre to emphasise its role in ensuring a standardised approach across all disciplines (DAMA International, 2017).

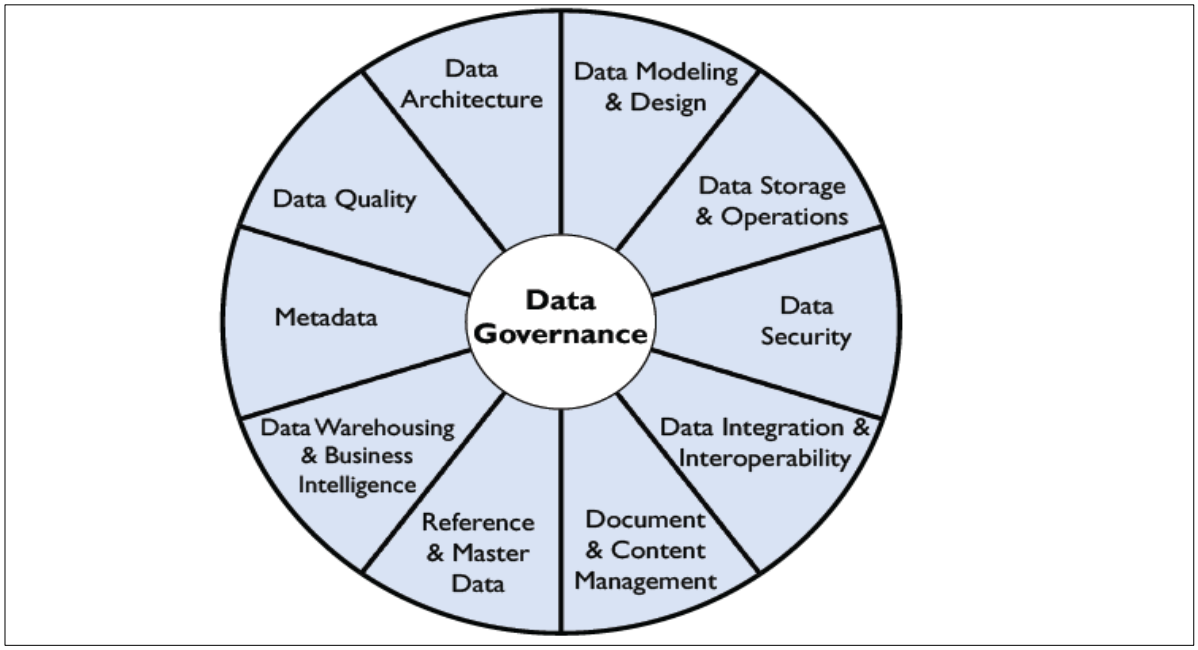


Figure 5. The DAMA Wheel Framework. Source: (DAMA International, 2017)

The framework emphasises the critical roles of people, processes and technologies in effectively implementing and managing data, as outlined by DAMA International (2017). It illustrates the interconnected nature of data protection regulations, policy implementation, their impact on individuals and the pivotal role of technology within this ecosystem (DAMA International, 2017).

The DAMA Wheel Framework is further expanded in the DMBOK2 by incorporating the data management lifecycle into its Wheel model, integrating foundational activities within the scope of data governance. Figure 6 below shows an evolved DAMA Framework. All core components important in enabling the successful protection and management of the data are highlighted in the framework (DAMA International, 2017). DAMA Wheel Evolved underscores the importance of Data Protection, Privacy, and security as activities in the framework, which further signifies the importance of implementing policies to ensure adequate data risk management.

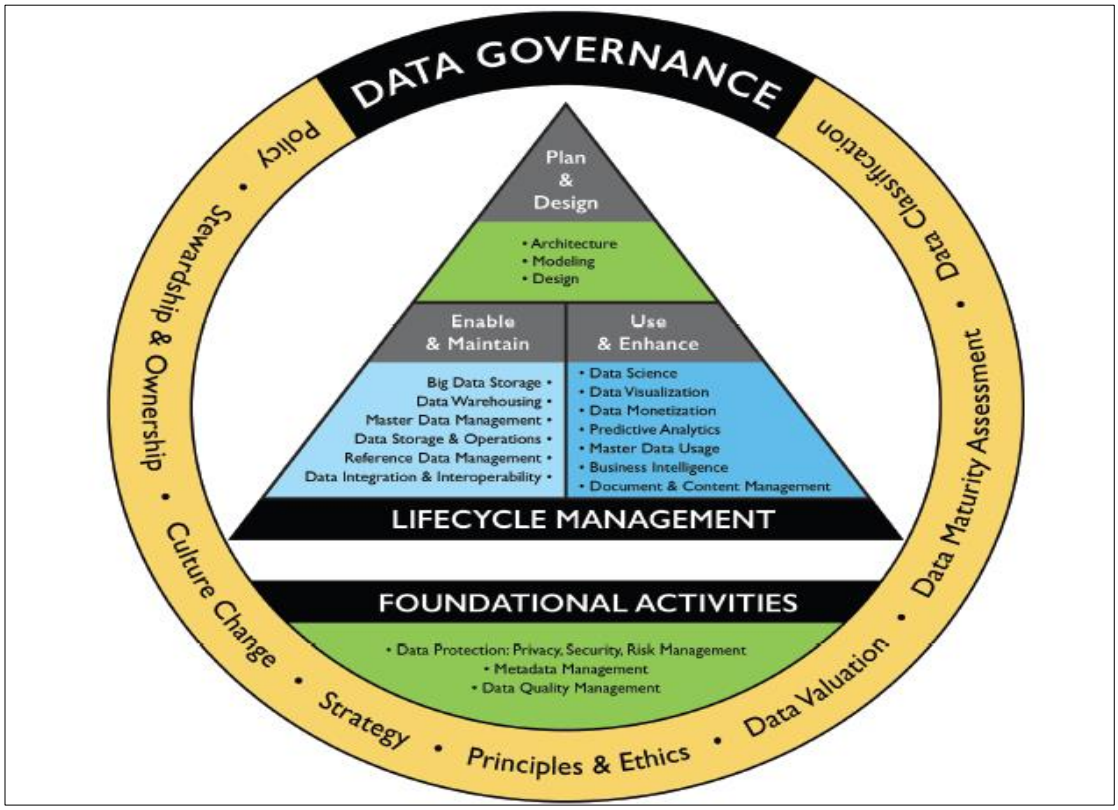


Figure 6. The DAMA Wheel Framework Evolved. Source: (DAMA International, 2017)

A study by Veiga (2022) uncovers a disparity between consumers' high expectations for data privacy and data protection versus their perception that organisations are not adequately addressing these expectations. This highlights the challenges in safeguarding consumer rights in the context of data privacy and protection further exacerbated by the rapid growth of AI. The gap highlighted in the study done by Veiga shows the lack of trust in organisations' capacity to maintain data personal, and this highlights the need for stringent and effective policy development and implementation in fostering trust and transparency (Veiga A. d., 2022).

Figure 7 below illustrates the relationship paradigm, outlining components within data governance and the data management lifecycle. It explores their interactions with emerging digital technologies and emphasises the inherent risks associated with these relationships on data privacy and protection.

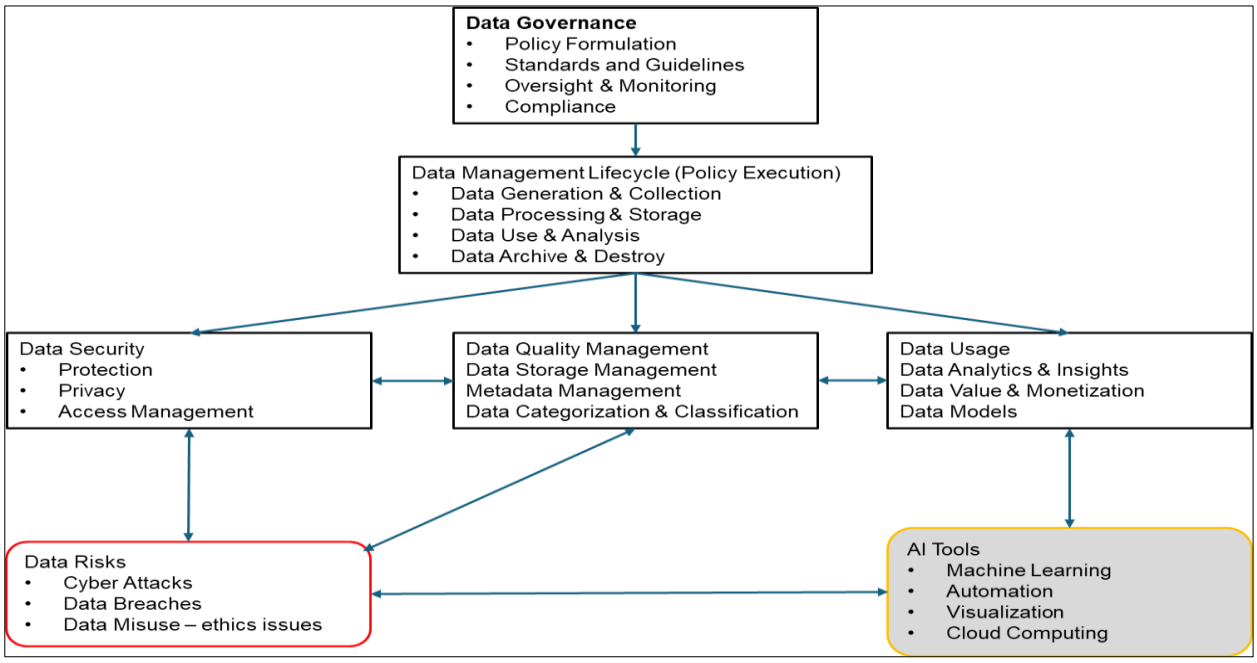


Figure 7. Data Governance, data lifecycle management & AI relationship illustration.

2.5 Prior Studies – Literature Review

This literature review assists in providing answers to the research questions outlined in Chapter One of this study. A Systematic Literature Review (SLR) approach was utilised focusing only on a selected SLR relevant to this study, to answer the formulated research questions. The primary sources of research material comprise a collection of scholarly journals from selected research databases, books, published reports, and regulatory policies. Additionally, insights are gathered through interviews and feedback from relevant stakeholders, including regulatory bodies, banking associations, and consultancy experts in data regulation compliance.

Regulatory Gaps in POPIA and Comparative Legal Frameworks

The Protection of Personal Information Act (POPIA) serves as South Africa's primary legislation for safeguarding personal data. However, its compliance and effective enforcement are frequently questioned, especially when benchmarked against international standards.

Lee (2021) compares POPIA with the European Union's General Data Protection Regulation, pointing to major weaknesses in enforcement mechanisms. Although POPIA entrenches the right to privacy as a constitutional right and offers avenues for data subjects to seek accountability and recourse from data handlers for breaches of data protection, its enforcement is weaker than that of the General Data Protection Regulation (GDPR). The research cites that although POPIA makes reference to international norms, it falls short in terms of civil remedies and administrative fines compared to the more robust GDPR framework (Lee, 2021). These weaknesses suggest that South Africa's framework may offer less deterrence or remedy than global counterparts.

Critically, Lee's study surfaces a regulatory weakness but stops short of exploring how these legal gaps impact compliance behaviour in practice. This study addresses that limitation by examining how such enforcement limitations are perceived by stakeholders and whether they influence organisational compliance efforts.

Sector-Specific Compliance Challenges

The practical application of POPIA across sectors reveals uneven levels of compliance, driven by resource, capacity, and awareness disparities. Warikandwa (2021) examined the suitability and adequacy of South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) in safeguarding personal data within the country's financial services sector. Warikandwa points out that while POPIA aims to protect personal data, its practical application within the financial services market reveals significant hurdles, such as insufficient regulatory infrastructure and enforcement mechanisms (Warikandwa, 2021).

Warikandwa's research provides valuable insights into sectoral POPIA enforcement challenges. Examination of enforcement and resource challenges highlights areas for improvement. Further analysis would be beneficial, however, in examining how these challenges affect other sectors and potential solutions to enhance regulatory effectiveness.

Building on this, Chimboza and Smith (2024) find a marked divide in POPIA compliance between large firms and SMEs, with the latter experiencing greater difficulties due to limited technical and financial resources. The study attributes the variance to resource availability since SMEs are likely to have limited financial and technical capacity to embrace sound data protection policies. Additionally, organizations are faced with serious challenges like expensive compliance, low awareness, and technical problems in matching their existing systems with regulations. Resistance of employees and leaders also renders compliance more challenging, as the majority view data protection as a burden rather than as a strategic necessity (Chimboza & Smith, 2024).

Similarly, Veiga et al. (2024) emphasize that SMEs struggle with inadequate infrastructure, limited understanding of compliance obligations, and poor regulatory support. Low levels of awareness and understanding of data protection obligations remain a major stumbling block, particularly for SMEs (Veiga, et al., 2024). Most business owners and operators have not fully grasped the complexities of compliance,

and as a result, they have been implementing data protection controls inefficiently. Resource limitations create the biggest challenge to compliance with data protection, particularly for small businesses that lack the economic and technological means to employ robust security measures (Veiga, et al., 2024). SMEs lack capacity to adequately invest in data protection infrastructure and capabilities, leaving their sites vulnerable to data breaches and compliance expenses.

Findings from the above studies collectively indicate a systemic challenge, while the legal framework exists, the organisational and technical ecosystem needed to support it remains underdeveloped. What remains underexplored is how these limitations affect not just compliance levels but the quality and sustainability of compliance practices.

This research seeks to close that gap by investigating how compliance challenges are experienced and managed across organizational contexts.

Institutional Enforcement and the Role of Regulators

Despite the legislative framework, enforcement remains a persistent weakness. Veiga et al. (2024) argue that the Information Regulator's limited capacity constrains its ability to ensure compliance. The absence of stringent penalties or proactive monitoring mechanisms allows organisations, particularly smaller ones, to delay or avoid full compliance. The study highlights that while the work of the Information Regulator plays a significant role in ensuring compliance, stricter guidelines and an effective mechanism of enforcement must be ensured for overall compliance (Veiga, et al., 2024).

This gap in institutional effectiveness calls into question the sustainability of voluntary compliance and highlights the need for a more aggressive regulatory posture. The current study investigates the role of regulatory bodies from the perspective of organisations, aiming to understand whether and how regulatory presence influences compliance decisions.

Emerging Technologies and Data Privacy - AI as a Disruptor

The rise of artificial intelligence (AI) introduces new complexities into the domain of data privacy. Sebastian et al. (2022) examine how AI systems, while offering advanced data processing capabilities, pose novel threats to privacy through algorithmic opacity and evolving threat vectors. Their study underscores the tension between maximising data utility and ensuring individual privacy, a balance that POPIA does not yet fully address. The study also discusses the regulatory and ethical considerations of using AI for privacy protection, noting that AI technologies themselves could generate new privacy risks that must be managed in conjunction with the design of privacy-enhancing technologies (Sebastian, Bernhard, & Jochen, 2022).

Mbonye, Moodley, and Nyika (2024) explore the extent to which South Africa's Protection of Personal Information Act (POPIA) addresses emerging privacy and ethical concerns associated with the growing integration of Artificial Intelligence (AI) in various economic sectors. Their study recognises that while POPIA provides a foundational legal framework for data protection, it was designed within a regulatory paradigm that predates the widespread integration of intelligent, autonomous systems capable of processing, learning from, and repurposing personal data in opaque ways. It further highlights that AI technologies often circumvent conventional data governance models by introducing layers of complexity that challenge core POPIA requirements like informed consent and purpose specification (Mbonye, Moodley, & Nyika, 2024).

Although the above studies present a strong conceptual foundation, they lack empirical grounding in how organisations manage AI-related privacy risks. Additionally, policy responses to AI threats remain underdeveloped, with current regulatory approaches lagging behind technological innovation.

This research contributes by investigating how organisations perceive and adapt to emerging technological risks and by identifying the policy blind spots in South Africa's data protection regime.

POPIA Awareness and Legal Consciousness

The Information Regulator (2023) report on the public opinion survey affirm that a large proportion of the South African public is still not aware of the Regulator and its role. 25% of the participants were reported as unaware of the IR and 28% were unaware of its roles and responsibilities (HSRC, 2023). These figures refer to an alarming communication gap between the regulator and the citizens. The report also observed that awareness of the Regulator was notably greater among individuals aged 18-19, as well as among females, those with tertiary education, employed individuals, and citizens from higher socioeconomic backgrounds. This highlights the persistent impact of gender, age, education, and class characteristics in influencing the levels of awareness and understanding of information laws and their regulation. A summary of the results is depicted in Figure 8 below (HSRC, 2023).

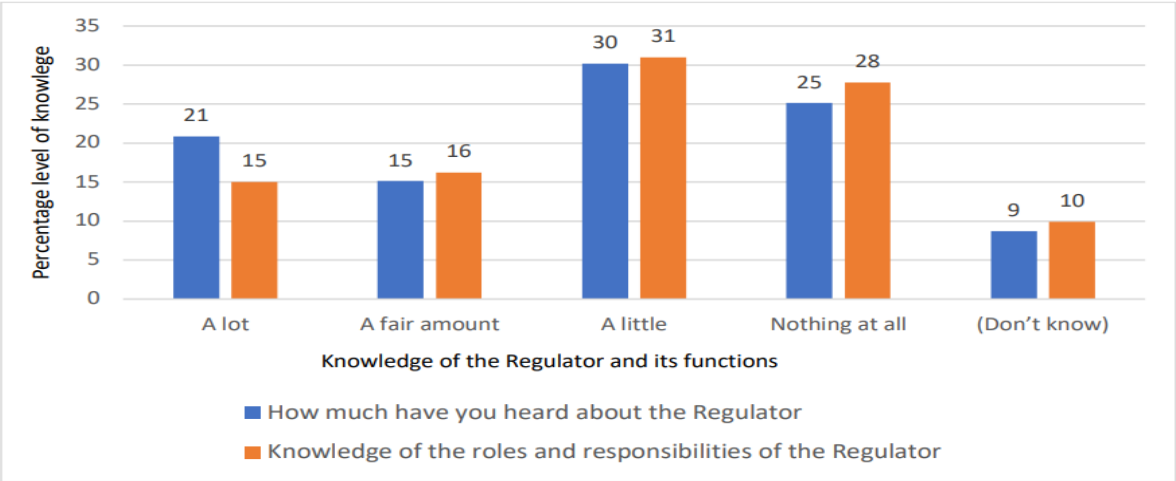


Figure 8. Awareness of the Regulator Survey. Source: (HSRC, 2023)

Netshakhuma (2019) presents a critical case study evaluating South African universities' preparedness for implementing the Protection of Personal Information Act (POPIA), with a focus on awareness, collaboration, information integrity, and international compliance. Through national consultative workshops, the study explores institutional efforts to formulate a sector-wide code of conduct aimed at aligning university practices with POPIA's legal mandates. The study reveals that while 80% of university representatives acknowledged awareness of POPIA as a regulatory tool,

this awareness was often superficial and lacking in operational clarity (Nkholedzeni, 2020).

However, despite their usefulness, these workshops had not yet permeated all administrative layers within universities, and implementation of training remained fragmented. A major finding of the study is the critical lack of collaboration between legal practitioners, records managers, and ICT departments, key actors in ensuring POPIA compliance (Nkholedzeni, 2020). Additionally, the study also finds that there was a major disconnect between legal, ICT, and records management departments. This siloed approach undermines effective POPIA compliance and weakens institutional governance over personal information. The study warns that South African universities may face reputational and operational risks in global partnerships due to weak alignment with international data protection laws, particularly the GDPR (Nkholedzeni, 2020).

While Netshakhuma (2019) makes a strong case for aligning POPIA with global data protection norms, there is little discussion of operational models or institutional readiness assessments that could assist universities in navigating complex international data flows. Furthermore, while the workshops are praised for raising awareness, there is no impact evaluation framework to assess what institutional changes (policies, training, systems) resulted from them.

2.6 Analytical Framework

Conceptual Framework of this research combines some of the key components to assess the effectiveness of South Africa's Information Regulator in implementing the POPI Act against the backdrop of rapidly evolving Fourth Industrial Revolution (4IR) technologies. The framework discusses the disruptive impact on data protection and privacy procedures in the Data Economy spaces. The digital technology such as AI and emerging Generative AI introduces new dimensions of data processing, storing and analysing, which largely challenge data governance.

The structure involves a critical analysis of South Africa's Information Regulator and its regulatory role within the implementation of POPIA. This section will assess the regulatory structures in place, the effectiveness of enforcement mechanisms and challenges experienced in the realisation of data protection law. The capacity of the Information Regulator to innovate with emerging technologies and novel risks arising with AI will be subject to critical analysis.

2.6.1 Conceptual Framework

The framework illustrates how, within the evolving data economy, the interplay between technological advancements, regulatory frameworks and policy implementation and enforcement impacts the effective management of data. Central to this framework is the role of the Information Regulator, which is tasked with ensuring compliance with monitoring and enforcing the POPI Act. This includes overseeing how organisations adhere to data protection, privacy, and consumer rights policies, thereby facilitating the effective management and protection of data amidst rapid advancements in 4IR technologies, including Artificial Intelligence.

The Information Regulator plays an intrinsic role in monitoring, compliance, and enforcement of data protection laws. This includes amongst others:

- Monitoring - Ensuring that Organisations adhere to data protection standards.
- Compliance - Enforcing compliance with POPIA and other relevant regulations.
- Enforcement - Taking corrective actions against non-compliance and breaches of data protection laws.

Selected aspects of POPIA are highlighted in the framework, focusing on Privacy, highlighting the need to ensure the privacy of individuals' personal information from unauthorised access and misuse. Protection indicates the importance of required measures and controls to safeguard data against breaches and cyber threats or potential risk exposure. Consumer Rights to ensure that consumers' rights to data privacy and protection are upheld. Ethics focuses on promoting the ethical use of data and AI technologies to prevent misuse and harm.

Forth Industrial Revolution Technologies, this component focuses on the selected technological advancements driving the Fourth Industrial Revolution relevant to this study:

- AI (Generative AI) outlines the role of artificial intelligence in transforming data governance practices. The increasing influence of generative AI on data generation, analysis and decision-making processes raises important issues regarding data authenticity, privacy and ethical considerations. Generative AI is being used by Organisations not just for answering queries and producing documents but also for experimenting with image manipulation, composing music and synthesising voices (Xia, Weng, Ouyang, Lin, & Chiu, 2024).
- Data Analytics indicates the application of analytical techniques to extract meaningful insights from data. Data experts employ a variety of methods and techniques, depending on the nature of the data and the insights sought. The use of data analytics should be guided by ethical considerations. If the data used in analytics is biased, the insights and decisions based on it will also be biased. This can lead to unfair outcomes and discrimination. Misuse of data or insights can lead to ethical dilemmas and potential backlash (Sarker, 2021).

Organisational Impact focuses on several critical components that collectively determine how effectively an organisation manages and leverages data within the context of evolving regulatory and technological landscapes. The conceptual framework is depicted in Figure 9 below.

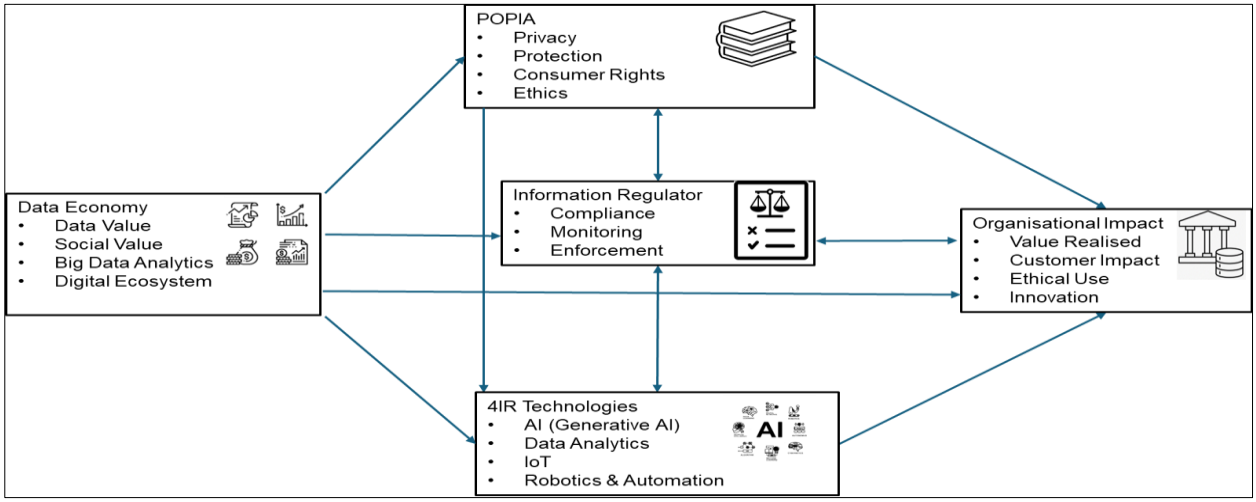


Figure 9. Research Conceptual Framework. Adapted from (Ndemo & Mkalama, 2023)

2.7 Conclusion

This chapter provided a critical examination of the theoretical and empirical literature that underpins this study. Drawing on foundational theories such as the Information Society Theory, Public Interest Theory of Regulation, and the DAMA Data Governance Framework, the literature review established the conceptual and standardising grounding for exploring the regulatory effectiveness of POPIA in a rapidly digitising economy. The chapter revealed that although POPIA aligns with global data protection principles, it faces serious challenges in enforcement, awareness, sectoral readiness, and adaptation to emerging technologies such as AI.

Empirical literature further highlighted significant disparities in compliance between large firms and SMEs, as well as a lack of institutional capacity within the Information Regulator. Moreover, emerging technologies, particularly AI introduce complex, opaque, and evolving data risks that current regulatory mechanisms struggle to manage effectively.

These findings confirm the necessity of this study's focus on assessing the Information Regulator's ability to enforce POPIA in the face of technological disruption and organisational limitations.

3. CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter presents the research methodology, including the research strategy and design implemented in the study. It outlines the data collection methods, specifying the targeted participants for the research interviews and the research tools utilised. Additionally, the chapter details the data analysis and interpretation techniques, the research approach, and the timeframe of the study. Ethical considerations are addressed at the end of the chapter.

3.1.1 Ontology and Epistemology

According to Saunders et al. (2011, as cited in Ndamase, 2014) ontology explores the nature of reality and existence, examining how entities are perceived and understood. Two primary ontological perspectives are objectivism and subjectivism. Objectivism posits that social entities exist independently of the perceptions and actions of individuals, maintaining an external reality separate from social actors (Ndamase, 2014). In contrast, subjectivism by other researchers such as Cavana et al. (2001, as cited in Ndamase, 2014) suggests that reality is socially constructed through individuals' perceptions and actions, with social phenomena emerging as a product of these interactions (Ndamase, 2014).

Goertz and Mahoney (2012) also point out that ontology in qualitative research involves exploring the nature of social phenomena and the assumptions made by researchers about the existence and nature of social entities. This involves exploring how reality is experienced and constructed through people's lived experiences and meanings (Goertz & Mahoney, 2012).

The ontology of this study focuses on assessing the role of the Information Regulator in the evolving digital technologies and their impact on data privacy and protection. It acknowledges the existence of objective realities related to data governance practices

while recognising the subjective interpretations and constructions of these realities by various stakeholders, including policymakers, regulators, businesses, and consumers. The study adopts a social constructivist approach, assuming that reality is socially constructed, particularly in the context of evaluating the effectiveness of South Africa's Information Regulator in enforcing the POPI Act.

Goertz and Mahoney (2012) explain that epistemology in qualitative research examines the nature and scope of knowledge, focusing on how reality is understood and interpreted. Highlighting how knowledge is constructed through the research process (Goertz & Mahoney, 2012). In this study, epistemology addresses how insights were derived from the collected, which involved recorded interviews and the analysis of existing evidence to assess the effectiveness of South Africa's Information Regulator in implementing POPIA amidst the evolving 4IR technologies. It considers the methods used for data collection and interpret data, the sources of knowledge and the criteria for assessing the validity and reliability of the research findings.

3.2 Research Approach

This study employed qualitative research. Leavy (2020) has described qualitative research as a research approach seeking to describe social phenomena in their natural settings, making sense of, or interpreting, phenomena in terms of the meanings that people bring to them (Leavy, 2020). It makes use of descriptive, non-numerical data, e.g., observations of behaviour or descriptions of experiences given by people. As the American Psychological Association (2018) and Leavy (2020) have already noted, such an approach provides rich information concerning the experiences and perceptions of individuals and is most valuable for looking at the multifaceted influence of AI technology on data privacy, consumers, and compliance with data protection regimes, as it captures the nuances of these exchanges and challenges (American Psychological Association, 2018).

With its rich tradition in studying human social behaviour and cultures, this research method aligns well with the current study, offering an in-depth understanding. It

provided the interview participants with a platform to express their views and perceptions regarding the role and effectiveness of the Information Regulator in implementing data regulation policies. Agius (2013) supports this view noting that qualitative methods give participants a voice to share their insights, which is important for exploring subjective experiences and opinions about regulatory practices and data protection issues (Agius, 2013).

Given the intricate and evolving nature of Generative AI technologies and their impact on data privacy and POPIA compliance, a qualitative approach allows for a nuanced exploration of how these technologies are perceived and experienced by different stakeholders. This is further supported by argument by Creswell and Poth (2007) that qualitative methods, such as semi-structured interviews and document analysis, are ideal for capturing nuanced views and detailed insights into how individuals and groups experience and interpret social phenomena. They highlight that qualitative approaches enable researchers to delve deeply into the contextual factors and personal perspectives that influence compliance and regulatory practices, thus providing a rich, contextual understanding essential for addressing the research questions (Creswell & Poth, 2007).

3.3 Research Design

Khanday and Khanam (2023) define research design as a systematic and structured plan that guides the collection, analysis, and interpretation of data to reliably answer research questions. Its effectiveness is measured by its capacity to generate insights that are valid, reliable, and relevant. Furthermore, a research design is asserted to be a logical and methodical plan formulated to guide a research study (Khanday & Khanam, 2023). Other researchers' definitions, as noted by Akhtar (2016), define research design as the cohesive platform that keeps all aspects of a research project together, serving as a plan for the proposed work. It is coordinating conditions for data collection and analysis, with an eye to marrying relevance to the research purpose with procedural thrift (Akhtar, 2016).

This strategy provides the ability to ask in-depth into participants' responses and monitor principal research questions. This is suitable for this project because it provides the opportunity to probe deeply into responses and the identification of new emerging findings.

To operationalise this design, the study employed a qualitative multi-method approach, combining interviews with document analysis to capture both the personal experiences of individuals and the objective features of regulatory and policy frameworks. This mixed-method strategy aligns with the goal of delivering a comprehensive understanding of the study while underpinning key findings and recommendations. Analysing policy documents, regulatory guidelines, and other pertinent materials yielded further insights into the current landscape of data governance and privacy laws. It also examined the legal and ethical structures surrounding AI and data privacy, including principles of ethics, fairness, accountability, and transparency. Khanday and Khanam (2023) argue that an effective research design integrates multiple components to reliably address research inquiries.

The data was analysed using inductive thematic analysis, which facilitate the identification of emerging themes, patterns, and concepts related to compliance mechanisms, institutional capacity, and policy effectiveness. This analytic approach is aligned with the study’s aim of generating grounded insights that inform both theoretical understanding and practical recommendations.

3.4 Research Strategy

In Johannesson and Perjons study (2021), research strategy is described as a master plan for conducting a research study. It is a methodical approach to resolving the research issues in a way that guarantees that every step taken aligns with the general objective of the study (Johannesson & Perjons, 2021).

The research design, therefore, plays a primary function of enhancing the validity and reliability of the research findings. It ensures that the research process is not only methodological and consistent, but also open and reproducible, and consequently

contributes to the study's integrity and strength. The methodology used involved a comprehensive review of literature existing on the implementation of data protection and privacy safeguards, AI-related risks, and how the South African Information Regulator has ensured compliance with data regulation policy.

The study's primary data was collected using qualitative approaches, including interviews with field experts and an examination of specific cases that breached the policy, along with the regulator's responses. The data underwent inductive thematic analysis to identify and explore recurring patterns, codes, categories, or themes. To enhance the findings' validity and reliability, the research design incorporated rigorous validation techniques, such as triangulation, which involved using multiple methods or sources to cross-verify the results.

3.5 Data Collection Methods

The collection of data was done using virtual platforms interviews. The interviews were conducted using the Microsoft Teams platform and Google Meet application with the identified participants from different sectors of society and industry experts as part of a qualitative data collection method.

Each interview was scheduled to last for one hour. Microsoft Teams and Google meet platforms were utilised to conduct interviews. Primary data was supplemented with relevant secondary data, sourced from research readings, published company reports, independent article reports and publicly available policy documents. Specific keywords were used to search from selected academic database sources and research journals such as ScienceDirect, SAGE Journals and SpringerLink. In addition, other research scholar search engines like Google Scholar were utilised.

3.6 Population and Sample

A total of fourteen (14) interviews were conducted across a diverse range of sectors and organisations, including regulatory bodies, government departments, private

sector institutions, legal experts, data privacy practitioners, and civil society organisations. This diversity was crucial to ensure a well-rounded understanding of how the Protection of Personal Information Act (POPIA) is enforced, interpreted, and experienced in practice—particularly in the context of emerging technologies such as Artificial Intelligence (AI).

Purposive Sampling, a method commonly used in qualitative research, was employed for participant recruitment in this study. This approach entails purposefully choosing participants with expertise offering rich and pertinent information related to the research goals so that the information gathered is rich and useful for in-depth analysis (Omona, 2013). By targeting individuals who are most knowledgeable or experienced in the subject area, purposive sampling enhances the quality and depth of the information obtained. Detailed job descriptions of participants are presented in Appendix A.

The sample size of fourteen (14) was deemed sufficient based on the principle of data saturation, where no new themes or significant insights emerged from additional interviews. This further supports the adequacy of the selected sample in achieving the research objectives. Moreover, the variation in participants' organisational roles and institutional affiliations enabled a triangulated and multi-perspective understanding of the topic under investigation.

3.7 Data analysis and interpretation

This study followed an Inductive Thematic Analysis of the data to unpack the complexities and nuances of data governance in the era of Artificial Intelligence (AI) from the perspective of industry experts and involved key stakeholders. Thematic analysis is a widely adopted method for analysing qualitative data, which identifies recurring patterns within raw data and organises them into coherent themes that convey meaning (Campbell et al., 2021, as cited in Thompson, 2022). Braun and Clarke (2017) describe thematic analysis functions as a technique for recognising, examining, and understanding key patterns in qualitative data. They argued that by

employing thematic analysis, researchers can reveal patterns in data that represent individuals' lived experiences, viewpoints, attitudes, and behaviours (Clarke & Braun, 2017). Paoli (2024) defines inductive analysis as a data-centric approach that enables themes to arise organically instead of being dictated by existing theoretical frameworks. This method of analysis improves the reliability of research findings by confirming that concepts are connected to the data (Paoli, 2024).

Vears & Gillam (2022) define inductive analysis as an iterative coding approach that involves several coding cycles and recurrent analysis and refinement of data. This ongoing improvement improves the analysis's precision and comprehensiveness (Vears & Gillam, 2022). This approach aligns with the approach followed in this research study.

ATLAS.ti v25 was used as a supporting tool for data analysis and coding. Smit and Scherman (2021) state that ATLAS.ti provides a structured approach to qualitative data analysis, enhancing the efficiency of coding, organisation and data visualisation, thereby improving the overall quality and credibility of research findings (Smit & Scherman, 2021).

3.8 Research Instrument

The research instrument explains the tool that was used in the gathering of relevant data for this study. Data gathering was conducted using semi-structured interviews via online (virtual) platforms. It enabled the research to be able to capture the depth and richness of the experiences and perceptions of the participants regarding the topic of study, e.g., existing gaps and issues in both the data protection legislation and policy implementation and adherence. It also allowed for probing and follow-up questions and responses from participants, providing the opportunity to investigate further into the issues.

3.9 Validity and Reliability

To ensure the reliability and validity of this study, a comprehensive approach was adopted. The research approach involved a carefully designed interview process, where participants were selected through purposive sampling. As Silverman (2004) highlights, purposive selection is crucial for the acceptability and relevance of qualitative research findings, as it targets individuals who are most knowledgeable about the research topics (Silverman, 2004). Schwandt (2007) situates the concepts of validity and reliability within the broader philosophical discourse on justifying interpretations in qualitative research. He highlights that, qualitative inquiry requires different criteria to assess rigor due to its interpretive nature. Lincoln & Guba (1986, as cited in Schwandt, 2007) introduced four key criteria to ensure the trustworthiness of the study: credibility, transferability, dependability and confirmability (Schwandt, 2007).

3.9.1 Credibility

To ensure that findings accurately represent participants' experiences, all participants were briefed before the start of the interview and given the option to decline participation into the study or choosing not to answer questions they are not comfortable to answer; ensuring data collection was from genuinely willing individuals.

3.9.2 Transferability

Transferability in this study was ensured by outlining the number of participants involved, data collection methods utilised, the quantity and duration of data collection sessions, which included regular reviews and alignment with the supervisor for guidance, the period over which data was collected. Furthermore, transferability was facilitated by providing thick descriptions that enable others to assess whether the study's context aligns with their own Lincoln & Guba (1986, as cited in Schwandt, 2007) (Schwandt, 2007).

3.9.3 Dependability

To ensure the repeatability and consistency of study findings, Lincoln and Guba (1986, as cited in Schwandt, 2007) suggest maintaining an audit trail to document methodological decisions and ensure transparency (Schwandt, 2007). A systematic and well-structured approach to participant selection, interview execution, data analysis and findings presentation was essential to maintaining consistency and reliability in this study. Ensuring dependability required meticulous planning at each stage, from developing a research calendar tracker with detailed activity task and milestones with specific target dates, recruiting suitable participants to conducting thorough and unbiased interviews. By maintaining consistency in data collection and interpretation, the research findings remain trustworthy and reproducible within similar contexts.

3.9.4 Confirmability

Confirmability guarantees that the findings of this study truly represent the viewpoints and lived experiences of the participants. To improve confirmability, Lincoln and Guba (1986, as cited in Schwandt, 2007) suggest techniques like reflexivity and maintaining audit trails (Schwandt, 2007). The findings accurately represent the experiences and observations of the participants. The data from recorded interviews were transcribed, coded in Atls.ti software and the findings presented without bias, misrepresentation, or omission of key insights.

3.10 Limitations of the study

The following limitations were recognised prior to commencing the research study:

- While the sample size may limit the generalisability of the findings, it provides valuable insights into the subject matter and serves as a foundation for further investigation.

- Access to large data and the relevant documents may be restricted by confidentiality or ongoing court hearings.
- The study's reliance on interviewees' honesty and openness may introduce biases, as participants might withhold information.
- The focus on specific sectors and organisations may result in insights that are not fully generalisable across all sectors or the broader South African context.

3.11 Ethical Considerations

All the ethical guidelines laid down by the University of the Witwatersrand were adhered to in letter and spirit. This includes obtaining clearance approval from the ethics committee of the university before gathering data (ethics protocol number: WBS/DB1488581/631). The ethics clearance certificate is shown in Appendix B. Informed consents were taken from all the subjects through an official consent letter clearly laying down the purpose of the study, the manner in which their data was going to be utilized and the steps taken to maintain their privacy. The letter also specified data handling procedures and made provision for all the data to be stored securely and eventually destroyed. Participants were informed of their right not to respond to questions they do not want to respond to.

3.12 Conclusion

This chapter outlined the research methodology employed in the study, highlighting the ontological and epistemological underpinnings, qualitative approach, and social constructivist framework. Semi-structured interviews and document analysis were used to explore the Information Regulator's role in the context of AI and data governance. A purposive sampling strategy ensured a diverse and relevant participant pool, while inductive thematic analysis using ATLAS.ti facilitated systematic data interpretation. Trustworthiness was ensured through credibility, transferability, dependability, and confirmability. The chapter also addressed key limitations and ethical considerations, establishing a solid foundation for the study's findings.

4. CHAPTER 4: PRESENTATION OF DATA

4.1 Introduction

This chapter presents the findings of the study employing the use of visual graphs, tables and verbatim responses from the interviewees. A detailed breakdown of the participants' demographic is presented in Table 4 under section 4.2 Demographics Data.

4.2 Demographics Data

Fourteen (14) interviews were successfully conducted and recorded with participants. Of the 19 individuals initially invited, two declined, citing a lack of expertise on the subject and concerns about their relationship with the South African Information Regulator. Another participant withdrew due to capacity challenges arising from recent personnel changes. Additionally, two individuals who initially expressed interest did not respond to subsequent email invitations.

The demographic profile of the respondents provides crucial insights into the study's exploration of data governance in the AI era and the effectiveness of the Information Regulator in enforcing POPIA regulation. The participants in the interview include an equal split of 50% female and 50% male, representing a balanced gender split. This balanced representation reflects global trends where women are progressively assuming leadership positions in governance, legal matters, and the data sector overall.

The study involved participants such as department heads, policy compliance officers, policy makers, legal professionals, data governance industry specialists, and academics, who represent a diverse range of roles and senior management level. The participation of legal and compliance experts provides a comprehensive regulatory perspective as well as in-depth knowledge of the challenges associated with implementing POPIA, its legal loopholes, and enforcement tactics. The perspectives

of Chief Data Officer (CDO) and industry experts provide real-world operational challenges, which include the preparedness of organisations for implementing micro-level data governance, and compliance practices in businesses. Additionally, academics and researchers add valuable theoretical and policy-oriented viewpoints to enhance the research, facilitating a comparison of South Africa's data regulations with global best practices.

Participants were from a variety of sectors, including banks, consulting businesses, regulatory bodies, and academic organisations. Officials from the Information Regulator are included to ensure that viewpoints from those who are directly involved in enforcement and policy-making have been taken into account. Inputs from other government regulators provide important insight into the existing legislative and bureaucratic obstacles in these institutions. While the financial sector participants offer insights into overall risk management and compliance challenges and cost implications. Expertise on emerging risks associated with AI and the changing environment of compliance readiness were provided by industry consultants. Table 3 presents the demographic breakdown of the 14 successfully recorded participant interviews. Further details on participants job descriptions are presented in Appendix A.

Table 3 Breakdown of Participants Demographics

Participants	Gender	Job Role/Level	Sector	Size of Sector
Participant 1	Female	POPIA SME compliance officer	Banking/Financial Sector	Medium
Participant 2	Female	Training Manager	Government Regulator	Medium
Participant 3	Male	Head of Data Governance and Management	Banking/Financial Sector	Large
Participant 4	Male	Manager Information Technology	Government Regulator	Medium
Participant 5	Female	Policies Developer	Government Regulator	Large
Participant 6	Female	Manager Policy Development Officer	Government Regulator	Medium
Participant 7	Female	Professor of Political Science	Academic Institution	Large

Participant 8	Female	Data Privacy and Compliance Expert (Industry expert and consultant)	Consultancy Agency	Small
Participant 9	Male	Attorney - Data Protection, Data Governance, AI Privacy Governance expert	Legal and Consultant Firm	Small
Participant 10	Male	Chief Data Officer (CDO) - data governance and policies and procedures around data management	Data Governance Consultant Company	Small
Participant 11	Female	Attorney (Analyst) – Digital Policy and Regulations	Consultancy Firm	Small
Participant 12	Male	Information Privacy officer	Government Regulator	Medium
Participant 13	Male	Managing Attorney	Legal and Consultant Firm	Small
Participant 14	Male	Professor – Teaching and Research	Academic Institution	Large

4.3 **Analysis Process**

The coding process started with verbatim transcription of the interview recordings and checking the accuracy of transcripts, where necessary, formatting was limited to excessive word repetitions in the same line or filler words. The identified codes were grouped into broader categories aligned with the study's research questions and the core issues discussed by participants. The categorisation process involved a comparative analysis of responses, merging overlapping topics and eliminating redundant codes.

The thematic analysis process resulted in the identification of:

- Nineteen (19) distinct codes, capturing key areas, enforcement and compliance challenges, data subjects' awareness, collaborations, opportunities or areas of improvement and perspectives on data privacy, protection and emerging technology impact and consumer impact.
- Eight (8) major categories reflecting regulatory enforcement and challenges, compliance practices, consumer awareness, AI-related risks, collaborations efforts and legal reforms.

4.4 **Presentation of findings**

A Word Cloud was generated with the Atlas.ti software to visually represent the most frequent words, as illustrated in Figure 10. The commonly used phrases identified through the data analysis are distinctly illustrated in this visual depiction, which also provides insights into key themes and recurring ideas. Key concepts vital to the research focus are featured in the Word Cloud, such as "**data**", "**information**", "**regulator**", "**privacy**", "**protection**", "**popia**", "**ai**" and "**governance**."

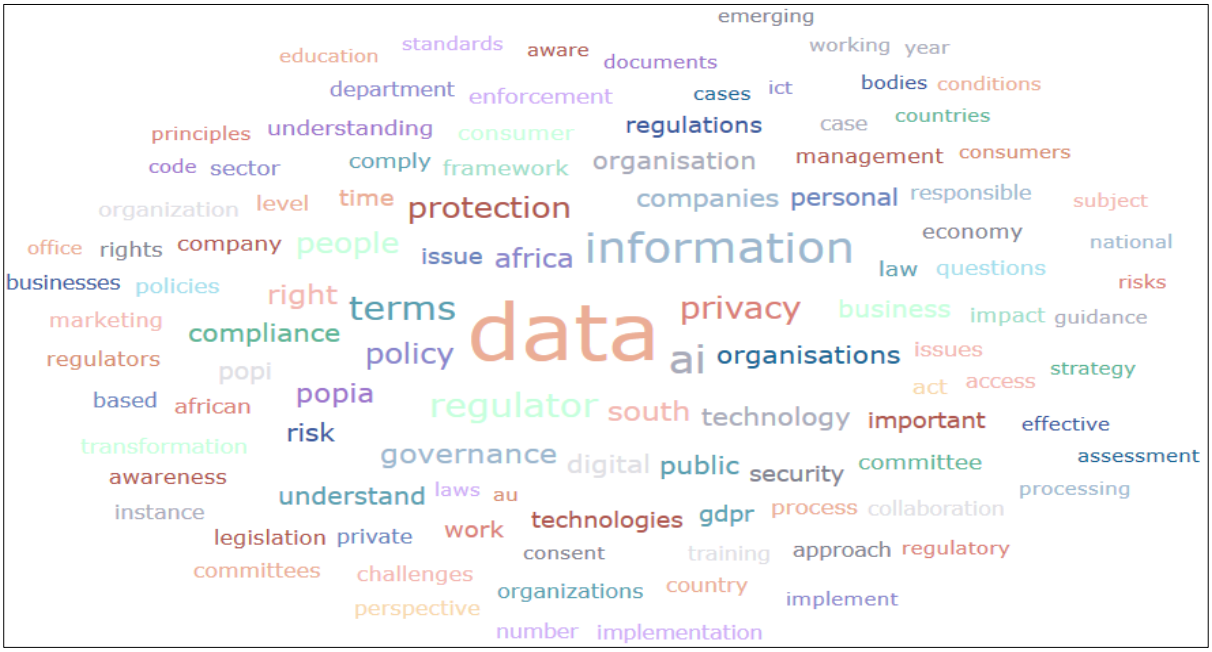


Figure 10. Word Cloud: Study Frequently used words. Source: Atlas.ti Data Analysis

Participants' contribution is presented in Figure 11, summarised based on extracted coded quotations, prepared using Atlas.ti. The distribution of coded quotations among interview participants reflects the breadth of expertise and the depth of engagement in the study, ensuring a well-rounded perspective on the regulatory, operational and theoretical dimensions of data protection. This multi-stakeholder engagement enriches the study's findings, ensuring a comprehensive assessment of Information Regulator's effectiveness, regulatory enforcement challenges and the complexities of AI-driven data governance in South Africa.

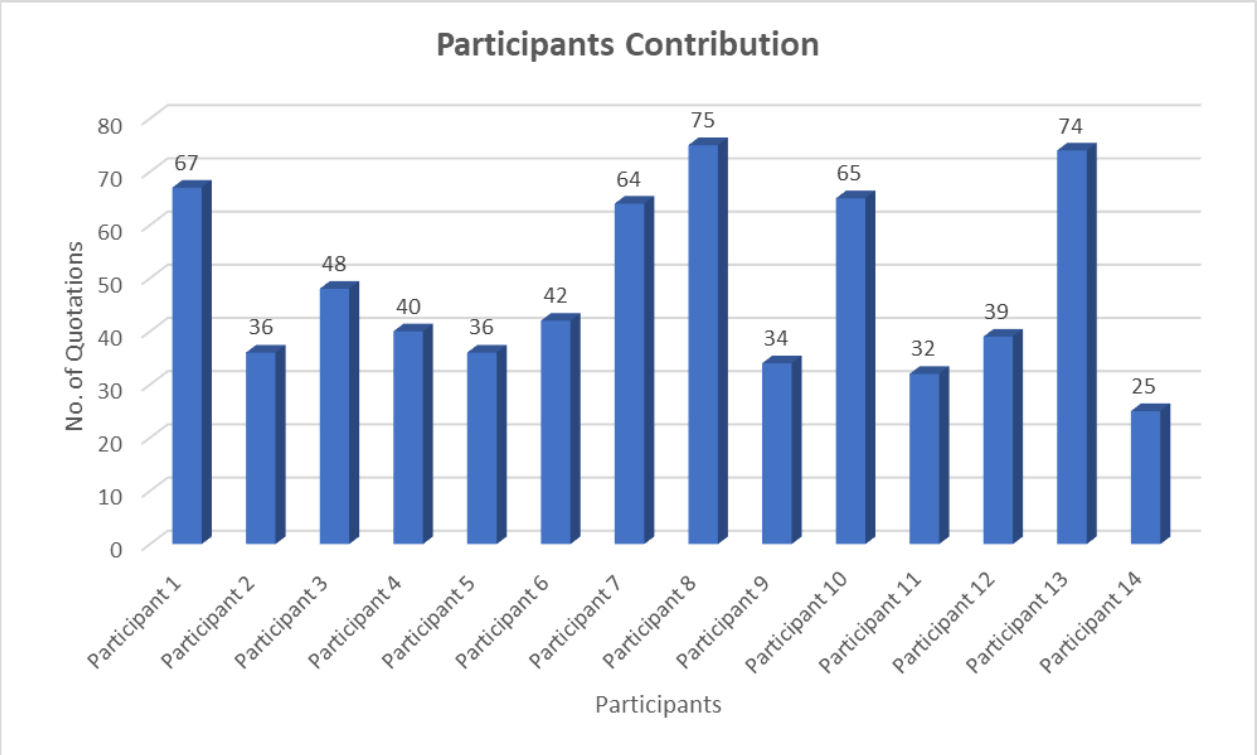


Figure 11. Study Participants Contribution. Source: Atlas.ti Data Analysis

Table 4 below presents a summary of mappings of each research question aligned with the corresponding research proposition, thematic categories and relevant codes to ensure a structured and comprehensive analysis of the data. It details the research questions that guide this study discussion, with its corresponding research propositions that frame the expected conclusions, and the thematic insights extracted from data.

Moreover, selected verbatim quotations from the interviews are included to offer direct insights and enhance understanding of their viewpoints. These quotations highlight the practical challenges, concerns and viewpoints expressed by participants and preserve the authenticity of their perspectives and to provide direct evidence supporting the thematic analysis. Themes and verbatim quotations are comprehensively discussed in the subsequent sections.

Table 4. Mapped Research Questions, Propositions, Themes, Codes and Verbatim

RESEARCH QUESTIONS	RESEARCH PROPOSITION	THEMES	CODES	SELECTED VERBATIM QUOTATION
1. How have POPIA and related data privacy infringement cases been dealt with in South Africa?	Data privacy infringement cases in South Africa have been handled ineffectively.	Handling of POPIA infringement cases	Infringement cases, Contravention, breach	**Participant 7:** "*There's a low compliance culture and the compliance seems to be low, the privacy culture is rather low in South Africa, so there needs to be more efforts in terms of awareness education, in terms of the investigation of those social media and large platforms, the investigation it is still in its infancy and the enforcement limit of 10 millions of South African rands is too little to act as deterrent for big tech if you compare it with GDPR 4% of the total annual turnover of a company."* **Participant 11:** "*In terms of implementation, the IR have issued a lot of enforcement notices. IR have also gone as far as taking cases to court like against the Department of Justice, which ironically is also like the home for the information regulator.*"
2. How effective is the Information Regulator in enforcing	The South African Information Regulator is not fully effective in	Effectiveness of POPIA Enforcement by the	Enforcement delays, Weak penalties, Reactive	**Participant 11:** "*participant definitely see their role and see how effective they are. they are probably one of the few data protection authorities in Africa where we are seeing movement. In a scale of one to 10 and then on that it is based not only on the challenges and the capacities I would place the IR*

POPIA regulations?	enforcing compliance requirements of the POPI Act.	Information Regulator	enforcement, Collaboration	*a solid 5. They're still young and they're still growing, but they have done like very great work and not only within South Africa, but globally. They have also made sure that their voices seen and that as an independent organisation, they have actually*." **Participant 13:** "*The IR have done a lot and they have tried hard. So they have been effective in some ways. But where they and they have worked hard, but where they have failed, in my view is that they have, put emphasis and enforced and taken action relating to the wrong things. So for example, this publishing the "matric" results story, they're much bigger issues that they could have focused on. The IR haven't picked the right issues to take action on. And, then the other major issue is that the regulator doesn't have the ability to issue big fines like in the rest of the world. It can be, it is millions and millions, whereas in South Africa it is up to 10 million Rand. And that is not really a significant stick to many organisations, really the bigger organisations. So that is one of the problems is that the fine is too big and again POPIA needs to be amended*."
3. How effective are POPIA provisions in governing the risks emanating	The current POPIA provisions are inadequate to fully address the rapidly evolving	POPIA provisions adequacy in	Provision, adequacy, emerging technologies	**Participant 8**: "*So in as far as those conditions are concerned, with POPIA in its infancy, they are effective, but sufficiency is a different conversation, especially given the rapid advancement of technology. Regulation in most cases is more reactive than proactive in most cases and also to legislate a law. It really takes time. So in as far as those conditions are concerned, they*

from AI technologies and mitigate data privacy issues?	risks and challenges associated with AI technologies on data privacy.	evolving technologies		*are effective, but given the rapid advancement of technology, they are currently not sufficient. So in that way I believe that there is a strong need for regulation to be the process of reviewing legislation needs to be more fast-paced. And more aligned to the developments within the technological space."* **Participant 1:** "*It is quite a massive task to regulate POPIA in an environment or country like South Africa, where we aren't necessarily a first world country with advanced technology or AI is not necessarily leveraged in every single organisation. So I do think that POPI is a good regulatory framework as a basis. However, it is still, in my opinion, vague in addressing the development of AI in organisations and how to use AI to improve data security measures and ensure.*"
4. What are the challenges emanating from Generative-AI concerning data privacy, protection and consumer	South African consumers face increasing exposure to risks associated with Generative-AI and are vulnerable to	Emerging Technologies (Generative-AI) challenges	Generative AI, Gen-AI, Emerging Technologies, AI, Artificial Intelligence	**Participant 1:** *"I think that the biggest challenge is Privacy violations because there's been a lot of, especially the big companies, the big technology companies in America, like Meta, then it was LinkedIn and things like that way they have very small fine print that consumers aren't necessarily aware that they are consenting to that violates the privacy. So I think the biggest challenge would be ensuring that generative AI doesn't go*

rights in South Africa?	data breaches and misuse.			*against our right to privacy. And also there's a lot of deep fake technology that is being used by generative AI."* **Participant 9:** "*The AI introduces a whole range of challenges, mainly from data breaches, so to expand that a bit more. So we are seeing companies or employees taking emails that contain sensitive personal information and inputting it into these AI systems to generate responses for them. And what they don't understand is that some AI technologies are trained on that data, and that is a data breach.* *AI is now being used to generate or to conduct data breaches as well to improve phishing attempts in companies. So AI provides a whole lot of data issues from a data perspective*"

Eight themes emerged from the data analysis, accompanied by verbatim quotes from participants to support the findings.

4.4.1 *Theme 1: Handling of POPIA infringement cases*

The enforcement of the POPI Act by the Information Regulator is central to ensuring accountability and compliance. Effective enforcement requires timely investigations, meaningful penalties, proactive oversight, and sufficient regulatory capacity. Participant views in this study reflect a general consensus that while the legislative intent of POPIA is sound, the enforcement mechanisms remain inconsistent and, in many cases, insufficient.

Several participants raised concerns about the current penalty framework. Participant 7 argued that having good policy framework on paper is not enough, as implementation of such policies is not easy. "*But the question is always, is it just law in the books or law in practice? So, implementation is not easy, and it is very important."* This view was echoed by Participant 9, who criticised the R10 million cap on fines, arguing that it lacks deterrent power for large corporations: "*The fine itself doesn't have enough teeth. what's 10 million rand to billion-dollar company? the fine needs to change needs to be, which of what companies earn that will give its more teeth and more incentive for companies to comply with POPIA? So that is an area for improvement.*"

Similarly, Participant 12 supported the idea of turnover-based penalties, highlighting the disproportionate impact of static fines: *"The organisations that are more likely not to comply with POPIA are the smaller organisations, 10 million to a smaller organisation is a lot, however, 10 million to a large organisation is basically nothing and they can pay it 5 times over if they wish to do so. These funds should be commensurate to the annual turnover."*

Participant 13 added a structural critique, stating that including the fine amount in the Act itself was limiting: *"The number should never have been in POPIA here, should have been through regulations to enable it to increase with inflation because already 10 million in 2013, now 10 million is a lot less than it was in 2013."*

In contrast, other participants acknowledged some progress made by the Regulator. Participant 6 pointed to enforcement actions taken against the Independent Electoral Commission (IEC), WhatsApp LLC, and the Department of Justice, indicating that enforcement tools are being used. However, they also noted that legal processes are slow and often delay meaningful outcomes: "It is successful in that they did what they were asked to do, legal work takes long." Participant further highlighted that the IEC was issued an Infringement Notice with an administrative fine of R100 000 (RSA Information Regulator, 2024). The IEC complied with the directives (IEC, 2024).

Other similar cases noted include the enforcement notices issued to organisations such as:

- The Department of Basic Education on the publication of Matricular results in the newspapers. The directive required the department to obtain consent for the lawful processing of personal information (RSA Information Regulator, 2024).
- WhatsApp LLC on terms of service and privacy policies for users (data subjects) (IR, 2024).
- The Department of Justice and Constitutional Development for security compromises. The department was issued with thirty-one (31) days Enforcement Notice, however, failed to comply with the enforcement or to exercise its right to appeal the matter in a court of law for adjudication (The Information Regulator of South Africa, 2023).

Participant 7 highlighted successful resolution rates: "*almost 70% of those complaints were resolved*," suggesting incremental improvements in enforcement outcomes.

However, this positive outlook is tempered by broader capacity challenges. As Participant 4 noted, the Regulator operates from a single office in Johannesburg with under 100 staff, which limits its national reach and responsiveness.

Notably, while some participants recognised these enforcement cases as signs of progress, others questioned the Regulator's prioritisation of issues. Participant 13 remarked that the Regulator focused on less significant matters, such as the publication of matric results, instead of addressing more critical systemic issues.

Overall, the findings reveal a nuanced picture, there is broad support for stronger enforcement, but concerns persist regarding the adequacy of current penalties, the pace of legal proceedings, and the strategic focus of enforcement actions. These perspectives highlight the need for more dynamic, context-responsive enforcement tools and a strengthened institutional capacity to ensure POPIA is implemented effectively.

4.4.2 *Theme 2: Effectiveness of POPIA Enforcement by the Information Regulator*

The effectiveness of the Information Regulator is fundamental to the successful fulfilment of its legal mandate. A well-functioning regulatory body serves as the cornerstone for ensuring that POPIA is not only implemented but also enforced consistently and effectively. Participant responses revealed both support for the Regulator's growing presence and concerns about its current capacity and impact.

Several participants acknowledged the Regulator's foundational progress. Participant 11 noted, "*I definitely see their role and see how effective they are probably one of the few data protection authorities in Africa where we are seeing movement.*" Similarly, Participant 7 commended the Regulator's work in resolving a significant portion of complaints, highlighting its credibility "*almost 70% of those complaints were resolved, a very good measure.*" These remarks reflect a perception that the Regulator is building institutional legitimacy and visibility.

Participant 4 argued that in assessing the effectiveness of the regulator needs to be looked at with a consideration of its staff complement and the national community it is meant to serve, *“looking at the numbers of staff that must do this, you'll remember that the information regulator is meant to be an organisation that is accessible nationally, but so far it only has one office that is based in Johannesburg. So, they are still serving the whole country, but they are based in one place and with a staff complement of less than 100.”*

However, this optimism is tempered by concerns around operational capacity and public impact. Participant 4 emphasised the mismatch between the Regulator’s national mandate and its limited infrastructure, stating, “only has one office that is based in Johannesburg, staff complement of less than 100.” Participant 12 supported this perspective by offering broader evaluative criteria: “look at its enforcement actions, awareness and educational efforts, stakeholder engagement, resource allocation”. These insights suggest that effectiveness must be assessed beyond enforcement volume to include stakeholder outreach and institutional growth.

Participants also raised issues regarding the Regulator’s communication and public engagement. Participant 10 expressed frustration with the lack of visible outcomes following data breach reports: “I hear breaches, but I don’t hear reactions.” This sentiment was echoed by Participant 14, who described loopholes being exploited by telemarketers and a lack of perceived action from the Regulator.

Others noted areas for strategic improvement. Participant 13 argued that enforcement efforts were misdirected, stating, “they have put emphasis on the wrong things,” while Participant 8 recommended simplifying enforcement notices for broader public understanding: “they’ll give an enforcement notice, but they won’t give an infographic to explain it.”

These varied views reveal that while the Regulator has established a foundation, concerns remain regarding its strategic focus, public visibility, and operational capacity. The findings suggest that to be fully effective, the Regulator must improve not only its enforcement mechanisms but also its ability to communicate outcomes clearly, allocate resources strategically, and engage more effectively with both the public and industry stakeholders.

4.4.3 *Theme 3: POPIA provisions adequacy in evolving technologies*

The eight conditions for the lawful processing of personal data under POPIA serve as fundamental pillars of South Africa's data protection framework. They ensure that organisations and individuals responsible for data processing comply with the legal requirements of the Act, thereby fostering transparency, enhancing public trust, and promoting ethical data practices across various sectors.

Below is a summarised descriptions of eight conditions for the lawful processing of personal information defined in POPI act:

- **Accountability** – The responsible party must ensure compliance with POPIA when processing personal data.
- **Processing Limitation** – Personal information must be processed lawfully, with consent, and only for a specific purpose.
- **Purpose Specification** – Data must be collected for a clear, legitimate purpose and not used for unrelated reasons.
- **Further Processing Limitation** – Any further processing must align with the original purpose of data collection.
- **Information Quality** – The responsible party must ensure that personal information is accurate, complete, and up to date.
- **Openness** – Data subjects must be informed about the collection and processing of their personal information.

- **Security Safeguards** – Adequate security measures must be in place to protect personal data from loss, damage, or unauthorised access.
- **Data Subject Participation** – Individuals have the right to access, correct, or request deletion of their personal information (RSA Government Gazette, 2013).

Participants acknowledged that POPIA provides a broad, principle-based framework, yet many felt it is not adequately equipped to respond to the challenges posed by rapidly evolving technologies. Participants expressed differing views on the Act's adaptability.

Participant 7 stated, "*POPIA is still a very strong Act, it doesn't tell you what to do, but it gives you principles*," suggesting that its flexibility is a strength. Participant 13 echoed this, noting that the Act's general nature allows it to remain relevant over time.

In contrast, Participant 10 expressed concern that the Act lacks sufficient clarity for emerging risks such as generative AI: "*I do think that the current legislation is not enough... no clear-cut responsibilities*." Similarly, Participant 8 noted the limitations of the Act in relation to AI-driven decision-making. While Participants 7 and 13 recognised POPIA's flexibility and principle-based strength, others such as Participants 8 and 10 argued that the Act is insufficient in addressing the complexities of AI and emerging technologies. This contrast reveals a tension between legal adequacy in principle and regulatory sufficiency in practice.

The findings suggest that while POPIA offers foundational legal protections, additional regulatory instruments or amendments may be needed to address new risks associated with advanced technologies

4.4.4 *Theme 4: Emerging Risks from AI and Generative Technologies*

Artificial Intelligence (AI) and Generative AI technologies rise providing new challenges for data governance, privacy and regulatory compliance. Although AI is a technology that has many of the advantages of automation, predictive analytics and better customer

service, there are also tremendous perils about data privacy, bias and regulatory oversight.

Participants consistently raised concerns about the ethical, legal, and security risks associated with AI and generative technologies. These concerns included data bias, algorithmic discrimination, lack of transparency, and risks of misuse.

Participant 3 warned of emerging bias issues: "*It doesn't give you a real view of the world, it gives you the views of people who had access to these systems*." Participant 12 similarly pointed to data quality and representativeness challenges. Participant 9 shared workplace-specific risks, such as using generative AI for performance evaluations, where the logic and data sources are not fully understood.

While Participant 3 raised broader societal and ethical risks, Participants 9 and 12 focused on implementation-related issues, particularly the lack of transparency in algorithmic decision-making. This divergence illustrates how AI risks are perceived across multiple dimensions, both in practical and ethical terms.

These concerns were echoed by Participant 10, who highlighted a growing gap in regulation for automated processing, "*there are certainly some problems that have put those controls in place and then there are other Large Language Models (LLMS) that haven't put the controls in place."* This was reinforced by Participant 12, who stated: "*the issues arise when data that is used to train these AI models is not collected with explicit consent, leading to concerns about transparency and unauthorised data use. There's also an anonymisation risk. As even anonymised data can be re identified and AI generated content may reveal sensitive information, compromising the privacy. Also vulnerable to cyber-attacks."* Participants agreed that there is insufficient understanding of how these systems operate and a lack of clear guidelines for ethical AI deployment.

Overall, the findings indicate that stakeholders see a pressing need for clearer legal safeguards, stronger transparency measures, and improved regulatory oversight

concerning AI. The risks posed by AI are not only technical but also societal, requiring a coordinated response from policymakers, technologists, and regulators. This highlights that South Africa's data protection framework has large and growing 'gaps' when it comes to emerging risks from AI and generative technologies. The lack of clear AI regulations, the risks of biased AI decision-making and the expansion of AI usage beyond legal coverage all pose serious challenges to data privacy and protection.

4.4.5 *Theme 5*: *Compliance Requirements and Challenges in Data Protection*

Data protection, privacy and compliance and data governance as an umbrella represents the combination of standards as well as administrative methods and operational procedures which ensure secure data management and ethical practices together with legal compliance.

Participants provided varying insights into how public and private organisations approach compliance with POPIA. While some viewed the level of awareness and effort as improving, others emphasised the persistent gap between legal understanding and practical implementation.

Participant 13 explained: *"there's a big gap between POPIA and then practically what you must do to comply. That is been a big gap. And it resulted in people not really knowing what they have to do. There are a lot of small organisations who just can't do what the law says you have to do."* Participant 1 commented that: *"I do think that South African companies do understand POPIA, but I don't think that it is taken the legislation as seriously as compared to FICA with regards to the non-compliance sanctions. I don't think South African companies are implementing POPIA compliance requirements that well compared to the finance sector, I think there's a lot more."*

This sentiment was supported by Participant 5 citing marketing businesses as one example of perpetrators: *" companies in South Africa do not really implement POPIA and*

compliance requirements entire. This companies or businesses that own marketing business or own marketing purposes, they continue to provide personal information about the consumer to call data subject without their consent."

Participant 3 remarked that, "*Compliance is not too bad, but it varies*. *Implementation because it tends to be vast and costly. Then that is when you find a lot of different areas. There are those who are very, very high up there and there are those who are lower.*" suggesting that while some progress has been made, practices remain inconsistent across sectors. Participant 6 highlight varying prospect between private sector and public sector: *"Private sector, it is very encouraging, they are quite compliant from a public sector perspective, we're still finding people that don't even know who the information regulator is."* This assertion is supported by Participant 11: *"private sector organisations, the understanding is quite well because a lot of them from the risk perspective, they invest a lot in education, they invest a lot in upskilling their workforce, including on data privacy and data legislation because they understand what's at stake. The public organisations on the other hand, I am not really quite sure what's the reason behind it. Whether it is lack of capacity, whether it is just unwillingness or certain cultural norms within the organisations that just do not regard POPI as a very important piece of legislation."*

A need to balance between complying with the regulation and business interests was raised by Participant 9. *"As a whole, organisations are trying. They are trying to implement it with while also balancing their own business interests as well. Because I have heard that some organisations feel as if it is too restrictive. And how could they grow because of POPIA poses all these obligations on us."*

Participant 10 pointed to limited organisational resources and expertise as barriers, particularly for small to medium enterprises: *"I don't think 90% of the small organisations understand the level that they need to go to be compliant.* And i*f you go to the regulator and say, please give us the toolkit. It is non-existent and then you have to pay lawyers and people like that."*

Participant 12 concluded with highlighting what could be possible contributing factors and added suggestions on how some of the challenges can be remedied: "*overall large organisations within South Africa generally have a good understanding of POPIA and are making strong efforts to implement compliance measures. However, many smaller organisations still face challenges in fully understanding and adhering to the requirements, often due to, for example, resource constraints in the lack of expertise within their organisations, so there is a growing awareness of the importance of compliance, but full implementation remains a work in progress for many. The role of the information regulator in providing guidance and enforcing compliance, is very key to driving further improvements across all sectors."*

This contrast between awareness and application reflects a broader challenge: understanding the law does not necessarily translate into compliant behaviour. These insights suggest the need for more accessible, sector-specific guidance and capacity-building support, especially for smaller organisations. These responses point to a financial accessibility gap that makes it difficult for businesses to comply with South African data protection laws. Data regulations implementation is becoming a more expensive affair. Many small businesses may not be able to compliant without scalable compliance models with limited financial support, which may lead to a remaining non-compliant and this may put consumer data at risk.

4.4.6 *Theme 6: Consumer Protection and Public Awareness in the Data Economy*

Data protection and privacy in the digital economy are crucial for safeguarding personal information and ensuring that individuals understand their data rights. As companies increasingly utilise consumer data, privacy concerns have intensified. Many consumers remain unaware of how their data is used or how to report violations (Quach, Thaichon, Martin, Weaven, & Palmatier, 2022).

Additionally, organisations often lack transparency in how they collect, store, and share data, leading to a growing sense of distrust among consumers. Even when internal data governance controls are established, they are frequently fragmented, causing project delays and hindering the successful implementation of data management strategies. In the context of South Africa's POPI Act, consumer awareness is essential in helping consumer know their rights and actions to take to prevent data misuse and to ensure accountability for non-compliance.

Participants widely acknowledged the role of public awareness in advancing data protection. However, they differed in their assessment of the Regulator's effectiveness in this area.

Participant 2 highlighted key educational and awareness programme undertaken by regulator: "*the IR is mandated to perform those other function, which is that of providing education, be it whether we do it informally, through our public awareness programmes or formally through training programmes. Section of 14 subsection one paragraph talks to Monitoring and Enforcing compliance through, among others, conducting an assessment. Training Framework helps organisation to understand measures to compliance, what needs to be in place"*

Participant 1 commented on consumer awareness, and it is required to better the situation in educating the data subjects: *"Consumers aren't necessarily aware that they are consenting to that violates the privacy. First, know their rights and then secondly, being aware that they need to also have some form of responsibility on their end"*

These sentiments were also echoed by Participant 4: "*the regulator has conducted or conducts quarterly the communication. These are community meetings all over the country. Areas such as taxi ranks, traditional councils and community halls and partner with local government in those places to ensure that the office gets maximum exposure."*

Participant 6 stated, "*The Regulator has public education programmes... targeting different sectors, The engagement and awareness session is called the "Kopanong/Dikopanong", meaning Meeting and also available in Regulator media pages, social media page.*" highlighting positive outreach efforts. Participant 7 added that awareness campaigns have been conducted through media platforms. Conversely, Participant 5 noted, "*Many people don't even know there's a Regulator*," raising concerns about the visibility and reach of such initiatives.

The second major concern is the perceived lack of adequate education on the risks associated with data protection in digital transactions. This includes issues such as consumers reading the "fine print", the role of Artificial Intelligence in data collection, and the implications of targeted marketing.

Participant 7 highlighted the following while proposing potential solutions to these challenges: *"There can be leaflets or other forms of making consumers aware. And in the digital realm, you always have to click that you have read the privacy conditions, the terms and conditions and things like that, and for many people it is just a nuisance, and they just click it, and they never read it and very often terms and conditions are also very lengthy, difficult to understand. So, some people say it is the biggest lie on the Internet. But of course, it is a form of a legal contract, also with a certain company. These terms and conditions. Other forms of enhancing consumer awareness is a form of education. For instance, in many countries there is the Data Protection Day, which is the 27th of January every year. And there can be didactic forms of going to the schools. Educating students about data protection. Trying to bring it across via games via short videos. So, I think this data, this educational purpose is very important in terms of trainings in the companies and in state agencies.*

This view was also advanced by Participant 5, indicated the insufficiency of the current efforts and a need to improve in the consumer awareness campaign drive: *"Not*

everybody is away of the risk, and anyone can fall into the trap, so my view will be that we need to enhance more consumer awareness"

Similarly, Participant 7 also raised the concerns with the following remark: *"The privacy culture is rather low in South Africa, so there needs to be more efforts in terms of awareness education."* Participant 9 also highlighted the educational responsibility on companies' sides: *"Companies also can do more for their consumers."*

Participant 12 concluded by highlighting the following: "*The major contributing factors that I've observed is basically, inadequate consumer consent and then another one would possibly be the lack of transparency in data use. So, consumers are consumers, customers or clients are often not clearly informed about how their personal data will be used, which ultimately leads to noncompliance with data protection principles*". Recommending translating awareness material into multiple official languages to reach rural and marginalised communities, while Participant 4 suggested more collaboration with civil society and schools.

A lack of digital literacy exacerbates the risks of data breaches and cyber exploitation. Educated consumers are, more active in protecting their data in the sense that they strengthen their passwords, always use two-layer authentication and restrict data sharing with other parties (Morić et al., 2024). The European countries, such as the UK and Germany have already introduced an extensive public education program that ask consumers to know facts about their rights per GDPR. South Africa could adopt similar strategy to enhance awareness of data privacy in the social media campaigns, adopt the use of local vernacular, or grassroots school and tertiary level education.

Low levels of awareness of the Information Regulator's functions can undermine efforts at building a robust data protection culture in South Africa. When a significant portion of the population is unaware of the Information Regulator, it is a weakness whereby data

privacy loopholes can be exploited, particularly in scenarios that engage emerging technologies like Artificial Intelligence (AI) and digital financial services.

This is not a unique problem confined to South Africa. In studies of GDPR implementation in Europe, even in places where the data protection rights are strictly enforced, consumer involvement in enforcing their rights is low (Kuner, 2023). There has been a recognition of strategies through which public awareness campaigns and consumer education programs can bridge this gap (Raab, 2024).

This range of perspectives reveals both recognition of existing initiatives and concern over their limited impact. While awareness efforts have begun, their depth, consistency, and inclusivity remain areas for improvement. Strengthening community-based outreach and tailoring materials to local contexts could enhance public engagement with data protection rights.

4.4.7 Theme 7: Oversight and Compliance

Effective data governance in the age of AI requires robust oversight and well-defined compliance processes. To successfully implement compliance regulations a multifaceted approach is required, with active involvement by key stakeholders, including internal oversight committee and business. The weakness in oversight process impact on effective enforcement of regulations.

Participant 4 highlight efforts the regulator undertakes to conduct oversights: *“The act allows the regulator, on its own initiative to conduct compliance assessment on responsible parties to ensure that they comply with the conditions of lawful processing. Also allow responsible parties to request self-assessment from the regulator.”*

Participant 15 emphasised the following on the data governance role at a micro-organisational level: *“Data Governance is about the providing of the oversight or the control or the monitoring and reinforcement.”*

The key role played by organisations' internal oversight committees such as ICT, audit and risk governance were highlighted by participants. Participant 8 explained: *"So, until you get IT steering committee or an audit and risk committee who understands digital marketing and who imposes policy and compliance obligations on the marketing offices, you're not going to see good privacy management. Every IT committee and risk committee in South Africa should be able to get the correct nuances of the act from the regulator."*

Participant 12 expanded on this by stating: *"I believe that it is quite crucial for modern companies, as these committees ensure focused oversight on technology risk, cybersecurity, data privacy and alignment with business goals. Effective ICT governance involves proactive risk management, continuous monitoring of trends and regular board level engagement. However, challenges such as the lack of technical expertise and resource allocation need to be addressed for the successful execution thereof. So ultimately, these committees are vital."*

Participant 14 added: "*The Information Communication Technology Governance (ICTG) committee are very important. And where they exist, they play in an important function in line with the King Four Code in ensuring that technology and this governance is put in the centre of that place, so without those governance committees on ICT issues, it would be difficult."*

4.4.8 Theme 8: Stakeholder engagement and collaboration

Stakeholder cooperation and participation are necessary to make regulatory governance and compliance efficient and sustainable. Active participation of all the significant stakeholders such as regulatory agencies, business corporations, technology creators, and members of civil society enhances compliance. Cooperation fosters a shared understanding of regulatory objectives, enhances transparency, and facilitates harmonisation of stakeholders' interests with compliance requirements.

Participant 8 stated the following on the current collaboration efforts between Information Regulator and other organisations: *“The collaboration between regulatory and other organisations in public or public private, I think it is pretty good. I mean we have seen early days collaboration between the direct marketing association and the regulator.”*

Participant 1 also agreed: *“more collaboration is needed between the* regulator and businesses.” Participant 4 referred to the newly established regulators' forum, through which the key stakeholders of the various regulatory bodies meet to collaborate and align on regulatory developments and issues of mutual concern with a view to resolving them. The forum is to foster cooperation, promote concerted action, and prevent overlaps and duplication of regulatory activities. “*Recently, the regulator announced its partnership and its participation in the Regulators Forum, with the Independent Communication Authority of South Africa (ICASA), the Film and Publication Board (FPB) and the Domain Name Authority (ZADNA). That collaboration is on information and communication technologies and emerging technologies.*”

This sentiment was also echoed by Participant 12, highlighting the importance of regional collaboration beyond South African boarders: *“I believe that this collaboration between the different entities is essential for enhancing data protection standards and key areas of collaboration could possibly include cross-border cooperation whereas. They align standards globally and they conduct a joint investigation, and they share best practises to address cross-border data in the data privacy issues.”*

Participant 14 elaborated further on the importance of working together stating the following: *“Absolutely paramount that there is collaboration between the regulator and sister entities. The departments that it is located in the broader government departments, but most importantly, the players in the public sector, because those are the players that enable us. Partner with those to ensure that the one that is awareness but two there is feedback mechanism on where there are shortcomings on the acts that needs to be tightened up and ensure that there is proper use and proper governance.”*

In addition, the participants explained the imperative of African data sovereignty, citing the danger of African data being exploited by multinational technology firms. As a counter, it was suggested that a combined strategy be undertaken where South Africa and other African states could better negotiate with global tech players if they were to appear as one in front of these entities. Such cooperation was argued to be key in terms of promoting stronger data governance processes and African agency on the world's digital stage.

The study emphasises the necessity of stakeholder cooperation and involvement in facilitating regulatory governance and adherence to data protection laws such as POPIA. Effective cooperation among regulatory agencies, businesses, technology developers, and civil society results in a mutual understanding of compliance objectives, increases transparency, and harmonises disparate interests. Nonetheless, the research also discloses that although some improvement has been made, greater collaboration is required, especially between the business sector and the Information Regulator, to establish a solid compliance culture.

5. CHAPTER 5: DISCUSSION

5.1 Introduction

This chapter present a discussion of the study's findings in relation to the four research propositions introduced in Chapters 1 and 2. It critically analyses how the insights gathered from interviews align with the research propositions and address the research questions. The chapter integrates qualitative data from participants with relevant theoretical frameworks and existing literature, highlighting areas of convergence and divergence.

Additional literature is included in this chapter to support and contextualise the discussion of findings. While the primary literature review is presented in Chapter 2, certain themes and insights emerged during data analysis that required further scholarly support to strengthen the interpretation of results. This inclusion enhances analytical depth and ensures alignment with current and relevant academic discourse.

Evaluation of Effectiveness

Effectiveness can be assessed using various measurement methods and indicators. In the context of the Information Regulator (IR), the following indicators were considered:

- Institutional Oversight involves examining the mechanisms in place to facilitate effective governance and accountability within the IR. The key indicators are:
    - The existence of steering mechanisms to guide oversight functions.
    - Existence and operation of oversight committees.
    - Compliance with parliamentary reporting obligations.
    - Audit results as indicators of regulatory performance and responsibility.

- External Assessment - public attitude and stakeholder involvement provide an indication of the IR's external effectiveness. This includes:
    - Awareness and attitudes of participants towards the IR.
    - Effectiveness of feedback mechanisms and the outcomes of external assessments.
- Enforcement Processes extent to which enforcement mechanisms are implemented and institutionalised serves as a measure of effectiveness:
    - Number of successful enforcement actions taken.
    - Fines imposed as a result of non-compliance.

Evaluation of Efficiency (Internal Resources)

Efficiency focuses on the IR's internal capacity to manage its operations effectively, ensuring timely and resource-conscious delivery of its mandate, such as:

- Target Setting and Achievement - assessing whether the IR establishes clear performance targets and the extent to which these targets are met.
- Case Management evaluating the IR’s ability to handle reported incidents efficiently. Key metrics include:
    - Number of incidents reported and successfully resolved.
    - Average time taken to resolve cases, providing insights into procedural efficiency.
- Organisational Capacity - assessing whether the IR possesses the necessary human, financial, and technological resources to fulfill its mandate effectively.

5.2 Discussion of findings related to Proposition 1

Proposition 1: "*Data privacy infringement cases in South Africa have been handled ineffectively*."

The findings of this study support Proposition 1, highlighting systemic and procedural inefficiencies in the handling of data privacy infringement cases in South Africa. These challenges are primarily attributed to regulatory enforcement processes and the inadequacy of penalties as deterrents.

Key challenges highlighted from primary data collected through interviews and supported by secondary data from relevant literature were:

- Enforcement Gaps and Delayed Processes
- Insufficient Deterrence Through Penalties
- Regulatory and Procedural Shortcomings
- Exploitation of Legal Loopholes

5.2.1 Enforcement Gaps and Delayed Processes

Participants highlighted a drawn-out process in issuing enforcement notices and fines for infringement incidences, often allowing non-compliant organisations to evade immediate accountability. Unlike with other similar data regulators, where fines are imposed immediately upon detecting a data privacy infringement, POPIA adopts a more lenient approach. Under POPIA, organisations are first given an opportunity to rectify identified compliance issues following an enforcement notice. Only if they fail to comply with the remedial actions does the regulator proceed to issue an infringement notice and potentially impose a fine. This step-by-step process may reduce the deterrent effect of the regulation, allowing non-compliant organisations to delay compliance actions without immediate financial consequences (Information Regulator South Africa, 2021). Such

delays diminish the effectiveness of regulatory actions and may perpetuate a culture of non-compliance. Figure 12 depict a high-level step-by-step process of infringement case and complains management (Information Regulator South Africa, 2021).

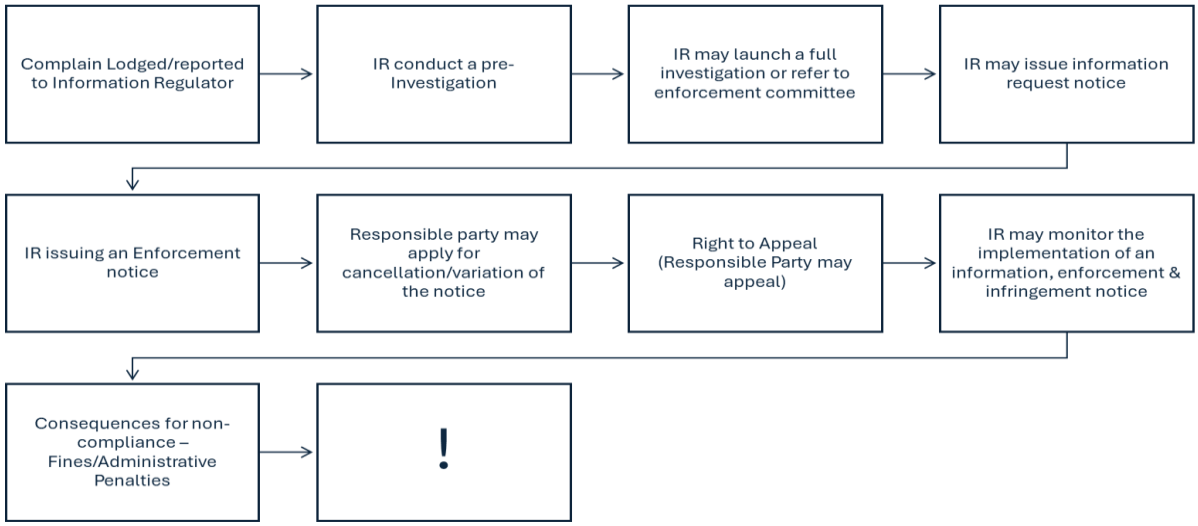


Figure 12. IR Infringement Case and Complain Step-by-Step High-level Process

5.2.2 Insufficient Deterrence Through Penalties

Lack of sufficient penalties to deter non-compliance penalties particularly for bigger corporate or multi-national companies who often cater for such fines in their annual budgets, was raised as a major concern by participants. POPIA prescribes a maximum fine of R10 million, an amount which may not be considered sufficient deterrent for large corporations with huge money (Jones, 2021). Pales in comparison to international benchmarks like the EU's General Data Protection Regulation (GDPR), which imposes fines of up to €20 million or 4% of global revenue for non-compliance (Oyewole et al., 2024). The significant fine imposed on WhatsApp LLC by the Irish Data Protection Commission (DPC) in 2021 (€225 million, approximately R3.7 billion) exemplifies a strong deterrence model that South Africa lacks (The European Data Protection Board, 2021).

In 2023 the Department of Justice and Constitutional Development (DoJCD) was reported to have ignored the enforcement notices issued by the Information Regulator of South Africa to comply with the act and implement remedial action after a data breach incident. The DoJCD was later issued with R5 million administrative fine for its failure to comply with the enforcement notice (The Information Regulator of South Africa, 2023). The disparity in enforcement severity may contribute to the perception among multinational corporations that non-compliance in South Africa carries minimal financial risk, thereby fostering a culture of non-accountability.

5.2.3 Regulatory and Procedural Shortcomings

A 2023 study conducted by the Human Sciences Research Council (HSRC) on behalf of the Information Regulator underscored several challenges impeding compliance with POPIA. A primary obstacle was the limited jurisprudence from the courts and minimal guidance from the Regulator, compelling responsible parties to interpret this nascent legislation independently. Ensuring that third-party service providers align with an Organisation’s privacy requirements emerged as another substantial challenge (HSRC, 2023).

The study by HSRC also revealed a deficiency in knowledge and capacity to implement the Act effectively, indicating a demand for more robust training and resources. A general lack of awareness regarding the specifics of POPIA was also noted. Interestingly, the study found that experiences with POPIA compliance varied, with some Organisations reporting no difficulties (HSRC, 2023).

5.2.4 Exploitation of Legal Loopholes

Participants also pointed to organisations exploiting gaps within the legislation. The Regulator's focus on less critical cases, such as the court case between the regulator media publications companies and the Department of Basic Education on publication of

matric results, at the expense of more impactful enforcement, was seen as a misallocation of regulatory resources.

5.2.5 Successes by the Information Regulator

Despite the challenges, the Information Regulator has achieved some success in handling data privacy infringement cases. Participants acknowledged positive outcomes in this regard highlighting the following:

- **Enforcement Notices Were Issued:** Both public and private sector organisations received enforcement notices for the infringement cases, demonstrating the regulator's independence.
- **Organisational Compliance with Remedial Actions:** Some organisations responded positively to the Information Regulator's remedial actions, showcasing instances where regulatory interventions led to compliance improvements.

Between May 2023 and November 2024, the Information Regulator issued only six enforcement notices under Section 95 of the Protection of Personal Information Act 4 of 2013. Of these, three were directed at government public institutions and other three at the private organisations (Information Regulator, n.d.). The successes highlighted by participants demonstrate that, amid challenges encountered in the overall handling of infringement cases, there have been instances of effective intervention. The scale of such action, however, diminishes its cumulative impact in increasing a culture of compliance. A comparison with international practice, particularly the GDPR approach, demonstrates South Africa's requirement to implement more aggressive measures. The GDPR's prescriptive approach to penalties and its emphasis on transparency and accountability have resulted in higher compliance rates within its jurisdiction (Oyewole et al., 2024).

5.3 Discussion of findings related to Proposition 2

Proposition 2: "*The South African Information Regulator is not fully effective in enforcing compliance requirements of the POPI Act*."

Findings from the interview data revealed mixed perceptions regarding the effectiveness of the Information Regulator. While some participants acknowledged the regulator's achievements and efforts, considering its early developmental stage and resource constraints, others expressed concerns that it falls short of expectations. Despite these differing opinions, most participants recognised the progress made by the regulator since its inception. Key points raised to support these perspectives include:

- Acknowledging the Information Regulator's efforts to become visible and have influence both locally and globally, positioning themselves as one of the more active data protection authorities in Africa.
- Advocating and maintaining its independence. Issuing of fines to other governmental department was highlighted as evidence.
- Improvements to their media platforms and social media, active investigations including cases taken on review to courts and their efforts in continue public engagement, host regular sessions across the country with their "Kopanong/Dikopano" initiative drive to take the Regulator to the people.

Findings from the study also highlighted operational challenges due to the limited resources and staff capacity at the regulator include concerns raised about the lack of visible communication on enforcement outcomes.

5.3.1 Resource and Capacity Constraints

The results of the study identify that insufficient resources significantly hinder the effectiveness of South Africa's Information Regulator. The other major issue the study

identified is lack of resource capacity in the regulator. With fewer staff members, the regulator's capacity to effectively implement its mandate across the whole country, particularly in thoroughly and in a timely manner investigating complaints, is weakened. The IR currently has a staff complement of less than 100, a number considered very low to meet the mandate of the Regulator.

Lack of provincial and regional offices serves to exacerbate this issue even further, with limited accessibility and outreach. The study also referred to budgetary constraints as being a major impeding factor towards the operational effectiveness of the regulator. These financial constraints curtail the regulator's ability to extend its reach, build capacity, and invest in resources and infrastructure required. Mitigating these limitations in resources is important for improving the regulator's ability to implement data protection laws properly and enforce compliance with the POPI Act throughout the nation.

5.3.2 Communication Gaps

The study found that the regulator’s effectiveness is hindered by inadequate communication, which limit broader public awareness and stakeholder engagement across difference society and social divide. Among the issues is the lack of simplified and accessible information exists for various audiences, making it difficult for the public to fully understand their rights and obligations regarding the Protection of Personal Information Act 4 of 2013 (POPIA). Furthermore, the predominant use of English as the primary language of communication presents further barriers, particularly for non-English speaking communities, thereby excluding a substantial portion of the population from meaningful participation and access to critical information.

Recognising these challenges, the regulator has set out on stakeholder consultative sessions aimed at enhancing its communication practices and gathering valuable input from diverse stakeholders (Information Regulator, 2025). Although such meetings are in

the right direction towards fostering greater inclusivity and transparency, yet their long-term impact on bridging the communication gap remains to be seen.

5.3.3 Lack of Adequate Guidance Notes

Interview participants highlighted the complexity of business understanding POPIA requirements and implementation, some defining it as highly complex. Lack of adequate practical guidance further exacerbates this challenge, leaving businesses, particularly small and medium enterprises, struggling to interpret and comply with the regulations. Some participants noted that for smaller organisations, compliance can be resource intensive and may even stifle innovation, often leading to “tick-box” exercises rather than genuine data protection. The gap between the high-level “principle-based” nature of POPIA and the lack of detailed implementation guidelines was mentioned as a contributor. The telemarketing sector was specifically mentioned as an example where compliance issues are prevalent, suggesting a need for more sector-specific guidance or a closer focus in this sector to address the challenge.

In its 2024/2025 Annual Performance Plan, the Information Regulator (IR) identified several challenges and weaknesses that hinder its operational effectiveness (Information Regulator, 2024). These include:

- Human Resource capacity (inability to attract skilled staff and inability to retain skilled staff).
- No Succession Planning Policy.
- Lacuna in POPIA not enabling effective enforcement measures.
- Lack of case management system to effectively manage and address complaints, notifications and queries.
- Inadequate office space.
- Lack of adequate training and public awareness on POPIA to the public
- Inaccessibility of the Regulator in terms of regional offices and a call centre.

- Inadequate human resources in relation to the workload.
- Lack of capacity to keep pace with technological advancements.
- Lack of jurisprudence.
- Lack of clear policy positions in respect of certain areas in the Act (legitimate interest, adequacy, electronic communication – telephones).

The study findings suggest that although the Information Regulator has achieved noteworthy advancements, focused enhancements in enforcement methods, resource distribution, and communication techniques are necessary. Increasing public awareness through communication in multiple languages, creating clearer guidance documents, and supplying industry-specific compliance assistance could greatly improve the regulator's ability to ensure compliance with POPIA.

These findings match global debates concerning data governance, especially when likened to the South African regulatory approach against the GDPR pro-active. The GDPR obliges organisations to provide rapid regulatory action by reporting data breaches within 72 hours (EU Data Protection Commission, 2018). POPIA is however, missing clear, time sensitive requirements because of which enforcement actions have a reduced deterrent effect. Investigations inefficiently, while remaining non-compliant, give organisations enough time to remain noncompliant to the law depending on the regulatory outcome. A need for frequent and random regulatory audits, real time monitoring and AI compliance assessments are some of the actions the Information Regulator can consider in improving their processes as they recommend that proactive enforcement improves overall regulatory effectiveness (Nguyen, 2024). For instance, the UK's Information Commissioner's Office (ICO) has introduced automated compliance checks to allow them to make sure that the respective organisations are compliant with data protection regulations. As such, voluntary compliance may be increasingly perceived to be inconsistent without similar proactive measures in South Africa.

The regulator has responded to these challenges by issuing selected guidance notes aimed at clarifying aspects of POPIA compliance. However, interview participants noted that these efforts remain limited in scope, leaving significant gaps in practical implementation advice, particularly for small and medium enterprises (SMEs) and sector-specific contexts (Information Regulator South Africa, n.d.).

5.4 Discussion of findings related to Proposition 3

Proposition 3: "*The current POPIA provisions are inadequate to fully address the rapidly evolving risks and challenges associated with AI technologies on data privacy*."

Central to POPIA are its eight conditions for lawful processing and handling of personal information, which are the backbone principles on which organisations must hold themselves in order to ensure compliance. These eight conditions include accountability, limitation of processing, purpose specification, further limitation of processing, quality of information, transparency, security measures, and data subject participation, all of which are aimed at responsible data management, privacy protection of the individual, and establishment of confidence in data activity. All conditions outline particular requirements for organisations like openness, data minimisation, security measures, and assurance of rights of data subjects.

POPIA, similar to other data protection legislation, was drafted before the advent and the mainstream evolution of AI technologies and hence may not adequately address the intricacies that are being present in Generative-AI technologies. Although POPIA insists on individual rights to access, correct, and delete personal data, the manner in which these rights may be exercised becomes murky in the context of Generative-AI.

The findings of this study support the Proposition 3. Most of the participants highlighted lack of clear AI-specific provision in any of the terms of POPIA. Although Section 71 of POPIA addresses automated decision making, including profiling of data subjects, which

may have significant implications for AI technologies, the study found that the Act is not adequately to deal with the broader risks associated with AI and emerging technology such as Generative-AI capabilities, specifically on the governance of the technology. No clear guidance is provided on the underlying algorithms, transparency and regulation. There are attempts, however, in the formulation of an AI Act or Framework (Discussion Document) within South Africa by another regulator, the department of communication and digital technology (DCDT, 2023). This process is still ongoing. The function of the Information Regulator was stated to have been non-existent or minimal. This raises a significant collaboration challenge amongst regulators in the data policy formulation framework.

Furthermore, POPIA also insists that Organisations obtain the people's consent before processing their data. Due to the fluid dynamics of Generative-AI, however, uncertainties exist as to how the consent can be captured and managed, particularly where the AI generates fresh data that formerly did not exist. Other participants noted that South Africa is relatively behind in fully adopting digital and AI technologies. POPIA drafted in 2013 has not went through material revision or strengthened since, contributing to the Act not been able to address the emerging technologies. Despite POPIA's principles establishing a point of departure for the protection of data, there are gaps in relation to the granting of informed consent by data subjects. Specifically, participants emphasised greater transparency on the collection, processing, and utilisation of personal information, particularly in light of sophisticated analytics and prospective processing in AI-based environments.

Other participants argued that POPIA is drafted in a generic form and technology independent focusing more on the lawfulness of processing personal information regardless of which tool is used to handle or process the data. This they argued, makes the Act to still be applicable in any technology making it more resilient and applicable against AI technologies.

While POPIA provides an overall framework of legal processing of personal data, AI systems involve complexity that must be addressed specifically. For instance, AI systems are likely to involve automated decision-making, profiling, and data processing on large scales, which may not be adequately addressed through general data protection principles (Steimers & Schneider, 2022). In the absence of specific controls, organisations will tend to struggle in knowing how they can apply POPIA's principles to AI technologies, and thus compliance practice will continue being inconsistent.

The second issue of concern raised is bias or potential bias in AI algorithm decision-making, which may lead to unfair decision or treatment against the subject. Global research on AI bias has been widely reported. The results of biased training data can result in discriminatory AI driven decisions within the field like banking, labour and law enforcement AI systems need to be under control of proper regulatory so that they do not further increase the social disparities or discriminate against the vulnerable groups (Kadiresan, Baweja, & Ogbanufe, 2022).

5.5 Discussion of findings related to Proposition 4

Proposition 4: "*South African consumers face increasing exposure to risks associated with Generative-AI and are vulnerable to data breaches and misuse*."

A report by Boston Consulting Group (2023) highlights these challenges and further notes that while South Africa has seen significant strides in adopting artificial intelligence (AI), there remains a critical gap in public awareness and understanding of AI technologies among consumers (BCG, 2023). Moreover, the legal and regulatory landscape for AI and data protection in South Africa, while evolving, may not be sufficiently robust or comprehensive to fully safeguard consumer rights in the face of these rapidly advancing technologies. The Protection of Personal Information Act (POPIA), for instance, provides a framework for data protection but may not fully address the unique challenges posed

by Generative-AI. The study found that the data support this proposition. Several arguments were raised in support of this as outlined below.

5.5.1 Tele-Marketing Challenges

Participants cited the ongoing risk and impact consumers are faced with particularly noting the tele-marketing industry where consumers are bombarded with unsolicited marketing on a daily basis with no protection. The participant noted that companies often rely on fine print, which consumers may not fully understand, leading to unintentional consent to privacy-invasive practices.

Participant 1 suggested that proactive and timeous issuing of guidance notes could be an effective interim measure to provide clarity to organisations on how to manage AI technologies responsibly. The Regulator has since issued guidance note in this regard (Information Regulator SA, 2024).

5.5.2 Organisational Vulnerabilities and risk management

Participant 3 highlighted the importance of a risk management strategy approach to AI technologies by organisations. The participant talked about applying the National Institute of Standards and Technology (NIST) framework with an emphasis on the categorisation of the risks and incorporating multiple stakeholders including governance, privacy, and risk owners. Participant also addressed the human element of AI risks like the intentional misuse and the risk of malicious actors. This point to human central approach is supported by existing literature, with the suggestion that AI governance must involve technological controls alongside human-centered policy (Sargiotis, 2024). Batool et al. (2025) argue that a need for human oversight, transparency, and ethics in managing AI risks fosters trust and accountability and balances innovation with data protection and human rights (Batool, Zowghi, & Bano, 2025).

5.5.3 Data Breaches

Concerns were also raised by participants on data breaches, data leaks, and the integrity of digital systems, particularly in light of capacity issues and infrastructure vulnerabilities. Participants quoted the NIST framework as pointed out by Participant 3, wherein the need for overall risk management considering technological and human factors was prioritised. Participant 2 referred to the perpetual issue of data breaches, giving the example that despite regulatory pressure for adequate security measures, majority of organisations do not manage to keep pace with evolving technologies. The frequency of reported data breaches across various organisations continues to rise, highlighting persistent vulnerabilities in data protection practices. Simultaneously, the Information Regulator has been receiving thousands of public complaints regarding the misuse of personal information by organisations across different sectors. This growing volume of incidents underscores ongoing challenges in ensuring compliance (IT Web, 2025).

5.6 Conclusion

The chapter presented a critical analysis of the study's findings in relation to the four research propositions, integrating empirical evidence with theoretical insights. It established that while the Information Regulator has taken meaningful steps towards enforcing the POPI Act, its efforts are undermined by procedural inefficiencies, insufficient deterrents, and limited institutional capacity. The discussion further highlighted that POPIA, though grounded in robust principles, lacks the specificity required to effectively address the evolving risks associated with AI technologies. Moreover, the chapter affirmed the growing vulnerability of South African consumers to data breaches and misuse, exacerbated by gaps in public awareness, inadequate organisational safeguards, and limited regulatory responsiveness. Overall, the findings underscore the urgent need for enhanced enforcement strategies, targeted legislative reforms, and more inclusive public engagement to strengthen data protection in the context of emerging technologies.

6. CHAPTER 6: CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This study assessed South Africa's Information Regulator's effectiveness in enforcing the Protection of Personal Information Act (POPIA), as well as its key challenges and emerging risks related to data privacy, regulation enforcement, and AI-driven technologies. The research used a qualitative approach, conducting interviews with experts and supplementing primary data with a review of secondary sources, such as literature, reported cases, and incidents related to the Information Regulator's handling of data protection infringements.

This chapter concludes the research study by summarising key findings, offering critical insights into the effectiveness and challenges of POPIA enforcement, and outlining practical recommendations to enhance regulatory oversight. Additionally, it identifies avenues for future research.

6.2 Conclusions Per Research Questions

6.2.1 Conclusions relating to research question 1

The first research question sought to examine: "*How have POPIA and related data privacy infringement cases been dealt with in South Africa?*"

The study reveals that while the regulation is an important step towards strengthening data protection in South Africa, several challenges hinder its successful enforcement. Key among these challenges is the way infringement cases are dealt with by the Information Regulator, which has resulted in varying successes of policy compliance. The study found that POPIA infringement cases are often handled ineffectively due to delayed

enforcement, weak penalties, and the exploitation of regulatory loopholes by organisations, rendering compliance efforts “tick-box exercise”.

This is also highlighted by a low number of infringement notices issued by the regulator, despite many reported incidents of data misuses and a low number of adherences to issued directives by organisations. The principle-based nature of POPIA and the enforcement approach coupled with relatively low infringement penalty fine is seen as lacking sufficient deterrence contributing to non-compliance. The current maximum fine of R10 million is insufficient to deter large corporations from non-compliance, particularly in contrast to global standards such as the General Data Protection Regulation (GDPR).

6.2.2 Conclusions relating to research question 2

The study research question 2 state: “*How effective is the Information Regulator in enforcing POPIA regulations?*”

The study found that the Information Regulator’s effectiveness is significantly hindered by structural and resource-related challenges. The office’s financial budget constraints hindering its ability to expand and have wide reach across the country has contributed to the office's ineffectiveness or having slow implementation and enforcement impact. Although the regulator has made strides in performing its oversight role by issuing enforcement notices, these efforts remain limited in scope and impact. Consumer awareness, education and overall meaningful participation of the data subjects were identified as challenges, particularly in relation to informed consent, understand of data subjects’ rights and data privacy risks.

The study stresses that the Information Regulator also needs to be more proactive and cooperative in enforcement, communication, and guiding. The steps towards developing increased regulatory capacity, increasing penalties, and developing industry-specific

guidelines are most important towards increasing compliance as well as protecting personal information.

Overall, the study highlights that weaker enforcement, delayed procedural actions, and insufficient penalties further undermine the regulator's ability to promote compliance, diminishing POPIA's effectiveness in protecting personal data in South Africa.

6.2.3 Conclusions relating to research question 3

The study research question 3 state: "*How effective are POPIA provisions in governing the risks emanating from AI technologies and mitigate data privacy issues?*"

The study also assessed the adequacy of POPIA provisions to manage AI-related risk and found that current legislation is inadequate to deal with the evolving complexities and capabilities posed by emerging technologies such as generative AI. The rise of AI and generative technologies has introduced additional complexities and major public concerns related to the handling and use of data. While POPIA has sections on automated decision-making (Section 71), these provisions are considered inadequate in dealing with AI-related risks such as algorithmic bias, generative-AI and machine learning evolving capabilities, processing large amounts of data, and ethical implications of AI-driven decision-making. The study also found that collaboration amongst other regulatory bodies, key stakeholders on the policy and framework formulation to govern AI usage is fragmented, with the Information Regulator not having much interaction with other relevant bodies.

In discussing South Africa's alignment with the AU Digital Transformation Strategy, participants underscored the necessity of bringing South Africa's national AI and data policy into alignment with continental aspirations to increase socio-economic development. The alignment, according to them, was essential for leveraging

technological innovations to address shared issues such as the digital divide within and across South Africa and the continent.

The study found that while support for continental integration was promoted, concerns were raised about the potential undermining of national sovereignty, emphasising the need for South Africa's policy climate to reflect its unique socio-economic context. Additionally, ethical AI adoption emerged as a key priority, with a strong focus on leveraging AI to address inequalities and integrate technological advancements into practical solutions for social and economic challenges.

6.2.4 Conclusions relating to research question 4

The study research question 4 state: "*What are the challenges emanating from Generative-AI concerning data privacy, protection and consumer rights in South Africa?*"

The research underscored the challenges associated with data breaches and the improper use of personal data, noting a consistent increase in reported incidents across all sectors. With the growing adoption of AI technologies in various industries, there is likewise a rise in the unlawful handling of data, consumer profiling and risk of exploitation.

One of the significant issues is the increasing data breach rate in which sensitive personal data is exposed due to poor security measures, poor compliance procedures, or the improper use of AI technologies. Poor regulation of guidelines to securely apply AI to organisational data management procedures has been one of the reasons for such vulnerabilities and has tested protecting personal data.

Furthermore, the research found that employees often share sensitive information with AI application without realising the potential consequences, leading to the risk of unintended data breaches. Participants highlighted that South African consumers generally lack awareness regarding how their data is utilised in AI-driven operations due to the black-box nature of AI and machine learning technologies, which further intensifies the issues

of transparency and accountability within the data ecosystem. This is also exacerbated by a culture of not reading fine prints and a low digital literacy level.

6.3 Recommendations

Based on the study's findings, the following recommendations are presented to enhance the effectiveness of POPIA enforcement, promote compliance, and address emerging challenges, particularly those related to AI and data governance. These recommendations are grounded in the themes and participant insights discussed in Chapter 5.

6.3.1 **Strengthening Regulatory Enforcement and Capacity**

Participants widely expressed concerns over the limited enforcement capacity of the Information Regulator, citing delays, low penalties, and limited visibility as barriers to compliance (Participants 4, 7, 9, 12, 13).

- It is recommended that the Regulator review the current administrative fine structure under POPIA. Participants noted that the R10 million cap is insufficient to deter non-compliance, particularly by large corporations. A performance-based or turnover-linked penalty model, aligned with global practices such as the GDPR, could offer greater deterrent value.
- Explore the possibility of establishing a public register of data breaches to increase transparency and accountability.
- Participants also noted that enforcement actions should be followed by accessible public communication (e.g., infographics or simplified summaries) to enhance awareness and promote transparency.

- To improve response times and broaden national reach, the Regulator may consider securing increased budgetary support and expanding its provincial presence.

6.3.2 Improving Policy Coordination and Stakeholder Collaboration

Several participants highlighted fragmentation in regulatory coordination, especially in the governance of AI and cross-cutting digital policies (Participants 1, 4, 8, 12, 14).

- The study recommends that the Information Regulator continue participating in multi-agency platforms such as the Regulators' Forum, and explore deeper collaboration with entities like ICASA, FPB, and NCC to harmonise regulatory guidance.
- Participants emphasised the value of industry-specific guidance notes, especially for sectors heavily impacted by AI. Involving technical experts, civil society, and the private sector in drafting such instruments can increase relevance and uptake.

6.3.3 Addressing Gaps in POPIA for Emerging Technologies

The study found that while POPIA offers a foundational regulatory framework, it is not fully equipped to address the complexities introduced by AI and emerging technologies (Participants 1, 7, 8, 10, 12).

- It is recommended that Section 71 on automated decision-making be reviewed and possibly expanded to include specific safeguards for AI-based data processing, including fairness, bias mitigation, and transparency requirements.

- The Regulator may also consider advocating for complementary legislative instruments or amendments to POPIA to better manage risks posed by generative AI and machine learning.

6.3.4 Supporting Organisational Compliance and Capacity

A recurring theme from the interviews was the implementation gap between POPIA's legal requirements and organisational capacity, particularly among SMEs (Participants 3, 5, 10, 12).

- It is recommended that the Regulator develop clear, practical compliance toolkits and sector-specific guides, especially for small and medium enterprises.
- The study further suggests promoting public-private compliance partnerships, where larger organisations share best practices and mentorship with smaller firms to foster broader compliance.

6.3.5 Improving Public Awareness, Engagement and Education

Participants consistently raised the issue of low public awareness and digital literacy as a major challenge to compliance and consumer protection (Participants 1, 4, 6, 7, 9, 12).

- Collaborating with educational authorities to integrate data protection into school curricula was proposed as a long-term strategy to foster a data protection culture.
- The Regulator, in partnership with the GCIS, DBE, DHET, and other stakeholders, should intensify public awareness campaigns using diverse media channels, including vernacular radio, community engagements, and social media.

- Participants also recommended that POPIA-related materials and consent forms be translated into South Africa's official languages to improve accessibility.

6.3.6 Encouraging Ethical Use of Data and Responsible AI

The research highlighted significant concerns around the ethical implications of AI in data processing (Participants 3, 9, 12, 13).

- The Regulator, in collaboration with academic institutions and technical experts, should promote ethical frameworks for AI governance, ensuring fairness, accountability, and transparency in automated decision-making.
- Participants also proposed publishing guidance notes on ethical AI, with practical case studies to guide responsible adoption across sectors.

6.4 Suggestions for further research

This study has highlighted several important issues for future research to enhance data protection practice and regulatory effectiveness in South Africa. Future studies can investigate the limitations identified in this study while enriching the discourse on regulatory usefulness, technological advancements, and consumer protection. A key area of interest is evaluating if public education campaigns and digital literacy initiatives are promoting greater awareness of data privacy rights, particularly among marginalized communities. Given the low compliance culture and widespread lack of awareness, targeted multilingual strategies that simplify complex data protection concepts could be explored to enhance consumer education and regulatory compliance. Additionally, the ethical implications of AI-driven data processing warrant further examination. Research can focus on the development of guidelines for the deployment of AI in an ethical manner, stressing fairness, reducing bias, and safeguarding consumer rights.

References

Agius, S. J. (2013, June). Qualitative research: its value and applicability. *The Psychiatrist, 37*(6), 204 - 206. doi:doi:10.1192/pb.bp.113.042770

Aglietta, M. (1976). Régulation et crises du capitalisme. Paris: Éditions du Seuil. This seminal work introduces the Theory of Regulation, discussing how regulatory frameworks impact capitalist economies. *OpenEdition Journals*. doi:https://doi.org/10.4000/11w7i

Akhtar, D. I. (2016). Research Design. *Researchgate*. Retrieved from https://www.researchgate.net/publication/308915548_Research_Design/citations

American Psychological Association. (2018, April 19). *APA Dictionary of Psychology*. Retrieved from https://dictionary.apa.org/qualitative-research

Batool, A., Zowghi, D., & Bano, M. (2025, February). Responsible AI Governance: A Systematic Literature Review. doi:http://dx.doi.org/10.48550/arXiv.2401.10896

BCG. (2023, September 28). *South Africa and Artificial Intelligence. The potential impact of AI and Generative AI across healthcare, education, financial inclusion, and agriculture.* Boston Consulting Group. Boston Consulting Group. Retrieved from https://web-assets.bcg.com/93/9f/1670ed264407b374a2eea9dcd95e/bcg-south-africa-and-artificial-intelligence-sept-2023.pdf

Castells, M. (1997). An introduction to the information age. doi:https://doi.org/10.1080/13604819708900050

Castells, M. (2010). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture.* (2nd ed.). Retrieved from https://deterritorialinvestigations.wordpress.com/wp-

content/uploads/2015/03/manuel_castells_the_rise_of_the_network_societybook fi-org.pdf

Castells, M., & Cardoso, G. (2006). *The Network Society from Knowlledge to Policy.* (M. Castells, & G. Cardoso, Eds.) The Johns Hopkins University: Center for Transatlantic Relations. Retrieved from https://www.dhi.ac.uk/san/waysofbeing/data/communication-zangana-castells-2006.pdf

Chen, D., & Dahlman, C. (2006). *The knowledge economy, the KAM methodology and World Bank operations.* World Bank. Retrieved July 21, 2024, from http://documents.worldbank.org/curated/en/695211468153873436/The-knowledge-economy-the-KAM-methodology-and-World-Bank-operations

Chen, Y., Zhao, Y., Xie, W., Zhai, Y., Zhao, X., Zhang, J., . . . Zhou, F. (2023, October 7). An Empirical Study on Core Data Asset Identification in Data Governance. *mdpi, 7*(4). doi:https://doi.org/10.3390/bdcc7040161

Chimboza, T., & Smith, E. (2024, September 12). How Does Compliance with the Protection of Personal Information Act (POPI Act) Affect Organisations in South Africa? *ACIST*, 17. Retrieved March 2025, from https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1210&context=acist

CIPIT. (2023). *The State of AI in Africa Report.* Strathmore University - Centre for Intellectual Property and Information Technology Law. Retrieved from https://cipit.strathmore.edu/state-of-artificial-intelligence-in-africa-2023-report/

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*. doi:https://doi.org/10.1080/17439760.2016.1262613

Creswell, J., & Poth, C. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.* SAGE Publications.

Croley, S. (2008). *Regulation and Public Interests: The Possibility of Good Regulatory Government.* Princeton: Princeton University Press. doi:https://doi.org/10.1515/9781400828142

DAMA International. (2017). *DAMA-DMBOK Data Management Body of Knowledge* (2nd ed.). Technics Publications. Retrieved November 2024

DCDT. (2023, October). *Department of Communications and Digital Technologies.* Retrieved from https://www.dcdt.gov.za/images/phocadownload/AI_Government_Summit/National_AI_Government_Summit_Discussion_Document.pdf

Drahos, P., & Krygier, M. (2017). Regulation, Institutions and Networks. In *Regulatory Theory: Foundations and applications* (pp. 1-22). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.7

EU Data Protection Commission. (2018, May). *A Practical Guide to Personal Data Breach Notifications under the GDPR.* Retrieved from https://www.dataprotection.ie/en/dpc-guidance/breach-notification-practical-guide: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022, February 28). Financial Risk Management and Explainable, Trustworthy, Responsible AI. *Frontiers in Artificial Intelligence, 5*, 14. doi:https://doi.org/10.3389/frai.2022.779799

G20 Brazil. (2024, April 10). https://www.g20.org/en/news/manuel-castells-we-must-find-ways-to-regulate-the-networks. *Manuel Castells: "We must find ways to regulate*

the networks". Retrieved from https://www.g20.org/en/news/manuel-castells-we-must-find-ways-to-regulate-the-networks

Gmiterek, G., & Kotuła, S. D. (2025, March). Generative artificial intelligence in the activities of academic libraries of public universities in Poland. *The Journal of Academic Librarianship, 51*(3). doi:https://doi.org/10.1016/j.acalib.2025.103043

Goertz, G., & Mahoney, J. (2012, May 24). Concepts and measurement: Ontology and epistemology. *Sage Journals, 51*(2). doi:https://doi.org/10.1177/0539018412437108

Grishin, V., Boichenko, A., & Lukinova, O. (2020, January). Information Society: Causes, Features and Risks. *113*. doi:https://doi.org/10.2991/fred-19.2020.111

Hantke-Domas, M. (2003). The Public Interest Theory of Regulation: Non-Existence or Misinterpretation? *European Journal of Law and Economics, 15*, 165-194. doi:https://doi.org/10.1023/A:1021814416688

HSRC. (2023). *A Public Opinion Survey on Awareness about the Right to Privacy as it relates to the Protection of Personal Information Act 4 of 2013.* The Information Regulator. Retrieved from https://inforegulator.org.za/wp-content/uploads/2020/07/POPIA-summary-report.pdf

IEC. (2024, November 15). *Electoral Commission complies with Information Regulator Enforcement Notice.* Retrieved from https://www.elections.org.za/: https://www.elections.org.za/content/About-Us/News/Electoral-Commission-complies-with-Information-Regulator-Enforcement-Notice/

Information Regulator. (n.d.). Retrieved from Enforcement Notices: https://inforegulator.org.za/enforcement-notices/

Information Regulator. (2022). *Powers, functions and duties of the Information Regulator*. Retrieved July 2, 2024, from https://inforegulator.org.za/about/

Information Regulator. (2024). *Guidance note on application for prior authorisation.* Retrieved from https://inforegulator.org.za/wp-content/uploads/2020/07/Revised-Guidance-Note-on-applications-for-Prior-Authorisation-adopted-by-Members-30-Jan14.pdf

Information Regulator. (2024). *Information Regulator Annual Performance Plan 2024/2025.* Retrieved from https://inforegulator.org.za/wp-content/uploads/2020/07/APP-2024-19-March-2024.pdf

Information Regulator. (2025, March 3). *INFORMATION REGULATOR HOSTS A STAKEHOLDER CONSULTATIVE SESSION ON IT'S ANNUAL PLANS FOR THE 2025/2026 FINANCIAL YEAR. .* Retrieved from https://inforegulator.org.za/wp-content/uploads/2025/03/Media-Invite-stakeholder-Engagement-Session-05-March-2025.pdf

Information Regulator RSA. (2023). *Annual Report 2022-2023.* Retrieved July 03, 2025, from https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf

Information Regulator SA. (2024, December 3). *Guidance Note on Direct Marketing.* Retrieved from https://inforegulator.org.za/wp-content/uploads/2020/07/GUIDANCE-NOTE-ON-DIRECT-MARKETING-IN-TERMS-OF-THE-PROTECTION-OF-PERSONAL-INFORMATION-ACT-4-OF-2013-POPIA.pdf

Information Regulator South Africa. (2021, October). Rules of procedure relating to the manner in which a complaint must be submitted and handled by the information regulator. Retrieved January 2025, from https://inforegulator.org.za/wp-

content/uploads/2020/07/20211012-InfoReg-RulesOfProcedure-HandlingPOPIAcomplaints-1.pdf

Information Regulator South Africa. (n.d.). *Guidance Notes*. Retrieved from https://inforegulator.org.za/guidance-notes/

IODSA. (2016, November 1). *King IV Report on Corporate Governance for South Africa.* Retrieved from https://cdn.ymaws.com/www.iodsa.co.za/resource/collection/684B68A7-B768-465C-8214-E3A007F15A5A/IoDSA_King_IV_Report_-_WebVersion.pdf

IR. (2024, September 11). *Information Regulator Presents Developments on High-Level Paia Cases, Non-Compliance by Public Bodies and Progress on POPIA Matters.* Retrieved from https://inforegulator.org.za/: https://inforegulator.org.za/wp-content/uploads/2020/07/Media-Address-Quarter-1-progress-on-PAIA-and-POPIA-cases-11-September-2024-Final.pdf

ISO. (2022). *ISO/IEC DIS 22989(en)*. Retrieved from Information technology — Artificial intelligence concepts and terminology: https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:dis:ed-1:v1:en

IT Web. (2025, March 6). *InfoReg receives mounting data privacy complaints*. Retrieved March 8, 2025, from Public Sector: https://www.itweb.co.za/article/inforeg-receives-mounting-data-privacy-complaints/wbrpOqg2oVKMDLZn

ITWeb. (2022). *Over 3.6m records exposed in Dis-Chem cyber attack.* ITWeb. Retrieved June 28, 2024, from https://www.itweb.co.za/article/over-36m-records-exposed-in-dis-chem-cyber-attack/PmxVE7KEABOqQY85

Johannesson, P., & Perjons, E. (2021). Research Strategies and Methods. 22. doi:https://doi.org/10.1007/978-3-030-78132-3_3

Jones, B. (2021). Is Popia Bad Business for South Africa? Comparing The GDPR To POPIA and Analyzing POPIA ‘s Impact on Businesses in South Africa. *Penn State Journal of Law & International Affairs, 10*(1). Retrieved from https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1311&context=jlia

Kadiresan, A., Baweja, Y., & Ogbanufe, O. (2022). *Bias in AI-based decision-making. In Bridging Human Intelligence and Artificial Intelligence (pp. 275-285).* Springer International Publishing. doi:http://dx.doi.org/10.1007/978-3-030-84729-6_19

Khanday, S. A., & Khanam, D. (2023). The Research Design. *Researchgate*. Retrieved from https://www.researchgate.net/publication/368257495_THE_RESEARCH_DESIGN

Kuner, C. (2023). Protecting EU data outside EU borders under the GDPR. *Common Market Law Review, 60*(1), 30. doi:https://doi.org/10.54648/cola2023004

Leavy, P. (2020). *The Oxford Handbook of Qualitative Research (2nd edn).* Oxford University Press. doi:https://doi.org/10.1093/oxfordhb/9780190847388.001.0001

Lee, A. W. (2021, July). An analysis of the Protection of Personal Information Act (POPIA) and the European Data Protection Framework: suggestions for South Africa. Retrieved from https://researchspace.ukzn.ac.za/handle/10413/20928

Lnenicka, M., & Komarkova, J. (2019). Big and open linked data analytics ecosystem: Theoretical background and essential elements. *Government Information Quarterly, ScienceDirect, 36*(1). doi:https://doi.org/10.1016/j.giq.2018.11.004

Mbonye, V., Moodley, M., & Nyika, F. (2024, August 30). Examining the applicability of the Protection of Personal Information Act in AI-driven environments. *South African Journal of Information Management, 26*(1), 9. doi:https://doi.org/10.4102/sajim.v26i1.1808

Mckinsey & Company. (2022, August 17). What are Industry 4.0, the Fourth Industrial Revolution, and 4IR? Retrieved from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir

MIT Technology Review. (2021). *Capitalizing on the data economy.* MIT. Retrieved from https://www.technologyreview.com/2021/11/16/1040036/capitalizing-on-the-data-economy/

Morgan, B., & Yeung, K. (2007). Theories of regulation. In *An Introduction to Law and Regulation: Text and Materials. Law in Context* (pp. 16-78). Cambridge University Press. doi:https://doi.org/10.1017/CBO9780511801112.003

Ndamase, Z. (2014, August 29). The impact of data governance on corporate performance:. Retrieved from https://open.uct.ac.za/server/api/core/bitstreams/d3b8e4e2-0efe-4b85-b4f6-3d8643058918/content

Ndemo, B., & Mkalama, B. (2023). Digitalisation and Financial Data Governance in Africa: Challenges and Opportunities. In B. Ndemo, N. Ndung'u, S. Odhiambo, & A. Shimeles (Eds.), *Data Governance and Policy in Africa. Information Technology and Global Governance.* Palgrave Macmillan, Cham. doi:https://doi.org/10.1007/978-3-031-24498-8_6

Ndemo, B., Ndung'u, N., Odhiambo, S., & Shimeles, A. (2023). Data Governance and Policy in Africa. In *Data Governance and Policy in Africa. Information Technology and Global Governance.* doi:https://doi.org/10.1007/978-3-031-24498-8_1

Nguyen, K. (2024, May). Enhancing Data Privacy in Artificial Intelligence - A Study on Corporate Practices and Regulatory Compliance. Retrieved from

https://www.utupub.fi/bitstream/handle/10024/178070/Nguyen_Khanh_Thesis.pdf?sequence=1&isAllowed=y

Nkholedzeni, S. N. (2020). Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication, 69*(1), 58-74. doi:https://doi.org/10.1108/GKMC-02-2019-0026

OECD. (2021). *Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers.* OECD. Retrieved from https://www.oecd.org/finance/artificial-intelligence-machine-learning-big-data-in-finance.htm

Omona, J. (2013, July 3). Sampling in Qualitative Research: Improving the Quality of Research Outcomes in Higher Education. *4*(2). doi:https://doi.org/10.4314/majohe.v4i2.4

Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data Privacy Laws and Their Impact on Financial Technology Companies: A Review. *Computer Science & IT Research Journal, 5*(3). doi:DOI: 10.51594/csitrj.v5i3.911

Paoli, S. D. (2024, August). Performing an Inductive Thematic Analysis of Semi-Structured Interviews With a Large Language Model: An Exploration and Provocation on the Limits of the Approach. *Sage Journals, 42*(4). doi:https://doi.org/10.1177/08944393231220483

POPIA. (2019, September 10). Category: Data subject rights. *Protection of Personal Information Act*. Retrieved from https://popia.co.za/category/data-subject/

Pressman, J. L., & Wildavsky, A. (1984). *Implementation.* University of California Press.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022, March 05). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*. doi:https://doi.org/10.1007/s11747-022-00845-y

Raab, K. S. (2024). Consumers' Disposal Behavior at the Base of the Pyramid. doi:https://doi.org/10.17170/kobra-202404039888

RSA Constitution. (1996). *Constitution of the Republic of South Africa, 1996 - Chapter 2: Bill of Rights*. Retrieved from https://www.gov.za/documents/constitution/chapter-2-bill-rights

RSA Government. (2022). *Post Office on Postbank cybercrime attack.* Government Communications Department. Retrieved from https://www.gov.za/news/media-statements/post-office-postbank-cybercrime-attack-31-mar-2022

RSA Government Gazette. (2013, November 26). *https://www.gov.za/documents/protection-personal-information-act.* Retrieved from South African Government Official Information and Services: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

RSA Government Gazette. (2013, November 26). *https://www.gov.za/documents/protection-personal-information-act.* Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

RSA Information Regulator. (2024, Nov 13). *Information Regulator Issues an Update on Developments in its International Cooperation Work, Innovation and Progress on POPIA Matters.* Retrieved from https://inforegulator.org.za/: https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT_INFORMATION-REGULATORS-LATEST-UPDATE-2.pdf

Ruslan, I. F., Alby, M. F., & Lubis, M. (2023). Applying Data Governance using DAMA-DMBOK 2 Framework: The Case for Human Capital Management Operations. doi:https://doi.org/10.1145/3568834.3568866

SABRIC. (2020). *Experian Data Breach.* Retrieved from https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach/

SAFPS. (2024, May 1). *https://www.safps.org.za/Home/Article_FraudSummit_FraudLandscape*. Retrieved January 10, 2025, from https://www.safps.org.za/Home/Article_FraudSummit_FraudLandscape

Sargiotis, D. (2024, July 29). Fostering Ethical and Inclusive AI: A Human-Centric Paradigm for Social Impact. Retrieved from https://ssrn.com/abstract=4879372

Sarker, I. H. (2021, July 12). Data Science and Analytics: An Overview from Data-Driven Smart Computing, Decision-Making and Applications Perspective. *Springer*. doi:https://doi.org/10.1007/s42979-021-00765-8

Schillemans, T., & Bovens, M. (2019, January). Governance, accountability and the role of public sector boards. *Policy and Politics, 47*(1). doi:https://doi.org/10.1332/030557318X15296526490810

Schwab, K. (2016). *The Fourth Industrial Revolution.* World Economic Forum.

Schwandt, T. A. (2007). Judging interpretations: But is it rigorous? trustworthiness and authenticity in naturalistic evaluation. 11 - 25. doi:https://0-doi-org.innopac.wits.ac.za/10.1002/ev.223

Sebastian, F.-M., Bernhard, H., & Jochen, P. (2022, February 28). Financial Risk Management and Explainable, Trustworthy, Responsible AI. *Frontiers in Artificial Intelligence, 5*. doi:https://doi.org/10.3389/frai.2022.779799

Sestino, A., Kahlawi, A., & De Mauro, A. (2023, August). Decoding the data economy a literature review of its impact on business, society and digital transformation. *ResearchGate*, 27. doi:http://dx.doi.org/10.1108/EJIM-01-2023-0078

Silverman, D. (2004). *Qualitative Research: Theory, Method and Practice.* London: Sage Publications.

Smit, B., & Scherman, V. (2021). Computer-Assisted Qualitative Data Analysis Software for Scoping Reviews: A Case of ATLAS.ti. *International Journal of Qualitative Methods, 20*, 3. doi:https://doi.org/10.1177/16094069211019140

Statista. (2024). *Artificial Intelligence - South Africa.* Statista. Retrieved from https://www.statista.com/outlook/tmo/artificial-intelligence/south-africa

Steimers, A., & Schneider, M. (2022). Sources of Risk of AI Systems. *International Journal of Environmental Research and Public Health*. doi:https://doi.org/10.3390/ijerph19063641

Stigler, G. (1971). The Theory of Economic Regulation. *Jstor*. doi:https://doi.org/10.2307/3003160

Swales, L. (2022, March 9). The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock? *PER / PELJ*. doi:https://doi.org/10.17159/1727-3781/2022/v25ia11180

The European Data Protection Board. (2021). *Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR.* Retrieved from https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en

The Information Regulator of South Africa. (2023, July 4). *Infringement Notice and R5 Million Administrative Fine Issued to The Department of Justice and Constitutional Development for Contravention of POPIA.* Retrieved from https://inforegulator.org.za/: https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf

Thompson, J. (2022, May 19). A Guide to Abductive Thematic Analysis. *27*(5). doi:https://doi.org/10.46743/2160-3715/2022.5340

Toivanen, H. (2012, April). Knowledge Economy and Globalization. *ResearchGate*. doi:http://dx.doi.org/10.1596/978-1-4648-0194-5_ch8

Toner, H. (2023, May 12). *CSET*. Retrieved Janury 11, 2025, from https://cset.georgetown.edu/article/what-are-generative-ai-large-language-models-and-foundation-models/

TransUnion. (2022). *March 2022 South Africa Cyber Incident.* Retrieved from https://newsroom.transunion.co.za/update-south-africa-cyber-incident/

TransUnion USA. (2022). *More Than 22 Million Identities Exposed in High-Risk Data Breaches in Final Quarter of 2022 That May Impact Public Sector Agencies.* USA. Retrieved from https://newsroom.transunion.com/more-than-22-million-identities-exposed-in-high-risk-data-breaches-in-final-quarter-of-2022-that-may-impact-public-sector-agencies/

Tunacan, T., & Hatipoğlu, C. (2021). Information Society Perspective in Turkey: Literature Study. *OPUS International Journal of Society Researches, 18*(41). doi:https://doi.org/10.26466/opus.937283

Vears, D., & Gillam, L. (2022). Inductive content analysis: A guide for beginning qualitative researchers. *A Multi-Professional Journal*. Retrieved from https://search.informit.org/doi/pdf/10.3316/informit.455663644555599

Veiga, A. d. (2022, November). A study on information privacy concerns and expectations of demographic groups in South Africa. *ScienceDirect, 47*, 19. doi:https://doi.org/10.1016/j.clsr.2022.105769

Veiga, A. D., Abdullah, H., Eybers, S., Ochola, E., Mujinga, M., & Mwim, E. (2024, December 4). Evaluating Data Privacy Compliance of South African E-Commerce Websites Against POPIA. *Journal of Information Systems and Informatics, 6*(4), 40. doi:https://doi.org/10.51519/journalisi.v6i4.917

Warikandwa, T. (2021, May 21). Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared. *Potchefstroom Electronic Law Journal*. doi:http://dx.doi.org/10.17159/1727-3781/2021/v24i0a10727

Webster, F. (1995, 2006). *Theories of the Information Society* (1st & 3rd Editions ed.). London: Routledge. doi:https://doi.org/10.4324/9780203991367

Webster, F., & Robins, K. (2013). Information Society. In *The International Encyclopedia of Digital Communication and Society* (pp. 595-607). Wiley-Blackwell.

World Bank. (2022). *Inequality in Southern Africa: An Assessment of the SouthernAfrican Customs Union.* Retrieved from https://documents1.worldbank.org/curated/en/099125303072236903/pdf/P1649270c02a1f06b0a3ae02e57eadd7a82.pdf

World Economic Forum. (2016, January 14). *The Fourth Industrial Revolution: what it means, how to respond*. Retrieved from World Economic Forum:

https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Xia, Q., Weng, X., Ouyang, F., Lin, T. J., & Chiu, T. K. (2024, May 24). A scoping review on how generative artificial intelligence transforms assessment in higher education. *Springeropen*, 21. doi:https://doi.org/10.1186/s41239-024-00468-z

Appendix A

Participants Job Descriptions

Participants	Role	Job Description
Participant 1	POPIA SME compliance officer	The participant is a POPIA Subject Matter Expert (SME) Compliance Officer at a bank. In this role, they liaise with the IT and Legal departments to assist with any POPIA-related issues. Their primary responsibility is to ensure compliance with the POPI Act throughout the entire data lifecycle. This includes overseeing that personal information is collected, processed, and ultimately destroyed in a manner that complies with POPIA. The participant ensures that data processing and collection are secure from the outset, and that when data is no longer needed, it is destroyed securely in line with POPIA requirements.

Participant 2	Training Manager	Responsible for training public and private bodies on key legislative frameworks, specifically the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA). Primary duty involves capacitating officials by enhancing their understanding of the eight conditions for lawful processing of personal information under POPIA, as well as promoting access to information in terms of PAIA. In addition to delivering training, the participant plays a role in the review and implementation of the education and training strategy, which guides how educational programmes are conducted. They are also involved in the development of a collaboration framework aimed at supporting education and training initiatives related to both legislations.
Participant 3	Head of Data Governance and Management	Head of Data Governance and Management within the organisation's Group Compliance division. Lead a cluster responsible for enabling the organisation's data strategy, with a scope that spans key business areas including compliance, internal auditing, and group legal. The role involves building and overseeing a Data Management Office, with a focus on supporting Management Information (MI) and Business Intelligence (BI) reporting. The primary emphasis of their work is on compliance, regulatory reporting, financial crime reporting, and internal auditing, ensuring that data governance frameworks and practices support these critical functions.

Participant 4	Manager Information Technology	Primary responsibility is to bridge the gap between legal experts and technological developments, particularly in the context of emerging technologies that affect the processing of personal information. They support teams, primarily from legal backgrounds, by enhancing their understanding of how advanced technologies, such as artificial intelligence, operate and potentially impact personal data. In addition to their advisory role, the participant assists the POPIA division in conducting compliance assessments, with a specific focus on security safeguards as outlined under Condition 7 of POPIA (Section 19(2) and 19(3)). They also conduct research on emerging technologies and their implications for personal information, while promoting basic security awareness in collaboration with the internal cybersecurity team.
Participant 5	Policies Developer	The participant is responsible for the development, review, and amendment of departmental policies, ensuring they remain aligned with ongoing developments in the Information and Communication Technology (ICT) framework. This involves continuously assessing the relevance and adequacy of existing policies and making necessary updates to reflect technological advancements and regulatory expectations. In addition to policy development, the participant also plays a key role in ensuring policy compliance across the department.
Participant 6	Manager Policy Development Officer	The participant is the Manager responsible for Compliance and Monitoring within the Protection of Personal Information (POPIA) Division of the organisation. Their primary responsibility is to oversee compliance and monitoring activities in line with the provisions of Section 41(b)(vi) and Section 89 of POPIA. A key part of their role involves managing the assessment projects related to POPIA compliance.

Participant 7	Professor of Political Science	The participant is a Professor of Political Science currently based in the Department of Computer Engineering at a university. Although their disciplinary background is in political science, their placement in a technical department reflects their longstanding involvement in interdisciplinary work on technology assessment. For the past eight years, the participant has focused on teaching and research related to ethics in information technology, with particular emphasis on data governance, data protection policy, and the societal implications of AI. Their role includes delivering mandatory courses on data protection, as well as broader topics such as the governance of data and the inclusivity of emerging technologies, aimed at broadening engineering students' understanding of the societal dimensions of technology.
Participant 8	Data Privacy and Compliance Expert (Industry expert and consultant)	The participant is a Senior Consultant specialising in privacy and information security within a boutique consulting agency. The role involves providing expert guidance to small and medium-sized technology companies and startups on privacy compliance. In addition to client consulting, they are responsible for implementing and maintaining privacy practices within the organisation, such as ensuring the accuracy and currency of the company's privacy notice. The work reflects a hands-on approach to applying data protection principles in practice.

Participant 9	Attorney - Data Protection, Data Governance, AI Privacy Governance expert	The participant is an attorney whose work focuses on data protection, data governance, AI privacy, and AI governance. Their role involves advising organisations on compliance with various data protection regulations, including POPIA, GDPR, and other African and international data protection laws. On a day-to-day basis, the participant assists companies in establishing and maintaining effective data protection and governance frameworks to ensure regulatory compliance across multiple jurisdictions.
Participant 10	Chief Data Officer (CDO) - data governance and policies and procedures around data management	The participant serves as the Chief Data Officer (CDO) of Systems, where they are primarily responsible for the daily governance of data and ensuring the effective implementation of policies and procedures related to data management. While the role does not include formal responsibilities as a Data Protection Officer (DPO), it focuses on maintaining organisational alignment with data management standards and best practices. The participant is recognised as an industry expert and thought leader in the fields of data management and data governance. They actively contribute to the development of the profession through conducting workshops and training sessions, where they equip organisations with practical knowledge on data management best practices, the formulation and execution of data strategies, and the design and implementation of data management frameworks. Their work supports both organisational maturity in data governance and the broader advancement of data practices in the industry.

Participant 11	Attorney (Analyst) – Digital Policy and Regulations	The participant is an Analyst in the Centre for Digital Excellence at an impact-based organisation focused on economics and digital policy. Their role involves mapping digital policies and regulations, including data privacy, cybersecurity, and artificial intelligence, across selected African and Asian countries. This includes engaging with stakeholders, analysing national frameworks, and preparing policy submissions to regional and national bodies. Prior to this, the participant was a practising attorney specialising in technology, media, and telecommunications law, with a particular focus on data privacy compliance and interactions with information regulators.
Participant 12	Information Privacy officer	The participant serves as an Information Privacy Officer within their organisation. Their primary responsibility is to assist with the development, implementation, maintenance, and enforcement of privacy policies and procedures. These policies govern the collection, use, disclosure, and protection of personal information. The participant's role is specifically focused on personal information and its handling across the organisation's ICT processes, data regulations, and policies. They are actively involved whenever personal information is implicated, ensuring that privacy and information governance requirements are met.

Participant 13	Managing Attorney	The participant is the Managing Director and Managing Attorney at their organisation. Their role combines strategic oversight, quality control, and direct client engagement. They support attorneys within the organisation, review outgoing work for quality, and contribute to the development of legal and compliance solutions for clients. In relation to ICT policy and data governance, the participant holds ultimate responsibility for data governance and compliance within the organisation. They lead the organisation's internal Morris Programme, which ensures proper data governance practices and adherence to relevant laws. Additionally, the participant plays a central role in the organisation's core business of assisting external companies with ICT policy development and data governance compliance.
Participant 14	Professor – Teaching and Research	The participant is an academic at a university, with a professional background rooted in teaching and research. Their day-to-day responsibilities primarily involve academic work. Previous experience also includes governance matters ICT/ICTG committees and participating in collaboration discussions on policy matters.

Appendix B

Ethics Clearance Certificate

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB1488581/631

This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).

Project title	Data governance in the AI era: analysing the effectiveness of information regulator in implementing POPIA
Investigator / Researcher	Mr Obopeng Goitsione
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	02/09/2024
Expiry date	Date of submission of the project / research report
Chairperson	Dr Ayanda Magida ☎ +27 11 717 3953 ✉ ayanda.magida@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Signature

2024/09/12
Date: