
# The Effect of Pertinent Factors in Preparation for Compliance with the South African Protection of Personal Information Act of 2013 (POPI)

**Amiel Myron Joshua (406165)**

A research report submitted to the Faculty of Humanities, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Arts in the field of Information Communication Technology Policy and Regulation MA (ICTPR).

May 2018

## ABSTRACT

While South Africa passed the Protection of Private Information (POPI) Act in 2013, it has not been fully enforced. Consequently there is only a basic understanding of the effect of preparation to comply with the Protection of Personal Information (POPI) Act on the organisation, staff and cost anticipated for the compliance effort. This study delves into these aspects to build a picture of various factors that are pertinent in preparation to comply.

This study is exploratory due to the Act being relatively new and not fully enforced yet. It is qualitative in nature, specifically employing a constructivist lens, and gathering opinions and feelings of respondents to gain insights on the research question posed. The tool for data collection was formal semi-structured interviews that allowed for all interviewees to be asked the same questions and for flexibility to drill down into responses to gain deeper insight. The analytical framework combines elements from two ISO standards - 19600 & 17799 (now 27002) and the OECD's Compliance Cost Assessment (CCA) framework.

The retrospective effect of the Act was determined to be a risk in preparation for compliance particularly the conditions for lawful processing of information as currently held information would need to comply with the Act as well as new information being collected going forward. Compliance with legal requirements works hand in hand with corporate governance. The King IV codes are an example of corporate governance standards in South Africa and have bearing on data protection and data governance and suggest that it be on the agenda of the Board of an organisation. While the codes of governance are detailed and good practise by many accounts they are not legally binding and as such the POPI Act can be seen to be the legal instrument to ensure a minimum standard of protection across the board.

A unique aspect of the POPI Act is pertinent to organisations in that juristic person's privacy is protected by the Act. Various reasons are given for this, but the analysis determined that the most plausible is that this is due to the constitution. How this is done could be determined by a future study into the matter. Governance and organisational theory are traversed also. Compliance with legislation is central to these. The Act stands to affects the structure of organisations and spur change. The study also proposes a model for compliance.

## DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Master of Arts in the field of ICT Policy and Regulation in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.

_____

Amiel Myron Joshua

10 May 2018

## DEDICATION

To my wife Emanuela, thank you for your love and support in spurring me on to completion of this study. There will be many more challenges on our onward journey, but none of them insurmountable. To my family here and around the world, you have instilled in our generation a desire to accomplish academically, I trust that we will be able to do the same for the successive generation. To my parents, especially my mum, Dr JJ Joshua, thank you for always encouraging and supporting me in this journey, as you have throughout my life. This research report is also dedicated to our son, born on 6 September 2016. My boy, Asher Manuel, we are grateful for your safe arrival and the many years we will share together!

*1 Corinthians 15:57 "But thanks be to God! He gives us the victory through our Lord Jesus Christ."*

## ACKNOWLEDGEMENTS

This research report was brought to fruition by the guidance of my supervisor Dr Kiru Pillay. Your input and insight were much appreciated. Also, to Dr Luci Abrahams and Charley Lewis for your input over the years, and for the opportunity to participate in this programme, I thank you.

I would also like to acknowledge the various participants who contributed to this study in interviews; your time and input were greatly appreciated.

To the good people of the East African and European countries where I wrote this research report, your hospitality was much appreciated.

To family and friends that have had to hear the endless: “I need to study”, that refrain has ended - for now…

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

# GLOSSARY OF KEY TERMS IN THIS STUDY

| | |
|---|---|
| Data | Numbers and letters, raw, unanalysed and unprocessed. |
| Data subject | As defined in the POPI Act as the person the personal information relates. |
| Information | Data that was been processed and analysed. |
| Operator | As defined by the POPI Act as a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. |
| Organisation | Groups of people who are working towards a common goal or outcome, could be a business, company, religious grouping or even non-governmental groups. |
| Personal information | That which identifies a person. These are various attributes such as identity number, full names, contact details and addresses. |
| Responsible party | As defined by the POPI Act as a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. |

## CHAPTER 1: INTRODUCTION - PREPARATION FOR COMPLIANCE

This chapter introduces the main concepts that underpin this study and provides an overview of the research methods and data collection tools.

### 1. Introduction

Data privacy has become a key concern in the information age. The Internet has made possible the capture and transmission of vast amounts of personal information across the globe in seconds (Pilgrim, 2016). Various legislative regimes exist around the world relating to privacy. 2015 was said to be the year that Asia would reach a turning point with regard to data protection regulation (Parsons & Colegate, 2015). A co-ordinated approach to privacy had not come about by the end of 2016 in the Asia–Pacific region, but developments in China and the Philippines may be seen as a guide to where the other countries may head. Both these countries did implement data privacy and cyber security laws (Schmidt, 2016).

Websites like WikiLeaks, and revelations by people such as Edward Snowden, have raised interest in the concept of privacy for both ordinary citizens and governments. The revelations of WikiLeaks include the way governments have misused their surveillance powers, to the great embarrassment of world leaders (Eger, 2006). Law firm DLA Piper notes that: "Personal information is an increasingly valuable – and increasingly risky – business asset" (DLA Piper, n.d., para. 1). Technology advances have created the need for regulators to implement privacy regimes, but the sheer pace of advances in technology has meant that regulation tends to lag behind the constant evolution and innovation in the technology sector (Wadhwa, 2014).

South Africa has only recently begun to formally safeguard the right to privacy of its citizens, despite privacy having become a constitutional right with the advent of democracy in 1994 (Naude, 2014). This is very necessary in the South African context. In August 2017 a large volume of South Africans personal information was found to have been mishandled and subsequently made public. The breach exposed over thirty million unique identity numbers and other information, there are fears of fraud, identity theft and other crimes taking place as a result this information being exposed (Davies, 2017).

The value of electronic transactions is increasing steadily. Global business to consumer (B2C) e-commerce turnover in 2014 was $1.895 billion which grew to $2.273 billion in 2015 and was forecasted to be $2.671 billion (Abraham & van Welie, 2016). In South Africa the number of online shoppers and their average spend was increasing also. There were estimated to be 6 million online shoppers in 2013 growing to 7.6 million in 2014 and 8.3 million in 2015

spending an average of $139, $148 and $171 in the respective years (Abraham & van Welie, 2016). This increase in transactions leads to greater privacy risks.

This chapter will introduce the research study by discussing the background, purpose, problem statement and methodological approach of the study. Included is the South African privacy landscape, and various existing laws that have a bearing on this and the lead up to the Protection of Personal Information Act no. 4 of 2013.

## 1.1. Background of the study

In the past few years various attempts have been made to legislate the right to privacy in South Africa, as espoused by the Constitution, which is the cornerstone of the new democratic dispensation. Due to other constitutional obligations to which fixed deadlines had been applied, the legislation with regard to privacy protection was not seen as an immediate priority (SALRC, 2005). The low priority afforded to privacy legislation resulted in the Protection of Personal Information Act being passed only in 2013 - a full 19 years after the advent of democracy in South Africa; and even today it has not yet fully come into force. The only section of POPI that has been applied is the appointment of the Information Regulator, who is intended to ensure compliance with the Act. The parliamentary process to appoint an Information Regulator concluded its work in September 2016, was approved by the president in October 2016, and became effective in December of the same year. It is anticipated that delays in commencement of the Act will cause full compliance to be reached only in 2018, considering the grace period of one year granted for organisations to become fully compliant.

## 1.2. Privacy: policy and regulation

Laws relating to regulation of privacy have been in existence for millennia. The Electronic Privacy Information Center (EPIC) suggests that the oldest religious texts of Judaeo-Christianity and Islam make provision for privacy (EPIC, 2002). Since the 1300s the British Justice of the Peace Act has put penalties in place for ‘peeping toms’ and eavesdroppers (Banisar & Davies, 1999). Regulation and laws relating to privacy have become commonplace in recent years.

### 1.2.1. Options for regulation

Three options apply to privacy: regulate, self-regulate or co-regulate. Regulation sometimes grinds to a halt as parties argue over a vigorous legislative response or encouraging self-regulation (Marsh, 2009). The EU is following a third path, one of government and industry participating in a co-regulatory model. This allows for industry to provide input on their complex

workings that may not be fully understood by regulators, and so facilitate responsible and practical regulations (Hirsch, 2011).

### 1.2.2. Privacy in South Africa

There are other Acts that contain elements of privacy in South Africa. The Electronic Communication and Transaction Act no 25 of 2002 (ECT) has elements of privacy and security in relation to E-commerce and other digital methods. The intersection of the POPI and ECT Acts emphasise security and privacy in transactions. A leading technology law practice in South Africa describes the ECT Act as having a bearing on "any form of communication by e-mail, the Internet, SMS etc." (Michalsons Law Firm, 2008, para.2). The Consumer Protection Act, no 68 of 2008 (CPA) bears on elements of data privacy with its opt-out register. This was intended to ensure that a person's details would not be used in marketing campaigns. This is closely linked to the intention of the POPI Act, which allows citizens to prevent themselves from being bothered by those who may have acquired their contact details by illegal or dubious means.

Besides these laws South Africa that contained elements of privacy mentioned above, some organisations, such as the Direct Marketing Association (DMA), have produced regulations for their members, though without stringent sanction for their breach (often these regulations are voluntary). These forms of self-regulation do not, however, offer a sufficient solution for data privacy and protection for individuals. The intention of the POPI Act is to fill this gap in the privacy regulatory regime in South Africa.

Work on comprehensive legislation for data privacy and protection began in 2000. A Draft Bill was included in the report of the South African Law Reform Commission (SALRC) in 2005. POPI was passed and signed into law in 2013, though so far, no commencement date has been set. Various challenges are anticipated in compliance owing to its greater comprehensiveness and rigour than previous legislation and its far-reaching consequences.

As recently as 2012 the South African Department of Communication (DOC) suggested including data privacy legislation in addition to those laid out by the Department of Justice, which championed the POPI Act. This is seen in the DOC's statement of intent gazetted before the policy symposium held in 2012, which was to review ICT policies that had been legislated since the advent of democracy, and how these policies could benefit the country for the next twenty years (RSA, 2012). This suggests that the government is not following a unified process to realise a well-developed privacy protection legislative regime.

### 1.2.3. The Protection of Personal Information Act (POPI Act)

The POPI Act was passed in November 2013. It gives effect to South Africa's constitutional right to privacy as per section 14 of the Bill of Rights (RSA, 1996). Privacy is considered a fundamental human right, and as such, its importance cannot be overstated. The Act provides for a regulatory body to monitor its compliance and enforcement, and to adjudicate in disputes and infringements.

A key area of the Act's provisions are the conditions for lawful processing of information; the majority of articles regarding the POPI Act focus here. These conditions are: accountability, processing limitations, purpose specification, further processing limitation, information quality, openness, security safeguards and participation of data subjects (person who the data pertains to) in the process (RSA, 2013).

### 1.2.4. Opinion of the POPI Act

Several law firms and consultancies have ventured opinions on the preparation for compliance with the POPI Act and its effect. These have appeared mainly in articles on websites advertising their services in terms of the Act, and in online journals and technology sites that have an interest in compliance with the law. The consequences of the POPI Act that have been foreseen include the possibility that current databases of contact information of customers for marketing purposes may become invalid unless specific consent for this purpose has been obtained from the data subject with regard to the appropriate use of their contact details. This has immense implications, particularly for IT professionals, who will need to verify that their organisation is in compliance with the POPI Act. The POPI Act sets a minimum standard for processing of personal data, and is considered "an important legal reform, creating a regime of consumer protection that has become essential to the information age" (Currie, 2010).

The purpose of the POPI Act is to give effect to the constitutional right to privacy; to regulate how personal information is processed; provide rights and recourse in protecting personal information, and to establish mechanisms to enforce these rights. Thus, it must be interpreted in a manner consistent with its purpose as set out in Section one of the POPI Act. On the other hand, it must not interfere with the organisation's rights to exercising or performing any function that is required by any other law with regard to processing personal information; this, too, is stipulated in the Act.

Uncertainty continues regarding the period within which compliance will be required. It is envisioned that there may be different commencement dates for the different provisions of the Act. So far, only the provision related to the creation and appointment of the Information Regulator has commenced.

### 1.3. Preparation to comply with the POPI Act

The main service arising out of the Act appears to be legal firms and consultancies that undertake compliance readiness assessments. Various terms have been coined to denote compliance, such as 'operationalising POPI' (KPMG, 2013). Jacobsen differs with this approach. For him the proper starting point is the database of consumers rather than systems and processes and determining whether consent has been received to use the personal information (Jacobsen, 2013). He describes consent in the Act as "any voluntary, specific and informed expression of will, in terms of which permission is given for the processing of personal information". It is noted that in terms of the Act this information must be gathered directly from the persons (data subjects) whose information is involved.

#### 1.3.1. Trans-border data flows (TBDF)

POPI provisions relating to trans-border data flows are similar to EU legislation. Data flowing to other jurisdictions needs provisions in local law that will guarantee adequate protection. For this, the conditions for lawful processing of information as set out in the Act need to be enforced. In certain instances, a data subject may need to consent to the data being transferred. A clause in the Act specifies that if consent cannot be obtained from the data subject; and that that person may benefit; and that the data subject would be likely to give consent, the transfer of data should be allowed (Dhont & Woodcock, n.d.).

Many of the laws around the world in this regard stipulate that the data may be transferred across borders if the entity receiving the information ensures an equal or higher level of protection as the home country of the subject, or the country from which the data is being transmitted (SALRC, 2009).

Early in the development of the legislation the need for cross-border provisions became apparent, as personal information was not only a domestic policy problem. The two examples below, from the SALRC Data and Privacy report released in 2009, highlight some of the difficulties in government processes, and how trade may be hindered without TBDF provisions.

#### 1.3.1.1. SARS, SAPS and Home Affairs, airlines and foreigners entering South Africa

In preparation for the FIFA Football World Cup, 2010, the South African Department of Home Affairs, in conjunction with The South African Revenue Service (SARS) and South African Police Service (SAPS) wished to prepare for a million visitors expected to attend matches and visit tourist sites. They requested airlines to supply passenger information to the authorities in order to expedite the processing of entry to the country. Airlines headquartered overseas declined the request, as South Africa did not have adequate data protection laws.

#### 1.3.1.2. Corporate need for trans-border data flow legislation

In the second example, Nedbank wished to widen their operations by providing a cost-effective data-processing solution. They intended to process various types of information offshore at a much lower rate than was possible in Europe. The only inhibiting factor was the privacy legislation, which prohibited the information from being transferred offshore without laws guaranteeing its protection. Nedbank thus decided to try to build their data-processing operation in Europe, but it was too expensive, and the venture failed. Had legislation existed for adequate data protection, the venture would probably have flourished (SALRC, 2009).

These examples illustrate the implications of inadequate Data Privacy Legislation for South African entities, and hence the need for effective legislation. The POPI Act makes possible additional business opportunities and more efficiency in government processes, such as border and passport control.

### 1.3.2. POPI Act and direct marketing

Many articles on the subject of direct marketing (DM) in relation to the POPI Act focus on the provision that consumers must opt in for correspondence to continue. DM is communicating, either in person or by some other form of communication in order to offer a service or product, or to solicit a donation of any sort (de Stadler, 2013). Another area is personal information gathered directly from the data subject. These two provisions will present significant challenges in compliance. This aspect will be analysed later in the study in relation to the eight conditions for lawful data processing.

Experts in the legal and DM fields have proposed alterations in the following aspects:

(a) Marketing databases may be invalidated if holders of the information have not received written permission from the data subjects for their contact details to be stored, or if the

holder of the personal information is unable able to prove consent for marketing (Meier, 2014);

(b) The regime for collecting personal information should be Opt-In. This means that subscribers must specifically consent to receive correspondence, or else be considered opted out. All contacts will need to re-subscribe to correspondence that they wish to continue to receive;

(c) Information must be deleted or rendered unidentifiable if the purpose for which it was collected is no longer applicable.

Many commentators have emphasised this need for marketing databases to be made compliant. The process of collecting personal information will certainly need to change (Jacobsen, 2013). Hitherto it has been possible to purchase databases of personal information, but with the promulgation of the POPI Act personal information must be gained directly from the data subject. A procedure for consenting to receive communication needs also to be established. Industries and sectors were examined in this study to assess whether comparable challenges in preparation to comply are to be expected. This data is presented in later chapters.

### 1.3.3. The role of Information Technology professionals

Professionals in the Information Technology industry will inevitably be significantly affected by the POPI Act coming into force. For example, security and database professionals will be obliged to implement changes in processes for data capturing and information retrieval, storage and access. Checks will need to be instituted to determine whether information thus captured may legally be used.

POPI will see the role of IT itself facing substantial changes. It is suggested that the IT team will assume the role of ensuring compliance within the existing "review and audit of current practices" (Moyo, 2013, para.9).

## 1.4. South African legislation and personal data protection

The Promotion of Access to Information Act no. 2 of 2000 (PAIA), deals with freedom of information, but not specifically with data protection. The purpose of this Act is to promote transparency by allowing for the public to request certain information from organisations, including government.

The Electronic Communication and Transaction Act no. 25 of 2002 (ECT) was intended to regulate electronic commerce (e-commerce) and relates only to electronic communication. The

Act is specific to consumers in e-commerce, but no requirements are specified for entities that process data.

The National Credit Act no. 34 of 2005 (NCA) was introduced to provide for a fair consumer credit marketplace, and as such is merely a "general regulation for consumer credit" (Roos, 2007). The NCA caps interest rates on loans to protect borrowers from unscrupulous lenders. The Act is responsible only for consumer information within the credit environment.

The Consumer Protection Act no. 68 of 2008 (CPA) was promulgated to promote fairness in the consumer marketplace. The Act governs return policies of retailers amongst others. The CPA Act also allows for consumers to opt out of marketing correspondence on a central database. Thus, marketers need to check against this database to determine if any of the intended recipients of their correspondence is opted-out, and to ensure that they do not receive the correspondence - unless specifically requested to do so after the opt-out. While it is generally acknowledged that the database ought to operate in this manner and is of obvious benefit to consumers in reducing unsolicited communication, it nonetheless constitutes a significant administrative burden for companies marketing to the public.

Figure 1 below illustrates the different facets of legislation relating to data privacy and protection. The constitutional right to privacy underlies all legislative and self-regulatory initiatives. The provisions of the POPI Act affects self-regulation and also other legislation where personal information is involved.

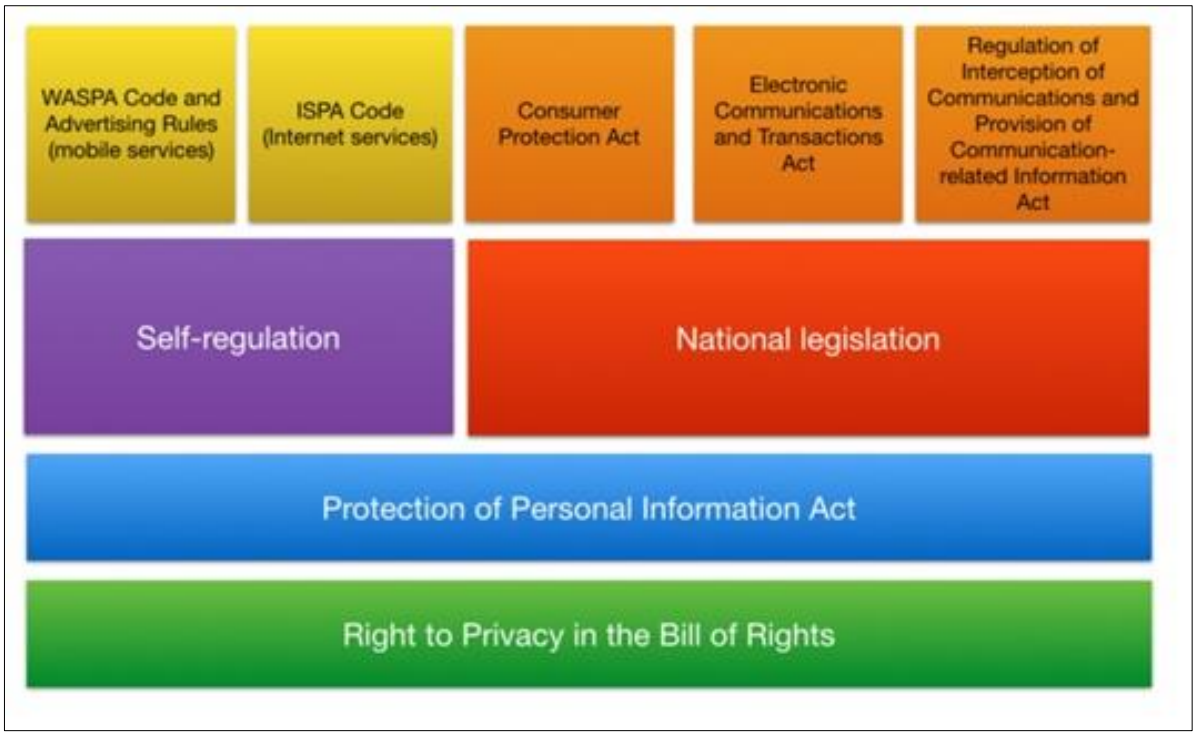


*Figure 1.* Layers of Data Privacy Legislation in South Africa. Reprinted from *Web Tech Law*, P. Jacobsen, 2014, Retrieved from https://webtechlaw.com/2014/01/14/dont-place-too-much-emphasis-on-the-protection-of-personal-information-act/

This figure suggests that the POPI Act underlies various previous initiatives to bring about privacy legislation in South Africa. It is thus an overarching piece of legislation.

### 1.5. South Africa's approach to privacy

In 2000 the SALRC initiated a programme to investigate privacy and data protection. This arose out of a report released by the South African Parliamentary *Ad Hoc* Joint Committee on the Open Democracy Bill (which later became PAIA). This Bill dealt with access to information but did not regulate the right to privacy or other aspects of correctness and control of information. It stemmed directly from the Constitution and had a specified period for promulgation. Due to the tight deadline, only the portion that became PAIA was enacted, and the privacy component was referred to SALRC for further investigation and research (SALRC, 2005). The project produced a report in 2005 containing responses from financial, legal, educational and other institutions. They were responding to the Issue Paper and Discussion Paper that had been released earlier. The draft Bill to regulate privacy and data protection incorporated the feedback received from these papers. This was considered necessary as at the time, the Protection of Information Bill (POI), lacked provisions dealing specifically with

personal information. Amendments legislated in POPI have amended the PAIA, ECT, NCA and CPA Acts.

Besides these particular laws, with their clauses regarding privacy, common law makes similar provisions. The term *actio injuriarium* broadly pertains to right of personality but is limited by the rights of others and the public interest. Privacy is considered a "valuable aspect of personality" (SALRC, 2005, p.iv). *Actio injuriarium* was provided for in Roman law, and this phrase gives the current meaning of privacy (Burchell, 1998): data protection ought to be part of a wider provision to safeguard the individual's constitutional right to privacy. The "interdependency between the common law and constitutional right to privacy" is also noted (SALRC, 2005, p.4).

Burchell (2008) notes that the European Court of Human Rights maintains that telephone calls and e-mails in business fall under 'private life' and 'correspondence', and hence are subject to a 'reasonable expectation' of privacy. The Court maintains further that 'privacy', 'dignity', 'identity' and 'reputation' are facets of personality that need to be protected.

The importance of this legislation is therefore manifest, and, together with the wide-ranging effect of compliance with the Act, the scale of the change in the way personal information is gathered, stored and used can be expected to be little short of dramatic. The implications for all organisations that deal with personal information in whatever context must be expected to be far-reaching, because the information being processed or stored is required to comply with the law once the dates and time period for compliance have been announced.

### 1.6. Case law in South Africa

One of the earliest relevant cases in South African law occurred in the early 1950s. A radio personality was photographed. As a public figure she had consented to this for the publication involved, but not for advertising purposes. The judge ruled that this could be considered an invasion of privacy, citing Voet's Commentary in *Digest* 47.10. He held that the defendant acted "in a manner inconsistent with the decencies of life and in doing so was guilty of an act for which there ought to be a legal remedy" (Burchell, 2008, p.7).

Another case that became known as 'Bogoshi': National Media v Bogoshi in 1998. The Supreme Court of Appeal has stated that the rights of an individual are to be balanced with press freedom, and that this is directly transferable to privacy (Hughes, 2014).

More recently, the judgement in Grütter v Lombard and Another refers to Professor McQuoid-Mason, who describes a violation of privacy in this case as:

> …the appropriation of a person's image or likeness (the same must apply to other features of identity) as 'a violation of a person's right to decide for herself who should have access to her image and likeness – something that goes to the root of individual autonomy or privacy' (SAFLII, 2007, p.6).

While case law has upheld the right to privacy, there are, clearly, grounds for formal privacy laws; and the POPI Act provides specific provisions for rulings with regard to the current information era.

Besides common law, the very Constitution upholds individuals' right to privacy. The relevant provision is that of the right to retain control over their personal information (Roos, 2007). Although the individual has recourse in law regarding infringement of their rights when his/her information is processed, there is no case law with specific findings based on data protection or data privacy. This lack in the legislation is remedied in the POPI Act with its provision for sanction.

### 1.7. Research problem

In many societies breach of privacy is understood variously as an invasion of the individual whose information is exposed, or as pro-transparency if a government (or individuals) misdemeanour is uncovered. With the dramatic increase of electronic communication and social networking violations of privacy are more prevalent. "In the last 15 years privacy regulations have had to evolve quickly to address operational and lifestyle changes brought forth by technology" (Leizerov, 2013, p.4).

While the POPI Act has been in the public domain for several years, little is known about what measures should be in place or what steps are needed in order to prepare to comply. Several sources suggest that, South African companies are generally poorly prepared for compliance, as cited by the consultancy Grant Thornton (Kolver, 2014). Several other consultancies and law firms have similarly offered readiness assessments that focus mostly on audits of systems and processes that collect, process and use personal information. This study assesses three areas: the factors pertinent to preparation for compliance and their affect in respect to the organisation, staff and the anticipated cost in preparation for compliance.

The work of IT professionals involves analysing and overseeing input of various types of information, much of it personal information. This information is sought-after for the purpose of DM. The challenge for the DM sector will lie in demarcating and coding acquired

information to verify the consent of the individuals concerned, and the legality of marketing to them. A major concern is the process of using personal information for purposes other than what it was initially supplied for – hitherto accepted as normal, acceptable practice. Retention of personal information, often kept for many years (and often unused), often becomes outdated. This, too, is clearly also a matter of concern.

The research problem is framed as the lack of a deep understanding of those factors pertinent to the preparation for compliance with the POPI Act and their effect on the organisation, staff and the cost anticipated in preparation.

## 1.8. Purpose statement

Preparation to comply with the Act will be the task of many organisations that process personal information and will involve several kinds of changes in their internal and external processes. The Act regulates the collection, storage, retrieval and usage of information. This study will serve as a guide to preparation for compliance with the POPI Act due to the current lack of available resources, by identifying the pertinent factors in preparation for compliance and their effect on the organisation, staff and the cost anticipated in compliance.

## 1.9. Research question

**Research Question:** What are the pertinent factors in preparation for compliance with the POPI Act and what is their effect?

1. What factors are pertinent to the **organisation** and what is their effect?

2. What factors are pertinent to **staff** and what is their effect?

3. What **costs** are anticipated in preparation for compliance and what is their effect?

## 1.10. Approach to the study

This section introduces the research approach, the type of research carried out and the research methodology.

### 1.10.1. Methodological approach

The research was undertaken with qualitative methods, thus allowing for effective capturing of concepts from the various sources to inform the study. Quantitative research does not allow for the same insights to be drawn from these sources.

This research is an exploratory study, and areas for further research are highlighted. Exploratory research is not required to be as formally rigorous as other types; an advantage,

considering the newness of the field in the South African context. Exploratory research is described as a foundation for future studies on a given subject. It can be undertaken for two main areas, namely, studies of a new subject, or new angle of an established research topic (Kowalczyk, 2015). Constructivism says that reality depends on the individual (Guba & Lincoln, 1989). In this research the constructs are based on the belief of the interviewees, and this is based on their experience and knowledge of various factors which shape their perspective. So too, the researcher uses their view of reality and background to analyse the responses.

### 1.10.2. Data collection

Data collection was conducted by means of formal semi-structured interviews. Structured collection methods lack the flexibility required to probe specific responses and were thus not suitable for this study. An example of structured responses is found in surveys being used as a research tool, where the response cannot be illuminated any further by questioning on the responses that arise. This process of drilling into responses is a key characteristic of semi-structured interviews. Thus, other aspects not directly related to the immediate research questions can emerge.

## 1.11. Chapter structure

*Chapter Two:* literature review that discusses privacy: its history and definitions; its relation to policy and regulation; the effect of technology from written records to contemporary electronic systems on privacy; the effect of social media; background to the field of compliance, and various theoretical frameworks that underpin the study.

*Chapter Three*: a detailed view of the research methods (qualitative and constructivism), and the tools used to gather data (formal semi-structured interviews).

*Chapter Four:* the data collected to answer the research question and sub questions is presented. This has three parts derived directly from the research questions posed by the study: factors pertinent in preparation for compliance and their effect on the organisation; staff and the cost of preparation for compliance.

*Chapter Five:* an analysis of the data collected and key areas arising from this. As with Chapter Four the chapter structure mirrors the research questions.

*Chapter Six:* this concludes the study, summarizing its various aspects, the main findings, and recommendations for further research.

## 1.12. Conclusion

The concept of privacy is not new, as it dates back to the oldest religious texts. Three models for privacy regulation exist: regulation, self-regulation and co-regulation. In South Africa the POPI Act was passed to give effect the constitutional right to privacy. Complying with the conditions specified by the POPI Act will possibly radically affect the processing of personal data and how collection, storage, transmission and access to information collected from individuals is undertaken. This study assesses three aspects: pertinent factors to preparation for compliance with the POPI Act and their effect on organisations, staff and the anticipated cost.

This chapter has presented an overview of the study, its main elements and some of the relevant background that aids this study. Chapter 2 will present literature on privacy, technology (particularly the Internet), compliance, cost of compliance and theoretical frameworks that underpin this study.

## CHAPTER 2: PRESENTATION OF RELEVANT LITERATURE

Chapter two reviews the literature relating to privacy, technology and security with a particular focus on the Internet, the field of compliance and concludes with the analytical framework adopted for this study. Taylor (n.d.) suggests that a literature review should convey both what is known about a subject and the established thinking on it.

### 2. Introduction

This study pertains to preparation for organisational compliance with the POPI Act. Four main areas are considered in this literature review: the conceptual foundation of privacy; the effect of an evolving technology landscape on privacy; a background to the compliance function, and the analytical frameworks that underlie these concepts.

A concept map is presented in Figure 2 to illustrate the relationship between the concepts:

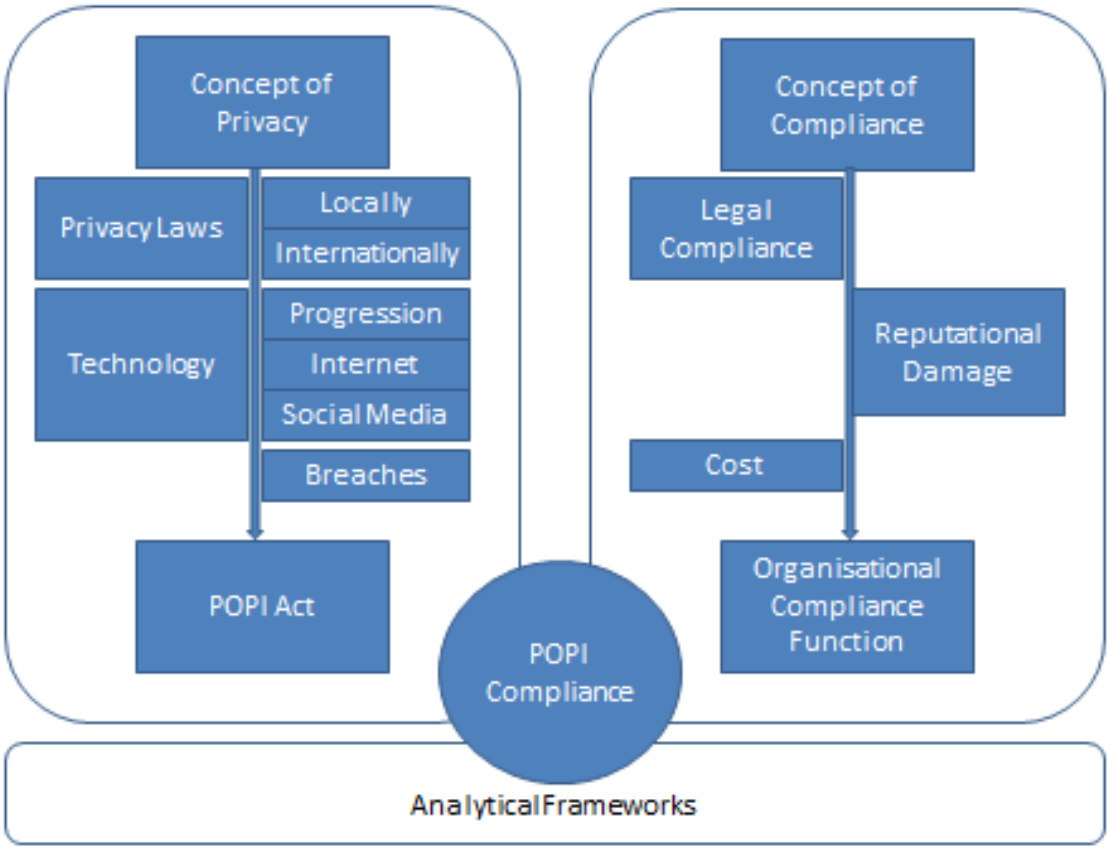


*Figure 2.* Concept map of Chapter Two – Literature Review. Source (Researcher, 2018).

## 2.1. What is privacy?

Literature pertaining to the field of privacy is presented, including the definition of privacy, types of privacy, privacy laws and sanction for privacy breaches. The concept of privacy can be described as a theory that takes into account various daily decisions about what information we make available to others about ourselves and what we do not want to share (Petronio, 2015). It is suggested that the need for privacy is fundamental to human beings (Neethling, Potgieter & Visser, 1996). Doubts exist as to whether privacy will ever be comprehensively defined: "Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all" (Post, 2001, p.2087). Posner (1981, p.405) notes three senses in which privacy is used. These are "concealment of information", "peace and quiet" and a "synonym for freedom and autonomy".

### 2.1.1. Definitions of privacy

With these difficulties in definition, the concept of privacy is expressed in a range from simple definitions, such as that espoused by Warren and Brandeis (1890, p.193): the "right to be let alone" to those more complex. Privacy might be defined from research on interaction of people in person in public places. Walking on sidewalks is used as an analogy where no formal rights or laws exist, but commonly accepted ground rules govern interaction in these public areas (Samarajiva, 2001).

Thus, while a comprehensive definition of privacy has been sought as far back as that quoted from 1890, there is still no complete, universally accepted definition (Foord, 2000). McCarthy (2005, p.479) goes further to state:

> It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.

What cannot be defined can often be described, as Privacy International has done. They consider the main features to be information privacy, bodily privacy, privacy of communications and territorial privacy (Banisar & Davies, 1999). The Australian Law Reform Commission notes that "the issues…do not fall neatly into one concept" (Australian Law Reform Commission [ALRC], n.d., para.6). Standler (1997) describes privacy as being an

‘emerging right’. He notes that examples are listed in discussions of where recognition of the right has taken place, rather than a definition as such; this usually takes place in two streams, namely, the “nature of the right and the source of the right”.

The South African Constitution enshrines the right to privacy in section 14 of the Bill of Rights, considering it “fundamental”, thus emphasising its importance. Common law also makes provision for privacy, and the term *actio injuriarium* broadly pertains to right of personality, though it is limited by rights of others and the public interest (Etzioni, 1999). The Constitutional Court noted (Bernstein vs Bester) that privacy is “amorphous and elusive”, yet went on to suggest a definition:

> …an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders, and in respect of which he has the will that they be kept private (Ncube, 2004, p.3).

Privacy is also said to be a “valuable aspect of personality” (SALRC, 2005). From all these varying definitions it can be seen that, while a definitive definition has been sought, none has been determined or generally accepted.

In many societies privacy is enshrined as a constitutional right and reflected in a number of laws to give effect to it.

> Privacy is an important right because it is a necessary condition for other rights such as freedom and personal autonomy. There is thus a relationship between privacy, freedom and human dignity. Respecting a person's privacy is to acknowledge such a person's right to freedom and to recognize that individual as an autonomous human being (Britz, 1996, para.8).

However, despite its importance and its place in underpinning other fundamental rights, it cannot be considered an absolute right. An example is surveillance by police or other state security apparatus in pursuit of crime intelligence and suspects (Britz, 1996). Privacy is thus limited by other rights.

For the purpose of this research, privacy is considered to be “controlling access to personal information” (Agre & Rotenberg, 1997, p.1).

### 2.1.2. Types of privacy

There are four types of privacy: information privacy, bodily privacy, communication privacy and territorial privacy. These are discussed below.

#### 2.1.2.1. Information privacy

Information privacy, also known as data privacy, is closely related to the individual, and implies that personal information should not be accessible to others against his/her will or without their express consent. The individual must be fully informed about the purpose that this information will be used for, and that she/he will be able to exercise control over this information. Clarke (2013, para.13) states: “it is useful to use the term 'information privacy' to refer to the combination of communications privacy and data privacy”.

Other sources suggest that information privacy refers to an ever-changing association that links technology and the legal aspects of privacy, specifically in the collection and distribution of information. This is closely related to the electronic or digital storage of this information (Banisar & Davies, 1999).

Westin (1967, p.7) summarises the general view of data protection as “the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others”. Legislation relating to data protection is said to be based on a “common set of fair information usage principles” (Bennet, 1992, p.95).

Privacy Rights Clearinghouse (2002) notes a number of areas where information privacy is key. For example, it is imperative that certain financial information be kept out of the public domain. People considered to be wealthy often do not want the extent of their wealth to be widely known for the sake of reduced risk of crime against them. Privacy of health information is vital in order to minimise the stigma attached to certain illnesses, among other considerations. The health sector has traditionally had strict privacy regarding patient-doctor confidentiality, a fundamental of medical ethics that may conflict with the law (Schleiter, 2009).

#### 2.1.2.2. Bodily privacy

Bodily privacy, formally known as privacy of the person is related to forced searches, immunisations, blood transfusions and as general protection against invasive procedures (Clark, 2013; Banisar & Davies, 1999).

Sivaranjani and Suganthi (2014) suggest a type of personal privacy where persons are vigilant of what they expose regarding their bodies, a type of personal modesty. Other aspects of personal privacy include physical barriers or:

> erection of walls, fences, screens, use of cathedral glass, partitions, by maintaining a distance, beside other ways. People who go to those lengths expect that their privacy will be respected by others. At the same time, people are prepared to expose themselves in acts of physical intimacy, but these are confined to exposure in circumstances and of persons of their choosing. Even a discussion of those circumstances is regarded as intrusive and typically unwelcome (Abuor, 2016, p.22).

In physical intimacy people are willing to be exposed, but the circumstances and the person/people they are exposed to are chosen. Even for this to be discussed may be regarded as "intrusive and typically unwelcome" (Sivaranjani & Suganthi, 2014, p.166). In the South African context, a major type of personal privacy would be preventing access to persons unauthorised from entering your home, work or place of worship and the vehicles we drive. Included with this is prevention of smash-and-grabs and hijackings (Roebuck, 2011).

Medical information is also included under the banner of information privacy, though it, too, can be considered a subset of personal or bodily privacy, as this also includes the right to make decisions regarding medical treatment without outside interference from the government or other parties (Roebuck, 2011).

The notion of privacy, according to Exploring Constitutional Conflicts by the University of Missouri, led to legalising of contraception in 1965, when a law banning the sale of contraception to married couples was struck down. Consequently women's bodily privacy rights were extended to legalise abortion in *Roe vs Wade* (1972), and more recently (2003) rights were also extended to men's choices as sodomy laws in Texas were deemed by the Supreme Court to be a violation of liberty (Linder, 2016).

#### 2.1.2.3. Communication privacy

The essence of this is that communication between individuals or organisations, in any type of medium (i.e. landline or mobile phones and devices, facsimile, social media, email etc.), are not scrutinised on a regular continual basis (Clarke, 2013). It is a matter of security in communication.

#### 2.1.2.4. Territorial privacy

This is concerned with the limiting of invasion into domestic and areas such as the workplace or other public areas. The Australian Government's Law Reform Commission details this as: "includes searches, video surveillance and ID checks" (ALRC, n.d., para.5).

### 2.1.3. Threats to privacy

Three main threats to privacy are noted: globalisation, convergence and multi-media. Globalisation is aided by the prevalence of the Internet across most parts of the world, allowing for information to be dispersed widely and quickly. Convergence removes technology barriers and allows different systems to interact with each other, so that information interchanges seamlessly. Multimedia allows data to be transformed into various forms and states for transmission and consumption (Banisar & Davies, 1999).

Another area of concern is government surveillance, as pointed out by, among others, Edward Snowden, who publicised the US government's PRISM program, and how this undermined individuals' privacy by the National Security Agency (NSA). This body connected directly to the servers of big technology companies; in doing so they bypassed privacy controls and whatever encryption may have been in place (Lyon, 2014).

In South Africa the Police Service (SAPS) seized a device known as a 'Grabber' in a sting operation. This device was said to have been obtained illegally with a fraudulent letter approving its purchase by the President, the only person able to authorise this kind of surveillance equipment purchase. The device could track and monitor up to 10000 mobile phone numbers at a time (Wakefield, 2015).

### 2.1.4. Security concerns

Two security concerns are mentioned in the information age: data protection and security of payment transactions. Legislation for protection of data was created early in the technological age, yet it is too early to determine its effectiveness, as breaches are often made public, and loss or theft of information and its general misuse come to light at regular intervals. Financial payments on electronic platforms are also a cause of anxiety for consumers (Mitchell, 2001).

### 2.1.5. History of privacy legislation

In the 1960s concern over information protection increased with the advent of 'modern' technology (Solove, 2006). The need for information privacy became more evident and began to be seen as vital. An effective level of information security and privacy became a key requirement for participation in the global economy, as information could now be spread more quickly and easily to any part of the world. World powers attempted as far as possible to protect their citizens' information from abuse and to protect their privacy (SALRC, 2005).

The history of privacy goes back further than the advent of technology. The earliest privacy law can be traced back to 1361, under which peeping toms and eavesdroppers could be arrested under the Justices of the Peace Act of 1361 in England. In 1765, when a warrant to enter a house in order to seize papers was struck down, Lord Camden is reputed to have asserted:

> We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have (Kurland & Lerner, 1987, para.6).

In another instance the British Parliamentarian, William Pitt, said in 1763 that:

> The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow though it; the storms may enter; the rain may enter, but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement (Hafetz, 2002, p.175).

In Sweden the Access to Public Records Act was passed in 1776, which required that all information held by government be used for legitimate purposes. France also enacted privacy legislation in 1792 - the Declaration of the Rights of Man and the Citizen (Banisar & Davies, 1999). In the United States Warren and Brandeis (1890) wrote an article in the Harvard Law Review regarding the Right to Privacy, which became decisive in the upholding of privacy rights.

The earliest international regulation regarding privacy can be found in the Universal Declaration of Human Rights of 1948, ratified in December 1949. Article 12 of this declaration reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (United Nations, 2015, p.26).

Modern legislation pertaining to protection of information came into being in the 1970s. Two pieces of legislation from the early 1980s were the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), and the Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Trans-Border Data Flows of Personal Data (1981). These continue to form the cornerstone of many laws on the subject.

At present over fifty countries have introduced similar legislation to safeguard personal information, and these are based largely on the principles of data protection contained in the OECD Guideline.

#### 2.1.5.1. International data protection and privacy

In the 1980s protection of personal information became an international issue. The world, now a 'global market', saw increases in transmission of information across national borders. This became known as "trans-border data flows, or TBDF" (Roos, 2007). The response by international organisations was to synchronise legislation among as many countries as possible. The aim was to make entities (businesses or individuals) in any particular country receiving data accountable to the laws of the country from which it originated, while still allowing for the free flow of information and uninhibited trade.

SALRC noted that foreign jurisdictions with 'access to information' legislation had instituted separate legislation regarding privacy and data protection (SALRC, 2005). Analysis of the legislation of various countries shows a key common goal: a standard for protection of personal data while maintaining free flow of information across borders (Roos, 2007).

In Europe data privacy is considered a human right, but not so in the US, where the view is that the industry should self-regulate the management of data. A system of 'safe harbours' was instituted for this purpose (Currie, 2010). Currie also maintains that specific legislation is preferable to allowing exceptions, as safe harbours do.

The US attempted to implement privacy regulation by the use of codes to lay down standards for using personal data. The Advisory Committee of the Federal Department of Health, Education and Welfare was among the first to use a code to regulate information practices in 1973 to address the lack of legal protection (Dixon, 2008). They sought what they termed a 'set of norms' that should be heeded by organizations collecting data (McFarland, 2012). Some of the provisions were that data should not be collected secretly; that individuals had the right to know what information about them was able to be collected; that this collection of data had

to be necessary, and to ensure that the information was used for only the specific purpose it had been collected for. This set of codes was the foundation for the Privacy Act of 1974. This is Federal and not state law, and thus has jurisdiction throughout the country. Under this Act rules were established to govern "the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies" (United States Department of Justice, n.d.,para.1). Furthermore, the government was bound to follow fair information practices. These two instruments – the codes and the Privacy Act - have influenced many countries and have become a kind of basic standard for fairness of information practices in both public and private sectors (Richards, 2005). It is important to note that the US Constitution does not mention privacy or the right thereto. However, sections of the Bill of Rights are interpreted as allowing for a right to privacy or guarantees of specific aspects of privacy (Linder, 2016).

In Europe a case regarding the 'right to be forgotten' was heard in 2014. Google Inc had been taken to court to remove search results of a person whose impaired financial history was accessible on the Internet, stemming from repossession of a property in the past. This matter was referred to the European Court by the Spanish court where the case was heard and ruled that under certain circumstances search engines are the custodians of personal information, and in this case, Google was to delete from search results the information deemed irrelevant, but this did not change the underlying source (Heywood, 2014).

#### 2.1.5.2. The General Data Protection Regulation (GDPR) in the EU

The GDPR was passed in 2016 and expected to be enforced from 2018. The GDPR is not a new piece of legislation, but an update of the previous privacy law repealing Directive 95/46/EC. The regulation is applicable to the European Union and those who wish to trade in the EU. The GDPR applies to storage, processing and sharing personal information of EU citizens (Lovatt, 2016).

### 2.1.6. Privacy: legislative differences

Analysis of the legislation of foreign countries reveals two key goals: a standard for protection of personal data and balancing that with the need for free-flowing information across borders (Roos, 2007). Shaffer (2000) refers to a tension between regulatory regimes and liberal trade agreements, where the EU and US are in conflict. This has led to mutual agreements to cater for specific purposes beyond the boundaries of the regulations, thus allowing trade to be

unaffected by the regulations. Elsewhere he suggests that this tension might be expected to cause the US to increase its data privacy protection for "greater social protection" as a result of foreign regulatory requirements.

### 2.1.7. Privacy breaches and sanction

A privacy breach is a violation of privacy regulation or law that leads to unauthorised access of personal information (Backman & Levin, 2011). According to Armerding (2018) the biggest data breach was against technology giant Yahoo Inc who had names, email addresses, dates of birth, password and security questions of three billion user accounts compromised.

Sanctions for privacy breaches often include a fine or jail term, depending on the laws under which the breach is prosecuted and the country in question. Often remedial action is undertaken before a fine or imprisonment is instituted; this is also determined by the severity of the infringement and whether it was first-time or repeat.

## 2.2. Progression of technology and communication

Progression of technology and communication goes as far back as the first writing and drawings from prehistoric days, beginning with rock paintings, with ink made from berries and pens; to brushes made from roots and twigs; the papyrus scrolls in ancient Egypt; the earliest paper as we know it from China in 105 AD (Smith, 1973). There has been much progression to the electronic systems that we know today. Some of the steps on the way include the printing press and photo engraving. Even photography has evolved in many ways (Miller, 1998). Telephonic communication was invented by Alexander Graham Bell in the 1870's. Bell invented the telephone by chance as he experimented in bettering the limit of a single message at a time via telegram, these original telephone systems progressed to mobile phones. Mobile phones have the ability to access the Internet, email and a variety of applications (Henderson, n.d.). This prevalence in society has led to many breaches of privacy.

### 2.2.1. Advent of the Internet

In 1962 a Massachusetts Institute of Technology (MIT) and Advanced Research Projects Agency (ARPA) scientist, Licklider, created the conceptual framework for a "Galactic Network", which would connect computers to each other all over the world (Licklider & Clark, 1962). In 1965 a packet switching solution from one computer to another was developed at

MIT. By 1969 information could be exchanged between different computers - these were between University of California Los Angeles (UCLA) and Stanford University. This form of communication became known as node-to-node (Graziani, 2012).

The Internet is governed by a number of organisations which adjudicate issues relating to domain names, protocols and standards related to the smooth running of the Internet. Domain names are managed by the Internet Corporation for Assigned Names and Numbers (ICANN) (Masters, 2014). A number of technologies underlie the Internet. Hyper Text Transfer Protocol (HTTP) caters for the hosting of information on the Internet. This Hyper Text is encoded into web pages in the form of Hyper Text Mark-up Language (HTML) that is transmitted on HTTP (Marshall, 2012).

The 'network effect', an economic concept, can be seen in the adoption of Internet technology as well, especially mobile telecommunication. The theory of the network effect is that the more people on a particular network or service, the higher the value per user. If, for example, a single user belongs to a network, there is no value in this; however, if another user joins, the value is increased to both of them. If a hundred people join, the value grows exponentially. Liebowitz and Margolis (1994, p.131) define the network effect as:

> …a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes. As fax machines increase in popularity, for example, your fax machine becomes increasingly valuable, since you will have greater use for it.

In Africa there are fewer than 331 million Internet users (Internet World Stats, 2015) in a population of a billion (Bish, 2016). Take-up of the Internet has been slow, though growing rapidly on mobile devices. Sub-Saharan African countries are expected to have a mobile penetration rate of over a hundred percent by 2021, although this is due to multi-SIM ownership, often across different networks for better rates (Ericsson, 2015).

In this context protecting electronic resources has become vital. Industrial espionage is rife as trade secrets are sought by competitors, so protecting data is key to maintaining competitive advantage, and, ultimately, staying in business (Mahoney, 2014). Theft of individuals' personal information, such as ID number – so-called "identity theft" - has become rampant. Using a person's personal information makes it possible to unlock much of his/her material possessions and can easily lead to financial and/or reputational harm (Britnell, 2008).

### 2.2.2. Social media

Two articles in Adnews document the history of social media. The first begins in 1978 and the second in 1969. While different in focus, they provide a very detailed picture of social media platforms (Glenn, 2012; Bennett, 2013). Hendriks (2013) suggests that social media goes back to 550 BC, when the first postal service began operation. In 1792 Telegrams proved to be a quicker method of communicating short messages that arrived faster than a horse and rider. In 2006 the major social networks became available to the public as Facebook and Twitter. It is also noted that "there were also other avenues for social interaction long before the Internet exploded onto the mainstream consciousness" (Shah, 2016, para.6).

Today it is estimated that there are thousands of social media platforms, with different purposes, yet serving one overall purpose. Some have millions of users; others only a handful. Social media remains driven by human nature, as social beings seek an ever-greater ability to communicate by appropriate means as technology evolves (Hale, 2015).

Social networking may be used to locate and reacquaint old friends, roommates, previous employers and significant others, but questions need to be asked about others who might gain access to this information - "identity thieves, scam artists, debt collectors, stalkers, and corporations looking for a market advantage are using social networks to gather information about consumers" (Privacy Rights Clearinghouse, 2016, para.3) - and whether they might use it for ulterior purposes.

Articles suggest that Social Media may play a role in the appointment process of a potential employee as employers may use social media to get to know a candidate better; thus, posts and pictures that may jeopardize future employment should be limited or made private (Cain, 2016). A Market Watch article notes a quote by the Chief Executive of Social Intelligence – Max Druker "Almost all employers do some form of background screening because they have to avoid negligent hiring. An employer has an obligation to make the best effort to protect their employees and customers when they hire" (Waters, 2011, para.2). This highlights the importance of one's social media profile to future employers.

Laws in some US states have begun to allow for disciplining employees for activities on social media should this be deemed to bring the company into disrepute (Privacy Rights Clearinghouse, 2016). Two South African judges who had this communication on Social Media platforms recently came to light. The first instance was a conversation on instant messaging platform WhatsApp, which was aired at that judge's interview for a role in a higher court

(Narsee, 2016). The other was of a private message on Facebook which was said to be racist, and unbecoming of a sitting judge (Jordaan, 2016). In another incident an estate agent was fined R150 000 for posting on social media a racially disparaging comment on social media about beach-goers in the holiday season (Wicks & Areff, 2016). While social media is becoming more prevalent in society there are privacy risks to contend with especially identity theft and the possibility of malware being transmitted and data stolen from devices (laptops, tablets and mobile phones) (Cohen, 2017).

### 2.2.3. Privacy risks due to technology progression

Technology has progressed and continues to progress to new levels of functionality and portability. An original computer used to fit in a room; and now its equivalent in computing power can be carried in your hand. Contemporary devices include cell phones, tablets and laptops; many people own these or combinations of all three, and thus technology is more and more intrusive in our lives. For convenience these devices are used to store various personal information such as contact details, ID numbers, and even bank account details. One's location can be tracked. Anecdotally it is said that your mobile device may know more about you than your close friends (Myhre, 2013). van den Hoven, Blaauw, Pieters and Warnier (2014, para.1) summarize the threat facing privacy in light of technology: "recent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data". Kroi (2017, para.1) goes further to relate this to personal information, and suggests that with technology developing it requires legislators, organisations and ordinary citizens to protect their data, and that "data protection goes hand-in-hand with cyber security".

## 2.3. What is compliance?

Compliance will be discussed: its definition and history, compliance in relation to laws and regulations and function within organisations. Compliance is seen as "an organisation's adherence to laws, regulations, guidelines, and specifications relevant to its business, in order to minimize risk and improve effectiveness in business operations" (Southekal, 2017, p.199) These are not profit generating activities (Kroi, 2016). Compliance is measures that are instituted by an organisation to meet requirements thrust upon them by laws, regulation or industry bodies that they may belong to These reduce the risk that stems from these laws, and could result in improvements in business operations effectiveness, but have no effect on profit

and (in many instances) cost to implement. A formal definition is said to be "being in accordance with established guidelines, specifications, or legislation, or the process of becoming so" (Buecker, Amado, Druker & Lorenz et el, 2010, p.417).

### 2.3.1. History of compliance

Adam's bite of the forbidden fruit could be seen as the first compliance violation with contemporary compliance programs being "traced back to the turn of the 20th century, when public safety agencies began to emerge. The Food and Drug Administration, for example, was created in 1906" (MacKessy, 2010, para.7). The field has grown significantly since then, and compliance is now estimated to be a $100-billion industry for global banks (McDowell, 2017).

### 2.3.2. Legal compliance

Compliance is common to all persons in some way or form. Compliance to road rules affect all who use the roads (Tabibi, Grayeli & Abdekhodaei, 2016), and these rules increase road safety when they are enforced and adhered to (Smith, 2015). In South Africa these road regulations fall within the ambit of the National Road Traffic Act no. 93 of 1996. When selling or purchasing a property various compliance certificates are required in terms of various laws and regulations: these include electrical certificate of compliance in order to comply with the Electrical Installation Regulation (RSA, 2009), a gas certificate of conformity to comply with the Pressure Equipment Regulation (RSA, 2015) and an electric fence system compliance certificate to comply with The Electrical Machinery Regulations (RSA, 2005).

### 2.3.3. Compliance within the organisation

Compliance comprises activities within the organisation that do not generate profit and are said to bother clients with the need to return documents to prove particular personal details. It is expected that breaches in compliance will lead to some form of sanction and reputational damage, thus having an economic effect on the organisation when publicised (Kroi, 2016). Organisations continually struggle to be in compliance with the burden of numerous laws and regulatory complexity increasing (MacKessy, 2010).

Many organisations opt for an internal compliance function to manage efforts to ensure that staff do not breach any laws or regulations (Miller, 2014). Internal controls are said to be espoused in the concept of Three Lines of Defence. These are, firstly, leaders of divisions and departments within the organisation; secondly, staff responsible for compliance of the

organisation, and, lastly, the internal audit function, who should verify compliance as a last line of defence (Miller, 2014). The cost of compliance is exorbitant and said to increase between 15%-25% annually. It forces banks to hire 100s or even 1000s of risk and compliance professionals (McDowell, 2017).

Literature suggests that compliance management should be seen as a program and not a project. The implication of this is that it is an ongoing process, and not a once-off fixed-term intervention (Bace, Rozwell, Feiman & Kirwin, 2006). This is critical to the success of a compliance intervention in the medium to longer term.

### 2.3.4. Reputational damage

Each breach or violation of compliance is a breach of a particular law or regulation which carries a specific sanction or penalty. This being exposed and publicised by a breach notification or similar means may result in reputational damage (Kroi, 2016). This could result in financial loss with great implications (Farha, Sekeris & Hermansson, 2017). Reputational damage has the effect of reducing the client base. The consequent loss of income might be so severe as to threaten the continuation of the organisation.

### 2.3.5. Cost of compliance

Literature suggests that it is possible to control compliance costs. This can be achieved by deliberate interventions to eliminate overlap of requirements, and likewise unnecessary complexity where possible (Bace et al, 2006). It has been estimated that a company that seeks individual solutions for each regulatory requirement might ultimately spend ten times more in IT costs compared with having an integrated compliance approach. The effect might be felt even in otherwise well-run organisations. A survey showed that financial management compliance systems cost up to 15% of IT operating budgets (Bace et al, 2006).

### 2.3.6. Corporate and data governance

Corporate governance is said to be the framework within which organizations are controlled and directed (South African Institute of Chartered Accountants [SAICA], n.d. a). In South Africa the King code of governance is said to be the institutionalisation of corporate governance (Walker, Ramashia & Rambau, 2013). Roe (2017) defines data governance as practises and processes that are used in the management of information in an organisation. This

is to get greater control of data assets with governance of methods, technologies and behaviours inclusive of security and privacy amongst others.

### 2.3.7. Organisational theory

Classical organisational theory is said to include three approaches (FAO, n.d. a). Firstly, the scientific management approach. Allowing for an increase in productivity where workers and managers have mutual trust with this leading to "planning of work to achieve efficiency, standardization, specialization" (Taylor, 1947). Secondly Weber's bureaucratic approach that suggests that the organisation is part of larger society where there is a structure, has specialisation, is predictable and stable, is seen to be rational and democratic. Thirdly the administrative theory based on a number of management principles such as discipline, unity of command and direction, subordination of the interests of the individual and personnel who are remunerated amongst other principles (FAO, n.d. a).

## 2.4. Analytical framework

According to Coral and Bokelmann (2017) no single definition of an analytical framework has been universally agreed upon. Ostrom (2009, p.419) proposed this: "the construction and use of a general framework could help to identify the elements a study is to consider, as well as the relationship of these elements to one another".

Literature has varying views on use of frameworks. The following two quotes highlight the extreme views held on the subject. The first is in favour – "I can't shake off the feeling that if I don't present formal theory, somehow my knowledge claims will be suspect" (Ellis, 2004, p.18). The second view seems to suggest that a framework would not be compulsory but generated from the research undertaken:

> Theory also appears as an end product of a qualitative study, a generated theory, a pattern, or a generalization that emerges inductively from data collection and analysis. Grounded theorists, for example, generate a theory grounded in the views of participants and place it as the conclusion of their studies. Some qualitative studies do not include an explicit theory and present descriptive research of the central phenomenon (Creswell, 2003, p.140).

The Researcher believes that using a framework for this research will serve to embed the research in theory' giving it additional credibility and standing. Several analytical frameworks were considered for use in this study. These are detailed below:

### 2.4.1. Framework analysis

Framework Analysis is a "qualitative methodology for applied policy research" (Srivastava & Thomson, 2009, p.72). This framework is suitable when the following four criteria are met: the research has a specific question; a fixed time period; sampling was designed beforehand, and with "priori issues". There are five steps in the framework analysis approach: "familiarization; identifying a thematic framework; indexing; charting; and mapping and interpretation" (Shrivastava & Thomson, 2009, p.75). This method has merit when information is acquired from people who are affected by the policy.

### 2.4.2. DG Markt Guide to Evaluating Legislation

Evaluation of policies and legislation is an emerging field that is gaining prominence as the need for better regulation grows (Stengg, Fitzpatrick, Pillar & Pocztowska, 2008). In order to determine the effectiveness of legislation - either previously or currently an "evidence-based assessment" is carried out (Stengg et al, 2008, p.6). This evaluation asks four questions: what has changed, and was it intended? Why is this so and what is it due to? Is the situation better, worse or unchanged? Who are the affected parties?

An evaluation should cover the "adoption, implementation and impacts" of the legislation. It should assess whether the legislation achieved what was expected since its adoption, and whether other consequences may have resulted. In this way it would be possible to determine how well the targets of the legislation have been met, whether positive or negative. (Stengg et al, 2008). This is the compliance phase.

There are seven elements of the evaluation mandate: the intervention logic; evaluation questions; data sources; stakeholders and steering group; timing; deadlines and expected outputs; quality criteria, and technical specifications (Stengg et al, 2008).

### 2.4.3. OECD Regulatory Compliance Cost Assessment (CCA) Guide

"The term 'regulatory costs' as used by the OECD embraces all of the costs attributable to the adoption of a regulatory requirement" (OECD, 2014, p.1). OECD countries are looking to make a more business friendly regulatory environment by reducing regulatory costs. While this occurs regulatory action to meet various social and economic imperatives is continually increasing. Governments are needing to be wise in their regulatory choices that are cost effective (OECD, 2014). Hence the CCA guide was instituted. The following figure details the categories of the CCA:

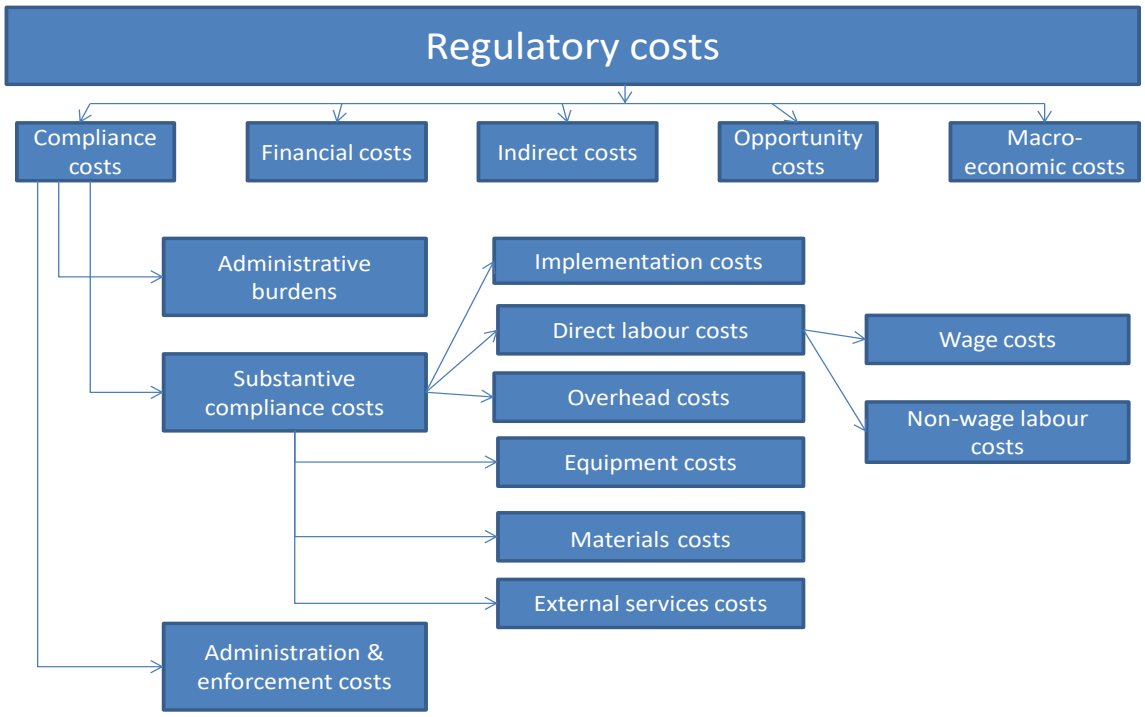


*Figure 3.* Categories of substantive cost compliance. Reprinted from OECD, 2014, Retrieved from https://www.bundesregierung.de/Webs/NKR/Content/EN/Publikationen/oecd_regulatory_compliance_cost_guidance.pdf

### 2.4.4. Kroi's ten steps for regulatory compliance

To comply with legislation internally Kroi (2016) suggests that the following: subscribe to services offering updates on the particular item in question, including regulators and law firms correspondence; attend conferences dealing with compliance to the particular law or regulation, paying close attention to what is involved and who is affected in complying; check for gaps in current processes that would need to be adjusted to be compliant with the new law; make all staff aware of the new requirements and ensure that they are knowledgeable in these; maintain a database of regulations pertinent to the organisation, with the relevant dates of compliance and measures undertaken to comply; clients should also be informed of the new legal requirements that are being complied with and how they are affected; a staff member should be assigned with the responsibility of compliance and finally seek professional input in the short term, or hire a professional to undertake the necessary compliance tasks as needed.

### 2.4.5. ISO 19600 - Compliance Management Systems

Henderson (2017) suggests that ISO 19600 is suitable for use as a framework for privacy compliance. The International Standards Organisation (ISO) produces standards which "give world-class specifications for products, services and systems, to ensure quality, safety and efficiency" (ISO, n.d., para.4). Standard 19600 covers Compliance Management Systems (CMS). Accessing the standard document was not possible without cost, as such other documents relating to the standard were used to highlight factors relevant to this study.

This standard uses the common high-level structure used for ISO Management Systems standards (Bleker & Hortensius, 2014). Morris (2015) and Croft (2017) refer to four phases in compliance management: plan, do, check and act. Croft presents the following clause structure of the 19600 standard:

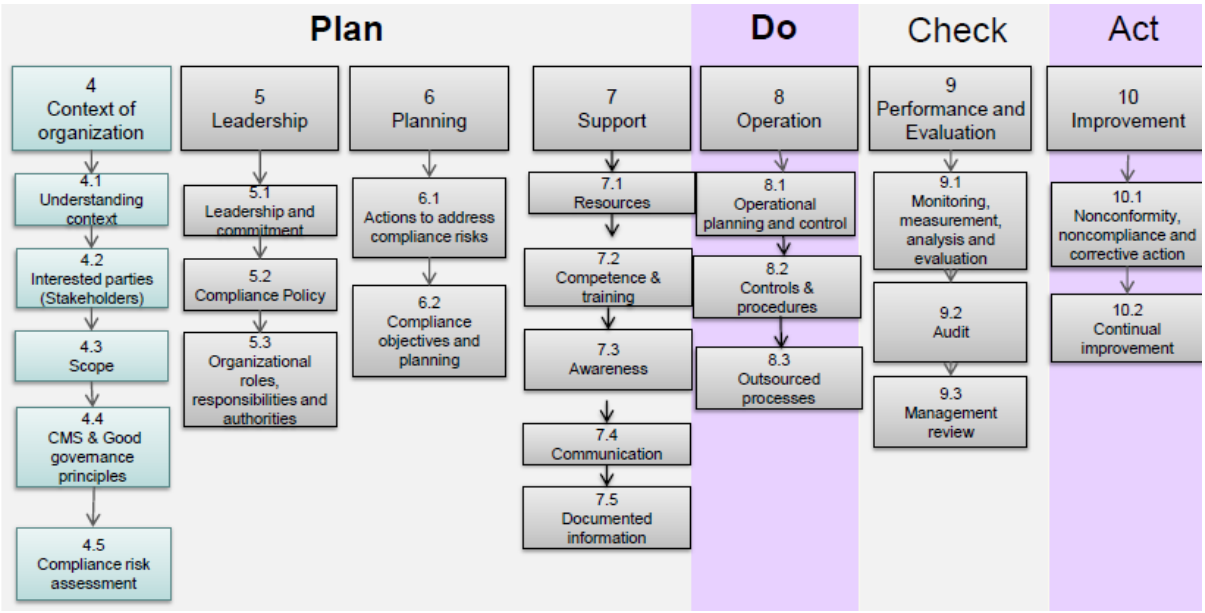


*Figure 4.* Clause structure of ISO standard 19600. Reprinted from Hong Kong Quality Assurance Agency, N.H.Croft, 2017, Retrieved from http://www.hkqaa.org/cmsimg/Symposium%202017/HKQAA_Symposium_2017_Nigel_AM_pp.pdf

Morris (2015) details the four phases as follows: Plan is determining the goals and intention of the compliance system; Do is the implementation of the CMS; Check is the monitoring and evaluation of the CMS; and finally, Act is maintaining and improving the CMS.

DQS, a consultancy offering audit services, provided the following flowchart, in which they note the source as being the standard. It appears in their product offering brochure on services related to compliance management. This flowchart shows two main areas: Establishing the mechanisms for compliance and Improving them. These are further broken down into:

Establishment - developing and implementing the mechanism; Improvement - evaluating and maintaining the mechanism.

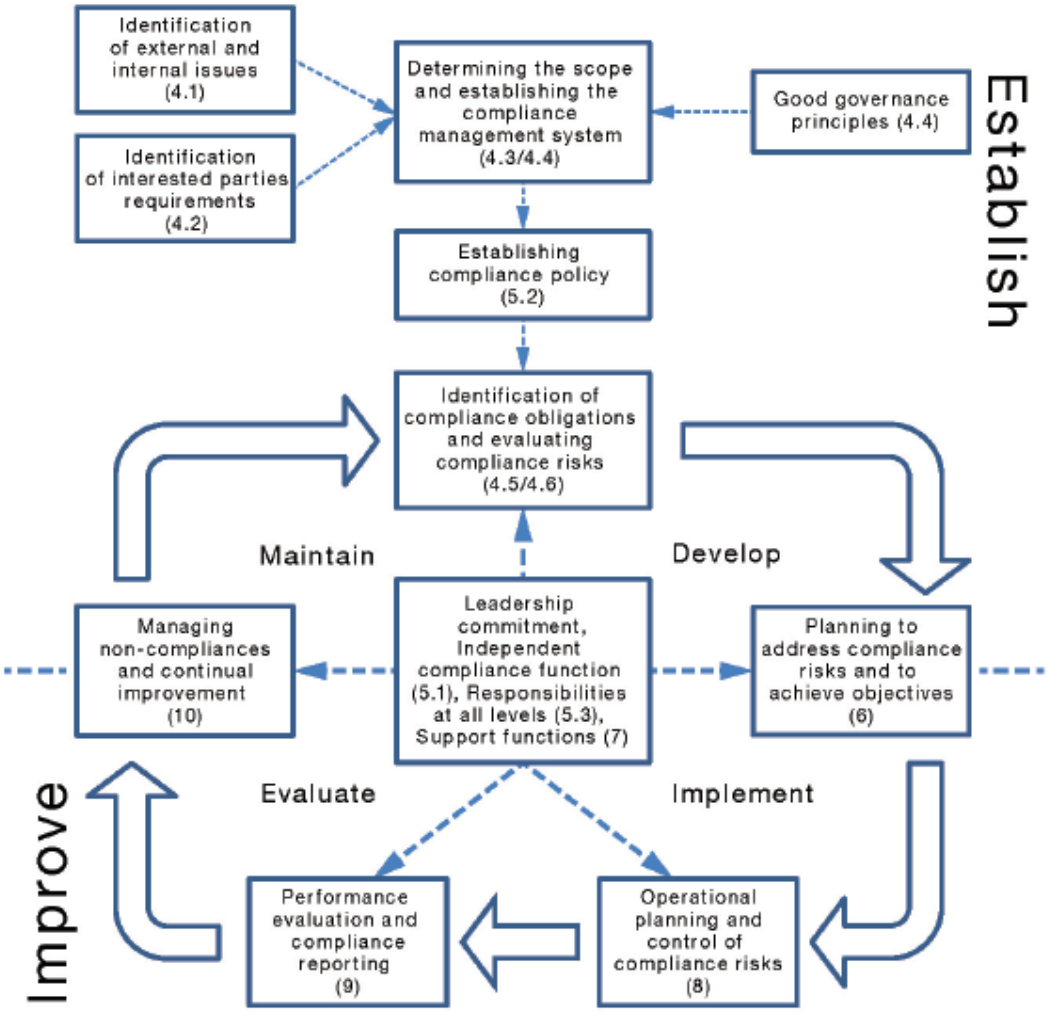


*Figure 5.* Flowchart attributed by DQS to the ISO 19600 Standard document page vi. Reprinted from DQS Consultants. Retrieved from http://www.dqs.co.za/wp-content/uploads/2017/08/ISO-19600-2014-Compliance-Management-Systems-1.pdf

It should be noted that the sub areas differ from those of Morris and Croft, who advocate Plan, Do, Check and Act. Ernst and Young (EY) present a similar flowchart, also attributing the source as the ISO Standard in their product offering brochure for services in the compliance management field, which does correspond to Morris and Crofts version of Plan, Do, Check and Act:

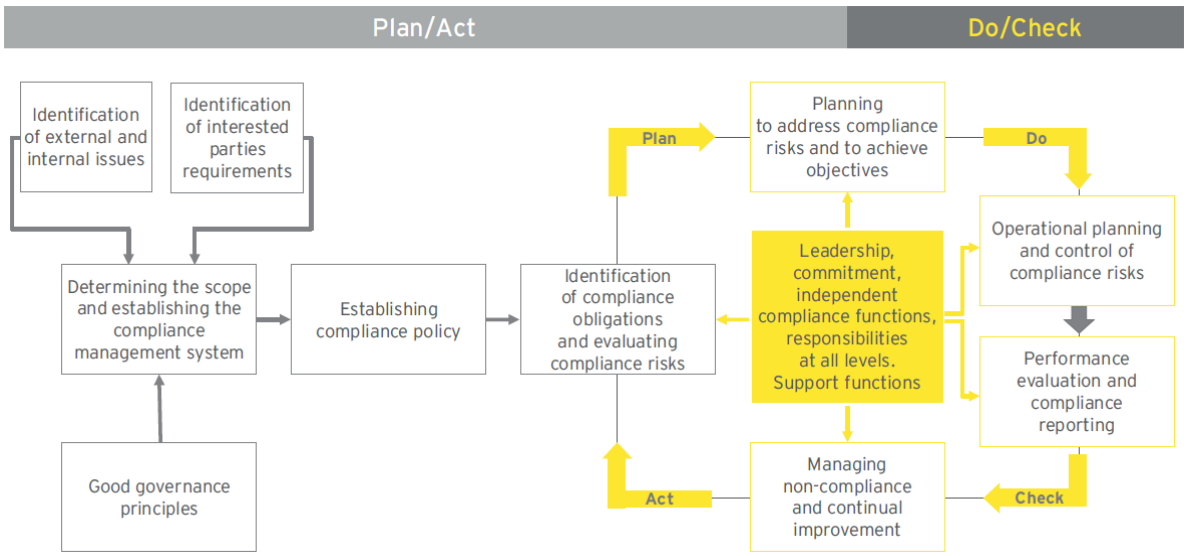


*Figure 6.* EY flowchart sourced from the 19600 standard (EY, n.d., p.2). Reprinted from *EY.* Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-iso-19600-international-standard-for-compliance-management/$FILE/EY-iso-19600-international-standard-for-compliance-management.pdf

### 2.4.6. ISO 17799 - Information Security

The SANS Institute Information Security Reading Room has published a case study into privacy compliance. A key factor in their approach to privacy was that "there is no privacy without security" (Robinson, 2003, p.2). Their approach to achieving compliance was to use the ISO 17799 Information technology - Security techniques - Code of practice for information security management. This standard is described as "a comprehensive set of controls comprising best practices in information security. It is an internationally recognized generic information security standard" (Stallings, n.d., para.7).

The four areas for compliance with ISO 17799 are: Risk Analysis; Risk Management; Sanction Policy, and Security Policy. ISO 17799 was renamed ISO 27002 in order to indicate that the standard was that of the Information Security Standards under ISO 27000. The content is identical except for some reordering and additions for emerging information security issues (Praxiom, n.d.).

This was used in achieving compliance with the Health Insurance and Portability Accountability Act (HIPAA). HIPAA sets out protected health information (PHI) standards for privacy and security. SANS decided that their "greatest area of risk was for unauthorised use and disclosure of PHI, and would therefore focus on protecting the confidentiality of PHI"

(Robinson, 2003, p.1). An absence of security safeguards is seen as increasing the risk of privacy violations (Robinson, 2003).

The 27002 standard covers a wide range of aspects of information security: information security policies; organization of information security; human resource security; asset management; access control; cryptography; physical and environmental security; operations security; communications security; system acquisition; development and maintenance; supplier relationships; information security incident management; information security aspects of business continuity management' and, finally, compliance. This approach of focusing on security agrees with Kroi (2017).

### 2.4.7. ISO 22307 - Privacy Impact Assessment (PIA)

The ISO Standard 22307 'Privacy Impact Assessment' was drawn up with the financial services sector in mind. The standard aims to have a privacy protection framework available. There is a strong focus on global banking and cross-border financial transactions. As a result of this standard there is now a standardised process for financial systems to be designed and built, taking into account personally identifiable information (PII) privacy (Ferris, 2012).

### 2.4.8. Analytical framework to guide this study

The frameworks presented above have varying degrees of suitability for application in this study. Table 1 below describes the elements of each framework presented and if they will be used or not in this study:

Table 1

*Analytical frameworks considered and reasons for rejection or use in this study.*

| **Framework** | **Element / Aspect** |
|---|---|
| Framework Analysis | Both of these frameworks might have been applied in a limited form regarding affected parties being part of the research process, but, as they are not specific to compliance and no literature was found to suggest that they could be used in compliance, they were rejected. |
| DG Markt Guide to Evaluating Legislation | |
| OECD Regulatory Compliance Cost Assessment (CCA) Guide | CCA is a key area of compliance and will be used. |
| Kroi's Ten Steps for Regulatory Compliance | Kroi is not a tested model for compliance and as such was not used. |
| ISO Standard 19600 | Elements of the Compliance Management Framework will be used to guide this study. |
| ISO Standard 27002 | Focus on security as per ISO 27002 should be included. Corresponds to Kroi (2017) also. |
| ISO Standard 22307 | Limited to the financial sector and is focused on systems that facilitate financial transactions and as such is not used. |

*Note.* A summary of the relevant elements of the frameworks considered in this study and why they were used or rejected. Source: Researcher (2019).

Of the seven frameworks presented four were rejected. Framework analysis and DG Markt Guide to Evaluating Legislation are not necessarily relevant to compliance and are rejected. Kroi is very general and as such not suitable for this study. The elements that could have been used are available from other frameworks that are more directly relevant. ISO 22307 Privacy Impact Assessment is a standard linked specifically to the financial sector and systems development and thus not suitable for this study also. Two other frameworks are included but secondarily. OECD's Compliance Cost Assessment (CCA) provides criteria within which to assess cost of compliance. The ISO 27002 as seen in the HIPAA case study has an emphasis on security. This agrees with Kroi's (2017) assertion that data protection is linked very strongly

to cyber security. The remaining framework is used extensively to guide this study. ISO 19600 is a model for compliance and was noted by Henderson (2017) as being suitable for compliance in the privacy field.

The table that follows summarises the various elements of the analytical frameworks that will form the basis of the study:

Table 2

*Mapping of analytical framework elements employed to research question and sub-questions.*

| **Research Question** | **Analytical Frameworks** | |
|---|---|---|
| **Main research question:** What are the pertinent factors in preparation for compliance with the POPI Act and what is their effect? | **ISO 19600 Compliance Management Systems** | **ISO 27002 Information Security** |
| **Sub question 1:** What factors are pertinent to the **organisation** and what is their effect? | 1.) Identify internal and external issues, **Compliance Measures:** 2.) Determine the scope of compliance, 3.) Establish compliance policy, 4.) Identify compliance obligations and evaluate risks, 5.) Plan to address compliance risks and to achieve objectives and 6.) Operational planning and control of compliance risks. | **Security** – 1.) administrative procedures, 2.) physical safeguards, 3.) technical security services and 4.) technical security mechanisms. |
| **Sub question 2:** What factors are pertinent to **staff** and what is their effect? | 1.) Identify interested parties' requirements and 2.) Leadership commitment, independent compliance functions, responsibilities at all levels, support functions. | |
| **Sub question** | **Analytical Framework** | |
| | **OECD Regulatory Compliance Cost Assessment (CCA) Guide** | |
| **Sub question 3:** What **costs** are anticipated in | 1.) Compliance costs, 2.) Direct labour costs, 3.) Implementation costs, 4.) Equipment costs and 5.) External service costs. | |

| | |
|---|---|
| preparation for compliance and what is their effect? | |

*Note.* Specific elements of the analytical frameworks employed in this study are pertinent to a specific part of the research question and sub-questions. Source: Researcher (2018).

An additional factor included in the study, that does not correspond to the other analytical frameworks, is the matter of cost of compliance, drawn from the OECD's CCA. This is a key area of preparation for compliance.

The framework diagram from EY is thus amended by the inclusion of these two additional factors is given below:

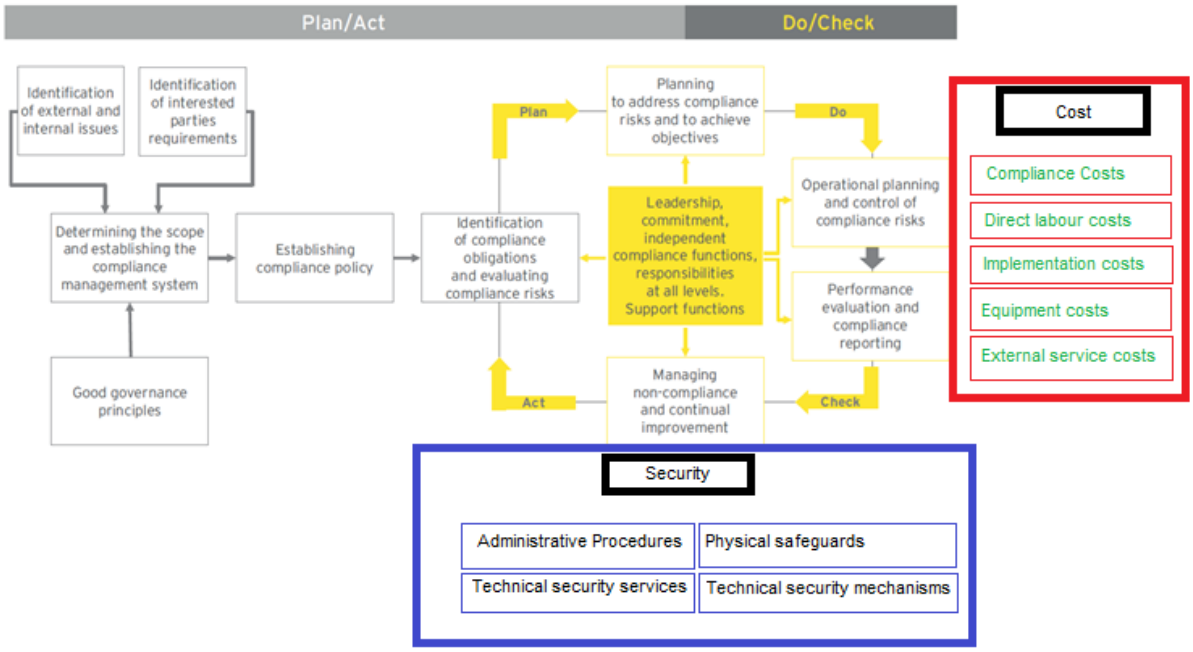


*Figure 7.* Analytical Framework adopted with additional factors added for this study. Source (Researcher, 2018).

## 2.5. Conclusion

Varying attempts at defining privacy have been made. There are also various legislative approaches to privacy that have gone back to the earliest religious texts. Four types of privacy are noted as being information, bodily, communication and territorial privacy. A number of threats to privacy are evidenced and in the contemporary era are spurred by the progress of technology and particularly the Internet. Legislation in the field of privacy often is a number of steps behind and are continually needing to play catch up. Compliance to regulations and

privacy laws are gaining ground internationally. There are however many differing regimes. A leading privacy law is seen in the UK - the General Data Protection Regulation (GDPR). Many countries mirror this as a standard. Breaches and sanction for violation of privacy are being seen more and more. This can also lead to reputational damage.

The field of compliance is vast and goes back many years. In the contemporary era this is seen to stretch back to the advent of public safety organisations. Compliance affects all people in some way or other whether it be following road rules or compliance certificate for a property sale they are inherent to our daily lives. Compliance in many instances comes with a cost.

Regarding analytical frameworks, seven were considered for this study. These are framework analysis, the DG Markt guide to evaluating legislation, OECD's CCA, Kroi's ten steps for compliance and three ISO standards – 19600 compliance management systems, 17799 information security and 22307 privacy impact analysis. Of these ISO 19600 was used in its entirety to guide the study and a section on costs was added as per OECD's CCA and lastly the aspect of security from ISO 17799 (now 27002). The research undertaken is guided by these.

# CHAPTER 3: RESEARCH METHODS EMPLOYED IN THIS STUDY

## 3. Introduction

This chapter details the research design and methods and discusses the development of the data collection instrument. The chapter also describes the data collection process and methods employed in the analysis of the data. The research methodology is said to be a "systematic way to solve a problem" (Rajasekar, Philominathan & Chinnathambi, 2013, p.5).

## 3.1. Contextualising the research problem

As has been mentioned above, POPI relates to the individual citizen's right to privacy as enshrined in the Constitution, and addresses many of the deficiencies of the previous laws dealing with various disconnected aspects of privacy. Compliance with the Act is anticipated to involve significant changes in a range of current practices and be costly. This study identifies pertinent factors in preparation to comply with the POPI Act and their effect on the organisation, staff and the anticipated costs associated with compliance.

As described in Chapter One there are far reaching consequences in respect of complying with the Act, specifically in terms of systems and processes that need to change, and as well on the staff who are responsible for ensuring compliance with the Act's provisions.

### 3.1.1. Research problem

Owing to the variety of elements of the Act and their far-reaching consequences, many considerations need to be taken into account when assessing factors pertinent to preparation for compliance. Preparation for compliance with the POPI Act is anticipated to entail significant changes in business processes for organisations that store and process personal information. It will also limit direct marketing in some instances, as personal information collected from an individual is prohibited from being sold to other organisations for marketing or other purposes different from what it was collected for; organisations that wish to market to these individuals needs to be able to prove that consent was received and that the information was collected directly from the data subject. The research problem is framed as the lack of a deep understanding of those factors pertinent to the preparation for compliance with the POPI Act and their effect on the organisation, staff and the cost anticipated in preparation.

### 3.1.2. Analytical framework

The analytical framework for this study was presented in chapter 2 – Literature review. The questions that guide this study are derived from this. The table that follows presents a mapping

of the analytical frameworks (including specific elements used from the analytical frameworks) with the research question and sub-question that are used in this study:

Table 3

*Mapping of analytical framework elements employed to research question and sub-questions.*

| **Research Question** | **Analytical Frameworks** | |
|---|---|---|
| **Main research question:** What are the pertinent factors in preparation for compliance with the POPI Act and what is their effect? | **ISO 19600 Compliance Management Systems** | **ISO 27002 Information Security** |
| **Sub question 1:** What factors are pertinent to the **organisation** and what is their effect? | 1.) Identify internal and external issues, **Compliance Measures:** 2.) Determine the scope of compliance, 3.) Establish compliance policy, 4.) Identify compliance obligations and evaluate risks, 5.) Plan to address compliance risks and to achieve objectives and 6.) Operational planning and control of compliance risks. | **Security** – 1.) administrative procedures, 2.) physical safeguards, 3.) technical security services and 4.) technical security mechanisms. |
| **Sub question 2:** What factors are pertinent to **staff** and what is their effect? | 1.) Identify interested parties' requirements and 2.) Leadership commitment, independent compliance functions, responsibilities at all levels, support functions. | |
| **Sub question** | **Analytical Framework** | |
| | **OECD Regulatory Compliance Cost Assessment (CCA) Guide** | |

| | |
|---|---|
| **Sub question 3:** What **costs** are anticipated in preparation for compliance and what is their effect? | 1.) Compliance costs, 2.) Direct labour costs, 3.) Implementation costs, 4.) Equipment costs and 5.) External service costs. |

*Note.* Mapping of research question and sub-questions to the elements of the analytical framework. Source: Researcher (2019).

### 3.1.3. Research questions

**Research Question:** What are the pertinent factors in preparation for compliance with the POPI Act and what is their effect?

1. What factors are pertinent to the **organisation** and what is their effect?

2. What factors are pertinent to **staff** and what is their effect?

3. What **costs** are anticipated in preparation for compliance and what is their effect?

## 3.2. Research approach and methodology

The research approach details the methods employed in conducting the research and the reasons for this. Both qualitative and quantitative research methods were evaluated in developing an appropriate research methodology framework for this study. A research approach was determined, and an appropriate data collection instrument was selected.

### 3.2.1. Qualitative research

The qualitative research approach was employed in this study. According to Hancock (1998, p.2), "Qualitative research is concerned with the opinions, experiences and feelings of individuals, producing subjective data". Research into policy or legislation is greatly benefited by obtaining the views of those who drafted the legislation and those affected by it. Qualitative research methods allow for in-depth probing of issues and detail in responses. Qualitative methods, through the use of in-depth interviews for example, provide a more nuanced and detailed account.

### 3.2.2. Exploratory and constructivist research

"Exploratory research tends to tackle new problems on which little or no previous research has been done" (Brown, 2006, p 43). Nargundkar (2008) suggests that exploratory research should

not necessarily be carried out with as rigorous a methodology as conclusive studies, and smaller sample sizes may be used. Furthermore, an exploratory study may show the feasibility of further, more extensive, studies into a particular area (Harvard University, n.d.). This research is exploratory in nature, as the POPI Act is new, and still not enforced. Thus, there is no case law available, which is needed to show how the Acts provisions may be applied or adjudicated on. Areas for further study are identified.

The particular type of qualitative research applied here is constructivism, a "research paradigm that denies the existence of an objective reality" (Mills, Bonner & Francis, 2006, para. 4), "asserting instead that realities are social constructions of the mind, and that there exist as many such constructions as there are individuals (although clearly many constructions will be shared)" (Guba & Lincoln, 1989, p.43). Therefore, Constructivism is used to analyse responses obtained in interviews of legal professionals and others who are themselves involved in complying with the Act or advising others on compliance. The Researcher interpreted the data to determine the factors pertinent to preparation for compliance. Many opinions have been ventured of how preparation for compliance with the Act could be undertaken. This study examines its provisions and how compliance can be achieved in terms of the focus areas outlined previously the constructivist approach is used for this.

### 3.3. Data collection: interviews

Qualitative and constructivist research lends itself to interviews as the data collection tool. Interviews are either structured, unstructured or semi-structured. The questions in semi-structured interviews are not predetermined, thus allowing for flexibility, giving the interviewee the opportunity to highlight aspects he/she considers important. The approach is conversational. According to the UN's Food and Agriculture Organisation [FAO] (n.d. b, para. 1), "Semi-structured interviews are conducted with a fairly open framework which allow for focused, conversational, two-way communication. They can be used both to give and receive information". Coupled with this, interviews could also be formal or informal. The formal interview uses an interview guide to gather information from all interviewees in the same content areas. This allows for more focus (Valenzuela & Shrivastava, 2002). These interviews are the selected tool in order to gather data in answering the research question and sub-questions. The Researcher's interpretation shapes the output of the research in terms of how the data gathered in the interviews is interpreted and reported. Based on this information above, this study employed formal semi-structured interviews as the data collection tool. This approach allowed for the same questions to be posed to all interviewees while being able to

drill into and understand more deeply the nuances of responses providing rich data to inform this study.

The interviewees were drawn from persons involved in the legislative process, the legal fraternity, consultancies offering services in the Acts compliance and organisations that process personal information. Representatives of the legal fraternity included IT law specialists and drafters of the Act. Consultancies assessing readiness to comply for organisations that process personal information were approached to inform this study. The purpose was to understand what measures have been suggested for their clients and specific areas of compliance by both these groups mentioned. Interviews were also conducted with representatives from organisations collecting, processing and storing personal information that would now require complying with the POPI Act. Both operations and IT professionals were interviewed to understand their view on preparation to comply with the POPI Act. Interviews are used to explore the interviewee's experience, or, as McNamara (1999, para.1) puts it: "Interviews are particularly useful for getting the story behind a participant's experiences". Kvale (1996, p.5) suggests that "the main task in interviewing is to understand the meaning of what the interviewees say".

### 3.3.1. Selection of interviewees

Sampling of interviewees was purposive. This means that each group was selected for a specific purpose, alternatively known as "judgmental, selective, or subjective sampling" (Crossman, 2017, para.1). Of the seven types of purposive sampling, this study used elements of three. The first is a homogenous group: all the interviewees are similarly involved in compliance, whether in an advisory or practical capacity. Secondly, an element of Critical Case sampling was employed – where specific insights are expected, which can be applied to similar situations i.e. the preparation for compliance on organisations, the staff responsible for compliance and the anticipated costs of this preparation for compliance. The third is Expert sampling, where experts' knowledge regarding the Act and its compliance was required (Crossman, 2017).

Three groups of individual were interviewed. Each group was chosen in order to provide a particular perspective of compliance. Prominent legal professionals who specialise in the Information, Communication and Technology (ICT) industry and are involved in advising on POPI compliance were approached to participate. They were considered the first category of interviewee. Various people involved in the Law Reform Commission study that initiated the Act were identified. They were Judges in various courts (current and retired), members of the

Bar and Law Society (Advocates and Attorneys) and academics. The previous Public Protector had been part of this commission and was invited. Only two of these individuals were available to be interviewed. Other legal professionals who had provided input to the Commission and made other representations during the drafting process on behalf of their clients – or who had consulted on particular provisions of the Act in other matters that their practice entails. Many of the leading law firms in Johannesburg offer services related to the compliance with the POPI Act. Eight legal professionals were available from this grouping and as such, ten legal professionals were interviewed in total.

The second group of interviewees represented consultancies, or consultants who worked independently or as part of smaller firms that likewise provide service on compliance. The larger firms were not willing to be interviewed, though several consultants who had previously been employed by them obliged. These are Consulting Professionals and five interviewees were from this grouping.

The last group of interviewees was professionals responsible for compliance in their organisations, IT professionals and other operational staff. Nine Operational Professionals were interviewed. A total of twenty four respondents across all of the described groups were finally interviewed.

### 3.3.2. Interview protocol

An interview protocol is a procedural guideline for carrying out qualitative research (Jacob & Furgerson, 2012), and this study too had an interview protocol that was the basis for interviews to inform this study. Its purpose was to ensure a uniformed approach to all interviews conducted. The interview protocol was designed to elicit specific information relating to particular aspects of the Act. Introductory questions were designed to build rapport, including sharing background, details of employment, educational information and other general information.

The question in the interview protocol emerged from a desktop literature review. The first draft of the interview protocol was pre-tested on 13 October 2014. Changes to the interview protocol were applied based on this pre-test and used in subsequent interviews. The interview protocol is Appendix 1.

### 3.3.3. Interview process

Respondents were approached and furnished with the interview questions to assist in deciding their participation: i.e. the interview protocol assisted potential interviewees in making an

informed decision about their participation in this study and allowed for some level of familiarisation with the content. This familiarisation with the content of the data collection tools interview protocol aided in shortening the interviews and the Researcher believes that this focused the data collected to the most pertinent aspects. The interviews were held between October 2014 and February 2015, a majority of which were face-to-face (seventeen), apart from seven conducted via Skype.

The interviews were conducted in the English language and digitally recorded, and following this they were then transcribed. They began with general questions to 'break the ice' before moving on to the main thrust of the interview questions. Interviews lasted between twenty to a hundred and twenty minutes. Written notes were taken during the interview.

### 3.3.4. Transcription of interviews

The interviews were transcribed. Various automated tools were evaluated for this purpose, but eventually a professional transcription service was used. A non-disclosure agreement was signed in October 2014. The recordings were uploaded, and the transcripts were often available within 24 hours.

The transcripts were consolidated into a spreadsheet for analysing the responses, and an association of responses and their relation to the research questions was made by coding and categorising the data to build a conceptual picture of the factors pertinent to preparation for compliance with the POPI Act.

### 3.3.5. Interview techniques employed

Some of the techniques employed included the Researcher remaining attentive, making written notes, and being aware of non-verbal communication, and ensuring the full and correct functioning of recording equipment. Care was taken to ensure that information was analysed neutrally, without prejudice (Yin, 2003). Neutral body-language was always being displayed, irrespective of the response received (Creswell, 1994).

Silence need not necessarily be filled: this gives the interviewee space to further consider their response to a particular question, although it might occasionally be appropriate to prompt the interviewee. Prompting techniques could entail clarifying or repeating an answer, offering examples or repeating the question. This was in the hope of additional relevant information being offered (Mathison, 1988; Maxwell, 1992). Certain responses needed clarification, and probing questions were used to confirm an answer or seek further explanation and drill into aspects that may be loaded concepts (Creswell, 1994). In concluding the interview, a last

question was asked to gather any additional information that an interviewee considered relevant to the study.

A conducive venue was identified for each interview so as not to inconvenience the interviewee. Skype calls were used where necessary. Coffee shops were convenient for face-to-face interviews, though, of course, it was not possible to regulate the noise level unless a booth was available. However, only once did background noise affect the quality of the recording. A time convenient for both parties was found, and every effort was being made to be punctual and keep to the subject at hand. Respect for another's time is an ideal that the Researcher holds strongly.

Prior warning with regard to the protocol and content of the interview was made available to the interviewee. This allowed for a certain level of preparation which contributed to an informed discussion with higher quality data being produced. The disadvantage was the possibility of a certain amount of shaping of output that may have masked certain aspects of the information. The Researcher believed that was a risk worth taking.

### 3.3.6. Ethical considerations for data collection

Anonymity was maintained at all times. No direct quotes that might identify participants or organisations were presented in this report. The intention of the anonymity clause was to promote a franker and more open interview. This was thought to generate higher quality data.

The notion of ethical clearance for research was communicated to the Researcher in mid-September of 2015 when an ethical clearance seminar was convened that was attended by the Researcher. This culminated in ethical clearance being applied for with the University of Witwatersrand's Human Research Ethics Committee via the online submission system RIMS and hardcopy submitted on 25 September 2015. This was reviewed on 23 October 2015. Outcome of this process was received on 9 November 2015. Various changes were requested and were being undertaken by the Researcher, during this process the Researcher was informed that the system had crashed and as such did not continue the process.

Note also that the ethics clearance process was undertaken after the research proposal was approved by the faculty (November 2014), the interviews to inform the study had already been conducted (October 2014-January 2015) and the data was in the process of being written up. As such the process to receive clearance was not considered again.

### 3.3.7. Identification of interviewees

To anonymise the identity of interviewees a system was developed to sequentially number an interviewee from 1-24, prefixed by INT, e.g. Interviewee 2 is denoted as INT2. This was later altered to denote the type of interviewee from the three groups (Legal, Consulting and Operations Professionals). The key is thus LP1-10, CP1-5 and OP1-9.

## 3.4. Data analysis

Analysis is undertaken by means of thematic analysis. Thematic analysis is defined by Braun and Clark (2006, p.79) as "a method for identifying, analysing and reporting patterns within data". The aggregation of responses provides a meaningful, cohesive perspective on the themes for analysis. In this study this applied to the focus areas: pertinent factors in preparation for compliance with regard to the organisation, staff and cost.

Once categorised, themes were noted in the analysis spreadsheet that was drawn up containing all transcribed interview data. The interviewee's initials and category, followed by three columns to note themes and emerging concepts were placed in columns in the spreadsheet used to group and analyse responses (See Appendix 2 for an example). Using basic Excel functions, filtering and sorting made grouping of common themes possible for the analysis of data to be conducted.

### 3.4.1. Analysis of qualitative data

The data was coded according to the themes, and similar elements were sought in order to identify common areas. These were grouped and matched to the focus areas. This is in line with a Surrey University guide for analysing data: "both qualitative and quantitative analysis involves labelling and coding all of the data in order that similarities and differences can be recognised" (Surrey University, n.d., para.1).

### 3.4.2. Measures of reliability and validity

Measures of reliability and validity are key to a studies rigor and integrity. They are central to the judging of how sound any particular research study is and if the results are appropriate and can be applied in practise. This goes to the methods employed in the study and the perceived integrity of results arrived at in the study. A number of criticisms are levelled against qualitative research for its lack of scientific rigour, shallow justification of research methods used in the study, procedures are lacking in transparency and that findings are nothing more than personal opinions that were collected and presented while subjected to bias on the part of the researcher

(Noble & Smith, 2015, p.34). From this it is seen that deep justification of the methods are required and that the analytical framework will assist in exposing procedures undertaken in the research thereby allowing for a greater degree of transparency. Weiner (2007) suggests that there could be reliability without validity yet there could not be validity without reliability.

#### 3.4.2.1. Reliability

Reliability is defined as *"*the degree to which a measurement technique can be depended upon to secure consistent results upon repeated application" (Weiner, 2007, p.6). Or stated differently, reliability could be repeatability or consistency that brings about consistent results (Trochim, 2006). Thus, a research study should yield the same or at least similar results if repeated under the same conditions.

There are three facets of reliability: stability or otherwise known as 'test-retest' where the same tool is used at different times to see how different the results are, equivalence that allows for the questions posed to be worded slightly differently to answer the same construct and lastly internal consistency "is a measure of how well related, but different, items all measure the same thing" (Michael, n.d., p.7).

The Researcher is confident that with the material laid out in this chapter a repeated study would come to the same findings thereby fulfilling the 'test-retest' facet of reliability. The equivalence facet would be met also if similar questions were posed differently and would have a high probability of garnering similar data. Internal consistency was enhanced due to interviews being semi-structured as additional questions were asked to hone in on specific responses further illuminating relevant aspects of preparation for compliance with the POPI Act. As such all facets of reliability would be met.

#### 3.4.2.2. Validity

Validity refers to how well a tool measures the construct that it is intended to. There are said to be three types of validity – construct validity that is an indicator of suitability of the scale set out to measure the construct, content validity that is a 'judgement' by reviewers on appropriateness of the item and criterion validity which gives an indication of how well or otherwise the tool compares to another for the same purpose (Michael, n.d.). The difficulty however is that an objective measure of determining validity does not exist, Schutt (2004, p.330) notes this and a possible solution to overcome it:

> …no set standards exist for evaluating the validity, or authenticity, of conclusions in a qualitative study, but the need to carefully consider the

evidence and methods on which conclusions are based is just as great as with other types of research.

Semi-structured formal interviews were the chosen tool for this study for reasons presented above. Therefore construct validity should rank highly. At the time of drawing up the tool the questions were appropriate yet there were questions that were not required that were included. As such content validity may rank lower than if this had not been the case. However content validity is subjective and as such the impact of this on the study maybe negligible. Criterion validity is not relevant to this study.

### 3.5. Conclusion of research methodology

This exploratory research study was completed undertaking qualitative research; the specific method was constructivism and data was collected by way of a formal semi-structured interviews. Purposive sampling was undertaken to identify interviewees, who were then invited to participate. The interview guide was sent to potential interviewees in the interests of their informed decision being made to participate in this study or not. They were kept anonymous. Data gathered from the interviews was consolidated into an Excel spreadsheet for sorting the data from all twenty-four interviews and to identify and group the various themes for presentation and analysis. This data was analysed by thematic analysis.

# CHAPTER 4: PRESENTATION OF DATA COLLECTED INFORMING THIS STUDY

## 4. Introduction

The previous chapter described the research problem and research questions and discussed the research methods and the data collection strategy. In structure this chapter mirrors the research question – pertinent factors in preparation to compliance with the POPI Act and their effect on (a) the organisation (b) staff, and (c) the anticipated cost of preparation for compliance. Presenting the data is said to be "the process of organising data into logical, sequential and meaningful categories and classifications to make them amenable to study and interpretation" (Perez, 2014, p.3).

## 4.1. Factors pertinent to the organisation's preparation for compliance and their effect

Data is presented outlining the various sectors and industries, and the specific factors pertinent to their preparation for compliance with the POPI Act. This is followed by the internal and external processes that are affected by preparation for compliance. The role of the conditions for lawful processing and security of information is presented, in accordance with the analytical framework. Data emerged regarding retrospective compliance with the POPI Act; this must be considered an important aspect of preparation for the organisation. Data regarding key data-driven business processes that are data driven is also presented. Lastly, views are presented on how onerous the preparation for compliance is expected to be.

### 4.1.1. Sectors and industries

LP2 (Interview, 20 October 2014) noted that the POPI Act has very few exclusions or exceptions in its application, and therefore many industries and organisations stand to be affected: "All processes, all data processing … because processing is defined very widely". LP8 (Interview, January 12, 2015) suggested that the following sectors stand to be affected by preparation especially greatly for compliance with the Act: Non-Governmental Organisations (NGO's) / Non-Profit Organisations (NPO's), the Financial Services Sector, Education, Direct Marketing and Health Care. This is because "personal information is intrinsic to their business". Eleven respondents noted that these sectors have higher volumes of data and large consumer bases, and therefore are affected more than others. Additionally, education and health care sectors have a large volume of information classified by POPI as 'Special Personal Information', which requires more stringent control than ordinary personal information. The take-up of complying with new legislation and sector regulation varies from one sector to

another. Data suggests that highly regulated sectors tend to be quicker to comply; an example mentioned is financial services (LP8, Interview, January 12, 2015).

### 4.1.2. Unique aspects of the Act

A majority of respondents pointed to provisions of POPI that they considered unique specifically the inclusion of juristic persons: the influence of Intellectual Property laws; and the Companies Act in as far as they relate to competition; the protection of small businesses who are "almost indistinct from their proprietors" (LP6, Interview, December 10, 2014). The third view (of a drafter) was that the inclusion of juristic persons stemmed directly from the Constitution. Though the notion of juristic persons being included was contested: "how is a juristic person going to comply with the same principles as a natural person" (LP6, Interview, December 10, 2014). LP3 (Interview, November 7, 2014) mentioned: "what is unique to me is how we deal with account numbers, the rights of privacy of juristic persons and the way we deal with consent is a bit unique"

LP10 (Interview, January 22, 2015) observed that, uniquely, all the latest developments relating to protecting privacy are incorporated in the Act (Interview, January 27, 2015). OP8 noted, critically, ambivalence in the opt-out regime and its application: "in section 69 they talk about the right of marketers to be able to approach a consumer without consent using electronic communications once. We don't know what once means: is it per brand, per product… it is unique". They also suggested that the Act's definition of children is also unique.

### 4.1.3. Internal and external factors

CP4 (Interview, January 16, 2015) considered that internal changes - those within the organisation, such as processes, security, protecting employee information, training and raising awareness of the POPI Act would be more extensive than external changes. Changes in controls and security surrounding collected information are internal: "internally ... they will also have lots of things based on controls, only use things for the purpose for which they are collected. There is the whole information security aspect to it" (LP3, Interview, November 7, 2014). A factor that has bearing on preparation for compliance is the size of the organisations systems architecture. These characteristics will affect the changes that may be enforced on organisations. Organisations with large systems architecture the chance of gaps is greater than in smaller companies with smaller, less complex ones (CP3, Interview, November 21, 2014).

LP5 (Interview, December 9, 2014) suggested that internal changes would also include security and safeguarding of the information: "security safeguards internally is a very big thing,

obviously. A lot of companies do not have adequate controls". Security measures for compliance would depend on the size of organisation, smaller organisations would not be able to apply the same measure of security as a big organisation: "if it is the simple thing like your 'mom and pop shop' making sure that at least their one computer where all their payment processing and records are virus protected and encrypted…right up to the big organizations" (LP6, Interview, December 10, 2014).

External changes refer to matters relating to clients, customers or service providers. LP2 (Interview, October 20, 2014) notes that "external will relate to information they hold about their customers and how they process that. And also, all agreements entered into with third parties, that is, the section nineteen and twenty obligations". When considering an external service provider to which data would be transmitted, an additional requirement would need to be to ascertain whether the information would remain adequately protected, consistent with the Act (OP4, Interview, November 24, 2014). Organisations' interaction and transmission of information between suppliers and clients should be assessed under the Act to ensure compliance "externally with suppliers, customers, information that you are giving out or receiving from them" (LP5, Interview, December 9, 2014). Additionally, they suggest that in the outsourcing industry other controls need to be instituted to ensure compliance. If the data is to travel across borders, measures need to be in place to ensure compliance with the Act. Agreements should be drawn up contractually to document the processes undertaken to comply with the POPI Act (LP5, Interview, December 9, 2014). A respondent mentions his awareness of a large health and life insurance provider which has made a user portal available to update clients' personal information. This is a way of ensuring that correctness of information is maintained in line with the POPI Act's provisions (OP5, Interview, December 10, 2014). This instituting of a client-facing system is an example of an external effect of the Act. Another perspective is that a new step in the collection, storage and processing of personal information process will appear, that of notifying the Regulator of what information is being collected and why (LP8, Interview, January 12, 2015).

### 4.1.4. Conditions for lawful information processing

A number of conditions for lawful processing of information emerged in the interviews. They are key to preparation for compliance (LP5, Interview, December 9, 2014). This section presents the data regarding the specifics of each of the conditions.

#### 4.1.4.1. Accountability

This condition refers to the responsible party making sure that the conditions for lawful processing are upheld. A respondent noted that "hitting the principles down; for me, that is adequate" for compliance (LP5, Interview, December 9, 2014). The essence of this is that the noted conditions are central to compliance. (In early drafts of POPI the conditions were listed as principles). As such compliance with the conditions for lawful processing of information aligns to the analytical framework in terms of scope of compliance, compliance obligations and security.

#### 4.1.4.2. Processing limitation

This condition has three parts - Lawfulness of Processing; Minimality and Consent, and lastly Justification and Objection. Processing of information needs to be undertaken lawfully and processed in a reasonable way. Minimality refers to guarding against processing information more than is necessary.

Regarding Consent, Justification and Objection the main thrust is seen to be consent. Two opposing views emerged from respondents whether the POPI Act is consent-driven or not. Only one respondent suggested that consent is not required, though they amplified their view in suggesting that some form of record should be kept proving that personal details of a data subject are collected in accordance with the POPI Act's provisions. It would also need to provide proof that the data subject has allowed it (LP3, Interview, November 7, 2014). This is in effect a form of consent, so the view was effectively unanimous; and all twenty-four interviewees noted this as a major area of preparation for compliance. OP1 (Interview, October 13, 2014) believed that, where possible, additional systems to facilitate compliance would record consent and other details about the manner and timing of organisation's correspondence to its data subjects. LP4 (Interview, November 18, 2014) agreed with the need for changes to systems: "we definitely have to upgrade our systems in terms of putting in more sort of alerts and triggers and more rules around specifics. So now we need to see that there is consent".

#### 4.1.4.3. Purpose specification

This condition requires that information be collected only for a specific purpose and retained for a defined period linked to that purpose. De-identification is also specified under this condition, where information must be deleted once the purpose for which it was collected has been concluded.

The purpose for which the information is collected must be made known to the data subject and must only be used for that specified purpose. Seven respondents noted this as a factor for preparation to comply: “POPI says that when you want information from a person you have to explain to them what the purpose of collecting the information is” (OP9, Interview, January 24, 2015).

Retention is the period that the information is stored for, and, again, should be only for the duration of the purpose for which it was collected. Seven respondents noted this as an area of preparation for compliance: “you may not keep it for any longer than you need to, so now they will have to look at their data management as well” (LP1, Interview, October 20, 2014). Information management processes will require attention within organisations preparing to comply with the POPI Act. A challenge associated with retention is how to destroy information securely and permanently once the purpose for which it was collected ends. To quote CP4 (Interview, January 16, 2015):

> …when you no longer need it how do you destroy it, and that brings in the technology aspects like how do you actually destroy information? Paper side, you shred it. On the electronics side how do you destroy information, because a good forensics team will be able to recover information off a hard drive that has been formatted more than seven times.

Technology could be employed for efficient destruction of information: “I have actually seen physical products that you put hard drives into and you pull a lever and it actually breaks the whole hard drive in half so that the information cannot be recovered” (CP4, January 16, 2015).

#### 4.1.4.4. Further processing limitation

Further processing is to be compatible with purpose of collection. Three respondents noted this as a factor in preparation for compliance. For example: “yes, and they are also going to have to inform the client exactly… The biggest way in how it is going to be processed” (OP6, Interview, January 15, 2015).

#### 4.1.4.5. Information quality

This condition will require various process changes within and without the organisation. The essence of this is that information should be correct, complete and up-to-date. Processes will thus be needed for verifying the correctness of information on collection, as well as regular checks to assess whether it remains correct.

The POPI Act is prescriptive in detailing how to manage information: "you know the Act is so minute; it tells you that if you are keeping somebody's information you must keep the address up-to-date" (OP3, Interview, November 6, 2014). They go further:

> …the law says keep the information up-to-date. If you don't want to keep the information up-to-date then you must de-identify that information. This requires processes to continually monitor information to maintain its quality: then also making sure that they are constantly cleaning up their information (OP6, Interview, January 15, 2015).

LP9 (Interview, January 15, 2015) gave the example of marital status:

> …so, I give you information, and it is pertinent to whether I am married or not…I get divorced at a later stage; you should have the process in place that my information can be updated to the fact that my status has now changed.

#### 4.1.4.6. Openness

The openness condition has several dimensions, including interaction with the Regulator (noted by two respondents) and with data subjects (mentioned by seven respondents). This is to specify what information is being collected and why.

OP6 (Interview, January 15, 2015) stated that data subjects should be informed about how their personal information will be used, and the processes this information undergoes: "they are also going to have to inform the client exactly what they do with the information, and the chain between that" this being to explicitly spell out the various steps in processing of the information. CP4 (Interview, January 16, 2015) agreed: "what do you tell your clients at the point of collection?" One respondent commented that there may be an overlap between openness and data subject participation. That openness is for transparency in how the information is being used (OP5, Interview, December 10, 2014).

#### 4.1.4.7. Security safeguards

Thirteen respondents noted security safeguards as an important area for preparation for compliance. The POPI Act specifies security measures for integrity and confidentiality of personal information. Responses included the need to enhance measures to secure information on various systems (OP2, Interview, October 21, 2014) and to limit access to the information (LP7, Interview, January 12, 2015). Only specifically designated people should have this access, and that should be only for specific purposes (OP3, Interview, November 6, 2014).

Security safeguards are seen as key internal processes affected by preparation for compliance (LP3, Interview, November 7, 2014). They vary with IT landscape and size of organisation (CP3. Interview, November 21, 2014).

If information is processed by an operator as defined by the POPI Act, then an agreement or mandate will be required for this to be legitimate. Operators are to fulfil the conditions of the Act, but Responsible Parties are ultimately responsible for the data's security. This should also be part of the notification communicated to the data subject (LP3, Interview, November 7, 2014).

Should security be breached, or information lost, a notification should be issued to all who may have been affected, namely, all data subjects whose information might have been mislaid or stolen. Considering the possible reputational damage, "even the smallest breach or loss of data is a contravention of the Act" (LP5, Interview, December 9, 2014). OP6 (Interview, January 15, 2015), additionally, foresees a "big impact on the industry".

Due to the provisions of the POPI Act in relation to access controls, only people who require access to data for specific work must be given, it and no one else. Thus, professionals who are responsible for system access need to ensure that correct processes for access to systems are in place - "there has to be a process for the people that require access to information" (OP2, Interview, October 21, 2014). Systems administrators maintaining systems storing information would need measures to ensure that those individuals are performing their data access activities correctly in terms of the Act (OP4, Interview, November 24, 2014). In addition, access should be reviewed at regular intervals to determine whether it is still required (OP2, Interview, October 21, 2014).

The centrality of security to privacy is seen in the HIPAA Act case study presented in chapter 2 with the introduction of ISO 27002. The analytical framework includes a component related to security. The King codes of governance emerged three times in relation to security and data protection. Particularly in relation to laying down standards for compliance regarding the POPI Act (LP9, Interview, January 15, 2015).

#### 4.1.4.8. Data subject participation

This condition drew four responses. The first concerned access to personal information. Any person may request to see any information that belongs to them, and, unlike PAIA, the request may not be refused. The effect of this will be felt in processes that need to be developed to accommodate this (LP7, Interview, January 12, 2015).

Correction of personal information was another aspect commented on. As seen earlier, the POPI Act demands this, so measures for it will be necessary. A new process will thus need to be created where none exists already. The affect is seen in the following quote: "also making sure that they are constantly cleaning up their information" (OP6, Interview, January 15, 2015). The process will need to allow individuals access to their information for them to correct and validate it.

### 4.1.5. Retrospective compliance

This appears to be fraught with potential hazard, for if the POPI Act is applied retrospectively, current databases that do not comply could be invalidated. This is confirmed by Jacobsen (2013), as noted in chapter 2. This section considers this factor.

LP4 (Interview, November 18, 2014), agreeing about the potential hazard: "I think it will be unfair if it is retrospective, because there will be no obligation, as far as I am concerned. But I think it would be wise from a practical point of view to get it". While retrospective compliance should not be obligatory, it should be nevertheless being undertaken so as to ensure that data subjects' rights are upheld.

CP3 (Interview, November 21, 2014) suggests that it could be crippling if companies with many data subjects' personal information had to comply retrospectively and once again obtain consent from each data subject. They outline each of the positions:

> It's a debate whether the Act is retrospective or not. Which I think is another big issue. Because if it is going to be for gathering information from here on in, then it should be okay. Then you should be able to get around it (sic) quite easily. But if it is retrospective, you have for some company's clients over a million clients and you are suddenly now going to have to get consent.

This will directly affect the time necessary for compliance and certainly increase the required effort to be compliant. This aligns to the analytical framework in terms of identifying risks.

### 4.1.6. How onerous preparation for compliance is anticipated to be

The data reflects a continuum of views. In all the discussion so far, it has been either implicit or explicit is that various aspects of the POPI Act will involve preparation in order to achieve compliance. Positively, three respondents considered the Act reasonable in its requirements. One opinion was that reasonable persons would have implemented a number of its provisions even in the absence of the Act, and that therefore compliance ought not to be difficult. Drafters

of the Act who participated in this study agreed that compliance would not be onerous, as the provisions are straightforward and reflect ordinary good practice. On this view the Act is merely common sense. Some remarked that the significant affect would be felt by the minority inclined to break the law (LP1, Interview, October 17, 2014).

Conversely, nine respondents maintained that POPI will be extremely onerous to comply with, requiring a comprehensive re-engineering operation. Views within this spectrum were concerned less with the requirements of the Act than its reach. Thus, for example, an organisation like Standard Bank will need to implement changes to a large number of systems – demanding in both time and staff. A further opinion pointed out that the affect will be felt in the short term, but that over time its requirements will become the usual way of doing business.

Eight respondents pointed out that implementation would be only as involved as individuals made it, depending on the size of the organisation and how much had already been done to comply: It (POPI) recognizes that what is expected of a huge medical aid scheme is not going to be the same as a doctor, a small doctor operating by himself (LP6, Interview, December 10, 2014). OP5 (Interview, December 10, 2014) held that the Act is no more than a framework for using information legally; it does not stop sending correspondence, but regulates how this is done, and as such it not onerous to comply with.

An interesting observation was that views on how onerous compliance might be would depend on who you speak to. Thus, service providers – legal or technical – might be inclined to emphasise the need for their services, and thus over-emphasise the difficulties. LP8 (Interview, January 12, 2015) suggested that POPI will be onerous because of new processes needed in order to submit disclosures to the regulator, and notification to clients or data subjects. (These relate to what information is collected and how it is used). Aligns to identification of risks from the analytical framework.

### 4.1.7. Key business processes

In some organisations collecting and processing data is a key business process, and so the POPI Act poses a significant risk. An assessment of whether this risk could be sufficient to cause the failure of the organisation should they not be able to comply, is detailed below.

OP1 (Interview, October 13, 2014) maintained that the POPI Act indeed has the potential to ruin an organisation, asserting bluntly: “we won’t be able to function”. Another view was that areas of an organisation would be hampered without completely halting day-to-day operations: “I am not too sure in terms of whether a business or a section of business might close because

of the Act, but I definitely think that some sections will be hindered" (CP3, Interview, November 21, 2014).

A drafter believes that the regulator could potentially close a company down: The regulator has quite wide powers … at the moment already the regulator can't really give you a big fine, but he can actually close your doors (LP10, Interview, January 27, 2015). A contrary view is that as the POPI Act is reasonable, there will not be much room for the closing down of organisations: "I don't think that is going to happen. POPI is not an unreasonable Act" (LP6, Interview, December 10, 2014).

Another opinion likens compliance with the POPI Act to compliance with previous legislation, which was ignored: some organizations might just take their chances and hope they are not investigated by the regulator, and thus avoid needing to institute changes for compliance (LP7, Interview, January 12, 2015). A further view is that organisations may be forced to close, but not in the short term. This will also depend highly on how diligent the Information Regulator is in carrying out its responsibilities (LP8, Interview, January 12, 2015).

Six respondents expected a wait-and-see approach, and that a great rush to comply will occur initially. However, this may change once the Regulator is in place. How effectively it carries out its role will determine whether some will ride it out and hope not to be taken to court (OP6, Interview, January 15, 2015). "They will hold out as long as possible. They will choose business over compliance (LP7, Interview, January 12, 2015).

A contrasting view is that, irrespective of the diligence of the Regulator, individuals could enforce the POPI Act to some degree, and that this may in some instances enforce compliance: "Even if our regulator is not up to scratch, maybe if the people start enforcing their rights we might see some change" (LP7, Interview, January 12, 2015).

LP7 (Interview, January 12, 2015) has seen behaviour and take-up in compliance with previous legislation and agreed that many will not comply until found to be in non-compliance, and then only to the degree forced to comply: "we have … seen that with other laws, like the NCA and CPA, where people keep doing their own thing until they get into trouble".

Data collected showed that organisations will not willingly close their doors until the regulator makes a finding against them, at which point will they take action:

> I think, due to the nature of man, they won't close. It is not going to be an effect where you see people who can't afford to implement that they are going to close.

> I see they will only be affected once they [have been shown to have been] negligent, and have been caught (OP9, Interview, January 24, 2015).

### 4.1.8. Concluding pertinent factors for the organisation's preparation for compliance

Data was presented answering sub-question 1: pertinent factors in preparation for the organisation's compliance with the POPI Act. The factors presented were internal and external relating to the conditions for lawful processing of information, including security. The matter of retrospective compliance was presented as an important factor for organisations to consider in their preparation for compliance. Unique aspects of the Act were presented as POPI was promulgated to protect the rights of juristic persons and as such is applicable to the organisation. Lastly, how onerous the Act was anticipated to be in terms of preparation for compliance was presented.

## 4.2. Factors pertinent to staff in preparation for compliance and their effect

Various factors regarding the effect on staff involved in preparation for compliance are presented below. Data is presented in terms of existing staff and of external consultants in the process of complying with the Act. A further section looks specifically at the preparation required by IT professionals for compliance, and lastly, data is presented in relation to the role of the Information Officer. The elements of the analytical framework with regard to staff are 1.) Identify interested parties' requirements, 2.) Leadership commitment, independent compliance functions, responsibilities at all levels, support functions.

### 4.2.1. Staff preparation for compliance

The broadest responses foresee all roles within the organisation, directly or otherwise, requiring some form of preparation for compliance, at the minimum that every individual would need to be aware of the requirements of the POPI Act, and to look specifically at the implications for their own roles, however slight (LP3, Interview, November 7, 2014).

Changes are anticipated within certain staff roles: for instance, regional sales people who carry client data while travelling would now need to take greater care to ensure its safety, possibly even installing safes in their homes to store information overnight (LP7, Interview, January 12, 2015).

A type of compliance oversight role should be set up to monitor the measures put in place: "first of all it will necessitate changes in terms of security, but then also compliance. ... it is all very well having security, but you need someone to ensure that security is being compliant"

(LP1, Interview, October 17, 2014). This again relates to who has access to the information. At present many individuals may be able to access a common database, despite not necessarily needing to in terms of their roles. Thus, an added responsibility would rest with security or system administrators in charge of ensuring correct access and use of systems.

A more specific response concerns functional teams. The marketing and communication functions collect personal information that is then captured often by another team. Then yet another team provides the system, secures the platform and has general oversight of its use (LP5, Interview, December 9, 2014). OP5 (Interview, December 10, 2014) suggested that many roles, from board level right down through the whole organisation would require preparation for compliance. Another response was that a committee, rather than an individual, should be responsible for processes related to the POPI Act (CP2, Interview, November 11, 2014).

In larger organisations compliance may be overseen by the existing compliance officer, or as an additional function of another existing role: "the person who is currently responsible for the information may just have an expanded role" (OP3, Interview, November 6, 2014). It is also uncertain whether the POPI Act requires an altogether new role, or that responsibilities might be added to an existing one. This consideration will affect costs. It is perceived that only larger organisations will be able to afford a new role. It is also uncertain whether the POPI Act requires an Information Officer, or other dedicated role, with responsibility for compliance.

Again, the responses received need to be understood in terms of the role of the respondent: the perspective of an in-house professional will tend to differ from that of a consultancy offering a related service. An industry professional said:

> …of course, our answer is that you will need a team to help you kick it off and ... implement some of the controls. So, you can get your external consultants or even independent consultants. That is now big business. like a big gap. The legal guys - I am seeing a lot of them are going off on their own being independent privacy consultants (CP2, Interview, November 11, 2014).

This respondent emphasised the initial setting-up: "there is definitely tons of work out there at the moment in terms of policies for POPI" and added, that outsourcing could minimise the effects of compliance within the organisation (CP3, Interview, November 21, 2014).

LP5 (Interview, December 9, 2014), who heads the POPI Act Compliance department of a consultancy, confirmed that the whole organisation needed to be familiar with the Act, and that in the case of is firm the legal advisers needed to be know the Act:

> …for us the main thing was getting our legal advisors on top of the new Act … it is a total (sic) new way of thinking for a legal person as well ... it is a total (sic) new way for advising a business.

This suggests that legal advisers will need to change their approach.

### 4.2.2. The need for consultants

With many roles in a wide range of industries, consultants may be employed to offer various services. The respondents offered views of what forms this might take. Seventeen responses thought that consultants would need to be engaged, though one disagreed.

LP1 (Interview, October 17, 2014) was adamant: "yes most definitely you will need outside information from specialists". A legal professional suggested that consultants like himself will be necessary to give the required tools. Once established, their further services would be needed only periodically, for specific issues (LP3, Interview, November 7, 2014).

Professional help will be required because the combination of specialised skills for compliance, being rare, makes their services to the organisation indispensable (CP2, Interview, November 11, 2014). LP5 (Interview, December 9, 2014) added that smaller companies experience a growing frustration with new legislation, causing pressure to hire a consultant.

Another need for consultants is that in-house staff, even if they possessed the combination of skill already mentioned, might not be able to transfer their skills to in-house staff over a period (LP6, Interview, December 10, 2014). Of course, this might equally apply to the legal and other professionals whom the organisation might hire.

### 4.2.3. Role of IT professionals

The literature and interviewees agreed that IT Professionals would bear the brunt of compliance. The implication is that this directly affects their daily tasks, as they "are actually playing with that information twenty-four hours a day" (LP1, Interview, October 17, 2014). IT professionals will need to examine the POPI Act to assess what exactly is required of them as they go about their regular work. LP3 (Interview, November 7, 2014) agreed, mentioning some of the specific roles involved in implementation. Those who work directly with data will now need to be aware of the conditions for lawful processing. Communication between technical teams (security, compliance and privacy) will be important to avoid misalignment (CP2, Interview, November 11, 2014).

CP3 (Interview, November 21, 2014) felt that the task to comply will be a massive one in-house, that might require a complete re-engineering of various systems, and that this would require great deal of preparation for internal staff. Agreeing with how heavily IT staff will be affected, CP3 (Interview, November 21, 2014) suggested that even after initial compliance has been achieved, daily checks will be necessary to ensure ongoing compliance. Fourteen interviewees agreed that security is a large, perhaps indeed, the largest, area of preparation for compliance. A drafter stated: "information security is absolutely critical to privacy" (LP9, Interview, January 15, 2015).

Moreover, data quality needs to be monitored (LP6, Interview, December 10, 2014). This arises directly out of the conditions required by the POPI Act, specifically condition 5 – Information Quality, which requires that only correct and up-to-date information is kept - a major challenge. A respondent from a leading African university working in records management highlights the practical difficulty: their data goes back many years and consists of information about many people that has not been updated (OP3, Interview, November 6, 2014). Others agreed that this situation is common. Thus, staff responsible for data integrity within their organisations would be required to prepare for compliance regarding this factor.

OP6 (Interview, January 15, 2015), observed that the POPI Act provides opportunities for IT professionals to derive income from systems development work related to the POPI Act as a source of additional income. Furthermore, the demand for security and penetration testing, data audit and process optimisation services will increase greatly.

CP4 (Interview, January 16, 2015) noted that the nature of the IT professionals' task of preparation for compliance will depend on the type of the organisation. Thus, an organisation in the medical sector will already have many controls to secure this information, in contrast to, say, an investment bank, where traders generally "are cowboys, because they like making money for the clients. It is not necessarily about protecting the client's information. And that culture feeds right the way through to the IT staff as well". CP4 (Interview, January 16, 2015) pointed out that a further area affecting preparation for compliance on IT professionals is the architecture of the systems in question.

### 4.2.4. The role of the Information Officer (IO)

Discussion regarding the role of an IO is an important factor for compliance with the POPI Act and is linked to where the position fits in the organisation. Various views were offered.

The designated IO role and responsibilities are not certain and range from the responsibilities of current staff being widened to accommodate the new responsibilities (CP4, January 16, 2015), to a new, high-level role being created. This might be on the board, a company secretary or even a so-called C-level executive (Chief Officer role, on par with the COO and the CFO) (LP6, Interview, December 10, 2014).

It was thought that the IO would need to be sufficiently high in the organisation to be able to drive the necessary changes in all areas of the organisation, and not limited to a specific team (LP8, Interview, January 12, 2015). One respondent argued against the person being in the company secretary role, as they needed the technical security and privacy skill sets. A specialist could be brought in at board level to provide oversight (CP2, Interview, November 11, 2014).A respondent who was part of drafting the EU Directive on Data Privacy suggested that the process of complying with POPI should be "top-down, not bottom-up" (OP8, Interview, January 22, 2015). Any new role for compliance could be filled by a junior person who is backed by someone more senior and able to mobilise the other senior staff to make the necessary changes in their teams or departments (LP7, Interview, January 12, 2015).

Together with position within the organisation is the skill set required. A person with compliance background, a legal professional or even a junior entry-level position (LP7, Interview, January 12, 2015). Some went further, suggesting that a combination of privacy and technology backgrounds is needed, or even that an external professional with the well-rounded skills needed should be sought (CP2, Interview, November 11, 2014).

Regarding adding responsibilities to an existing role, a view was that a process-oriented person would be required - for example, a records manager, compliance manager or possibly a legal secretary (OP5, Interview, December 10, 2014). LP10 (Interview, January 27, 2015) held that the additional responsibilities for the IO could be added to the person involved with requests under PAIA. Related to this is the view that the various teams within the organisation should be in close contact regarding compliance, and that a team should be assembled of stakeholders working on compliance (OP5, Interview, December 10, 2014). This would ensure that the various teams have their requirements for compliance met.

Only two respondents commented on the possibility of delegation of authority in terms of the IO's role. One view was that deputy-IO's should be appointed with clearly demarcated responsibilities and accountability (OP5, Interview, December 10, 2014). The following caveat

was added that the role of IO is not an IT function: “you don’t give the job of information officer or deputy information officer; ... to the IT” (CP5, Interview, January 20, 2015).

### 4.2.5. Concluding the pertinent factors for staff in preparation for POPI compliance

Data presented suggests that all roles within an organisation require some form of preparation in compliance with the POPI Act. This could vary between mere awareness of the Act’s requirements to the extensive day-to-day changes necessary for preparation for compliance. Data regarding use of consultants for preparation for compliance, and various factors that come to light if external staff are used were presented. Factors relevant to staff responsible for the IT of an organisation are presented. A large burden will rest on IT professionals in preparation for compliance with the POPI Act. An important factor to preparation for compliance is the question of hiring a dedicated Information Officer. Data suggests various options for this.

## 4.3. The anticipated costs in preparation for compliance

Various factors regarding cost are presented in this section. Opportunities for cost-saving emerge as being possible. The following are the elements of the analytical framework that are applicable to cost: 1.) Compliance costs, 2.) Direct labour costs, 3.) Implementation costs, 4.) Equipment costs and 5.) External service costs.

### 4.3.1. Compliance costs

Respondents OP1 and CP1 foresaw that new solutions would need to be implemented. For both these would be, in the emphatic words of CP 1, “the downright cheapest solution” (CP1, Interview, November 5, 2014). OP1 (Interview, October 13, 2014), further, suggested that electronic forms would be used to save on printing costs, and electronic mailing to process automated consent and opt-in confirmations. These all imply costs in preparation for compliance.

Five respondents considered costs an inhibiting factor for many organisations. A complete, holistic, data protection and information management approach is thus unlikely to be sought, despite the knowledge that compliance, whatever the initial costs, will mitigate potentially heavy fines from the regulator (CP3, Interview, November 21, 2014). Organisations will also need to choose whether to make a large investment in preparing to comply with POPI or risk a fine that, while less in monetary terms, nonetheless comes with possible reputational damage (OP5, Interview, December 10, 2014).

LP6 (Interview, December 10, 2014) foresaw a cost in implementing new systems or changes to existing ones, as well as the hardware those systems run on: “they will probably get more up-to-date hardware and software. There will be more spending on that”.

Security enhancements are also expected to incur costs. Protecting certain types of data will cost more, as the POPI Act is specific about special personal information that needs to be safeguarded:

> …if you are going to be dealing with sensitive data on the scale of a private school or a medical aid or a bank you have to factor in that there are going to be costs to protect that particular type of data (LP6, Interview, December 10, 2014).

The cost in preparation for compliance is also based on the size of organisation in question; bigger companies can budget millions, but, in the extreme view of CP5 (Interview, January 20, 2015) a small company might not spend more than they would on a mobile phone contract.

### 4.3.2. Staff costs and training

It is costly to hire specialized skills in preparation for compliance, though a contrary view was that compliance will not be a full-time role, and that millions in consulting fees could be saved if carried out by a person in the right part of the organisation (CP2, Interview, November 11, 2014).

Staff costs could rise, as the Information Officer would grow from an individual into a whole department (OP4, Interview, November 24, 2014). OP6 (Interview, January 15, 2015) agreed that an Information Officer would need to be hired in bigger companies, but for smaller companies this role could be outsourced, as is already the case with the Compliance Officer. Thus, the costs of consultants will need to be considered.

A further cost will be that of training where it is a fulltime role, which may require more than one person (OP1, Interview, October 13, 2014). LP6 (Interview, December 10, 2014) agreed: “I do think that there will be a lot more training … provided”.

### 4.3.3. Security costs

Protecting information will be costly:

> …we are going to shred a lot of information that we already have which we don’t need, because it is expensive to protect .... You must keep it at a locked

door. You must do all sorts of things. Access must be highly controlled, and that kind of thing can be very expensive (OP3, Interview, November 6, 2014).

### 4.3.4. Cost-saving

Another aspect is the positive spin-off of the POPI Act in cost reduction. While there may be a cost in changing systems and processes to enable collection of information, the actual amount of information should be reduced to only the absolutely necessary fields, as required by POPI. Thus, the volume of information will decrease, leading to reduced costs in both storage and also protection. (OP3, Interview, November 6, 2014).

Compliance costs can also be reduced if begun early – even before the POPI Act is fully in effect. If done over a longer period, the need for 'quick-fix' and makeshift solutions would be eliminated. In this way well tested and familiar measures will be in operation by the time the POPI Act is enforced (LP7, Interview, January 12, 2015). However, it is expected that this approach will not be widely adopted, and piece-meal solutions are expected to be the order of the day (CP1, Interview, November 5, 2014).

### 4.3.5. Concluding the cost factor in preparation for compliance

Various aspects of cost in preparation for compliance are presented. These include measures for compliance that will affect the 'spend' of the organisation, cost for staff (possible new roles for compliance) and training of existing staff. A major aspect is seen to be cost of security measures and systems to manage compliance. Despite these, there is the possibility of cost-saving being realised by reducing data collected and other innovation and efficiency measures.

## 4.4. Concluding the data presentation

Data was presented, stemming from the research question: factors pertinent to preparation for compliance with the POPI Act and their effect on the organisation, staff and cost of preparation for compliance.

Factors pertinent to the organisation's preparation for compliance are internal and external. A large part of preparation requires the conditions for lawful data processing to be acted on, particularly security. Internal factors are seen to be more extensive than those external for preparation. A symbiosis is seen between the conditions for lawful processing of information and the internal and external factors.

Regarding pertinent factors for staff in relation to preparation for compliance it is seen that all staff require, as a minimum, awareness of the Act. On the opposite end of the spectrum is that

staff roles are affected severely in the detail of their day-to-day tasks. Also, new roles could be created to cater for the requirements of the POPI Act: possibly an Information Officer, who should be senior enough to drive change in the organisation and have the relevant technical skills for this role. Consultants could be employed for expert knowledge in preparation for compliance.

Various pertinent cost factors were presented. These include staff and training in preparation for compliance and program costs. Strategies for cost-saving can be realised in preparation for compliance.

These are the areas in which data was presented in regard to factors pertinent to compliance with the POPI Act. They stem from the research question. These are the factors pertinent to the organisation; staff; costs in preparation for compliance, and lastly, data that emerged relevant to the preparation for compliance efforts.

# CHAPTER 5: ANALYSIS OF DATA AND FINDINGS

Data regarding the effect of pertinent factors in preparation for compliance with the POPI Act on the organisation, staff, together with the anticipated costs, was presented in chapter 4. This chapter will present analysis of this data, and also a proposal for a simple model for preparation for compliance based on that.

## 5. Analysis of the pertinent factors

Analysis is undertaken by means of Thematic Analysis. As seen in chapter 4, Data Presentation, themes emerged as data was grouped, presenting all views that arose within the application of the analytical framework. The present analysis explores these.

### 5.1. The effect of pertinent factors in preparation for compliance on the organisation

Elements of the analytical framework relevant to the organisation were: 1.) Identify internal and external issues, 2.) Determine the scope of compliance, 3.) Establish compliance policy, 4.) Identify compliance obligations and evaluate risks, 5.) Plan to address compliance risks and to achieve objectives, 6.) Operational planning and control of compliance risks from ISO 19600 Compliance Management Systems and 1.) administrative procedures, 2.) physical safeguards, 3.) technical security services and 4.) technical security mechanisms from ISO 27002 Information Security.

#### 5.1.1. Internal and external factors

Recalling from chapter 4 internal factors are processes, systems and security within the organisation while the external factors deal with clients and service providers outside of the organisation. Data regarding both internal and external factors affecting preparation for compliance showed that the internal effects would be the greater of the two, requiring more major process changes. According to Jacobsen (2013, para.3) it would be necessary to revisit all stored personal data to ensure its compliance. This naturally would be a major (internal) factor in preparation for compliance. A number of interviewees voiced concern about retrospective compliance noting that, although most international laws do not apply retrospectively, they may nonetheless have a retrospective effect. For example data already collected would need to be compliant going forward for it to be allowed to be used legally.

Another major area of internal and external compliance is consent. This arises out of the retrospective effect of the Act. It could be a major task, depending on the size of the database.

It could also be an opportunity to shed data that could be outdated. This could be a large amount, with considerable impact initially, but beneficial in the longer term. One view was that consent might not be required, but instead some form of proof of compliance in order to collect, process, store and use the data subject's personal information. Thus consent is required and this was a majority view.

The meaning of consent and its history is outlined by Whitely (2009, p.5):

> Consent to the processing of personal data is probably the most important mechanism that currently exists for determining how and when this data can be used. The notion of informed consent, for example, originated in the context of medical research and the development of the Nuremberg Code which clearly established the right to withdraw from medical research, effectively revoking any consent that was given or implied.

The requirements for consent have been amplified in new legislation in the UK. The previous Data Protection Directive 95/46/EC relied on an "opt-out" (Maldoff, 2016) i.e. implicit consent, but with the new GDPR "a statement or a clear affirmative action" is now required. The UK is seen as a leader in data privacy so this change may spread further afield, tightening up privacy controls of the legislation in other countries, including South Africa.

The external aspect of consent is that the process of rectifying a database would require contact being made with a data subject, and a reproducible form of consent obtained. This would be costly in terms of both time and staff. The retrospective effect of the Act is apparent.

### 5.1.2. Juristic persons

Chapter 4 presented three areas where respondents considered POPI unique: that juristic persons are covered under the Act; protection for account numbers, and requirement for consent. Of these, the inclusion of juristic persons was considered foremost, this for three main reasons:

- Intellectual property and company laws,
- Small businesses indistinct from the owner, and
- Rights derived from the Constitution.

The first two views are similar. If inclusion of juristic persons were due to company or intellectual property laws, there would be some reference to this. If the original Act were not

up to standard in this regard an amendment would be included under 'Laws Amended By Section 110'. Secondly, POPI is relevant to both larger organisations and those that are indistinct from their owners. This reason is thus invalid unless, as in the case of the CPA, the minister sets a threshold for the POPI Act to be applicable. This is detailed shortly.

The last view, is that juristic persons are covered under POPI due to the Constitution. The Bill of Rights, section 8 – 'Application' in (2) states:

> A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right; and (4):

"A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person" (RSA, 1996). These extracts illustrate how the Constitution makes provision for juristic persons to be protected by its rights.

Other laws were examined for provisions relevant to juristic persons. The South African Institute of Chartered Accountants (SAICA) notes that the National Credit Act (NCA) has aspects relevant to juristic and natural persons (Kendall & Dijkman, 2007). SAICA also notes that under the CPA a threshold for transactions is set for juristic persons by the Minister of Trade and Industry where the Act will not apply. This threshold is R2 million (SAICA, n.d. b).

These two Acts indicate that POPI is not unique in South African legislation in its inclusion of juristic persons, although it is unique internationally in terms of privacy. This lends plausibility to the reasoning that POPI is merely extending the Constitution's rights to juristic persons.

### 5.1.3. Conditions for lawful processing of information

As seen in the data presented in chapter 4 the conditions for lawful processing of information comprise a major factor in preparation for compliance with the POPI Act. The elements of the analytical framework are addressed here in terms of compliance and security (security is one of the conditions). Data showed that compliance with the conditions is adequate for compliance with the Act. As presented in the literature review (Chapter Two), most of the material available speaks of the conditions to the exclusion of other sections of the Act. The conditions for lawful processing of information is considered as being of great importance. Literature and data collected agree in this regard.

Security is one the eight conditions in the Act and was seen to be highly important in preparation for compliance in terms of the organisation, staff and cost. The ISO 27002 standard

was included in the analytical framework, and this, too, highlights its importance. Closely aligned with security is governance and the King codes of governance in respect of data protection. King IV (the fourth edition of the codes of governance) stresses that IT governance and security should be on the agenda of the Board of an organisation (Crest Advisory Services, 2017). This clearly highlights its importance for the organisation, and the seriousness that should be accorded to this.

### 5.1.4. Evaluating risks

Retrospective compliance with the POPI Act was presented as an area of risk due to the profound effect that this could have on the organisation. It would have direct bearing on staff and costs of preparation for compliance. The conditions for lawful processing of information are key to compliance with the POPI Act. Their retrospective effect constitutes a risk for various reasons.

As far as Accountability the processing of information collected both before and after the enforcement date will need to comply with the conditions for lawful processing of information. Regarding the Processing Limitation condition both old (currently stored) and new (to be collected) information will need to be processed reasonably. Consent will need to be producible if required, or else this information should not be used. Reproducible consent would be required to be obtained should it not have been done previously. Conditions around direct collection from data subjects could have the effect of invalidating a database that was not collected from the individuals themselves.

On the Purpose Specification where information is used for purposes other than what it was collected for, it needs to be stopped. Information collected previously should be deleted or de-identified once its purpose for collection is no longer in effect. This poses a risk as currently held information will need to be assessed for this and dealt with accordingly.

For the Further Processing Limitation both old and new information should be processed further only if this meets the purpose for which it was collected. Otherwise, consent is required, which may be challenging if it was collected over years or is large in volume. If the Information Quality condition is to be met both old and new information should be verified as correct, with procedures in place for this to be carried out at regular intervals - a challenge for databases built over many years, involving many data subjects. The Openness condition requires information pertaining to the responsible party should be made known to the data subject, as well as how their information is being used and processed. Data subjects should also be

informed of third parties who process the information, and whether the information is transmitted across borders, consent to these would be required. Adequate Security Safeguards should be in place in order to protect both old and new information. Lastly, Data Subject Participation affects both old and new information and would be a challenge for information is out of date and data subjects cannot be contacted. This would require deletion or de-identification to take place and the information to be used.

### 5.1.5. Corporate and data governance

The concepts of corporate and data governance were introduced in the literature review (chapter 2). As presented earlier, the King IV code of governance institutionalised corporate governance in South Africa. Data regarding the King code was presented in chapter 4 (Data presentation) particularly with regard to security. The relationship between the code of governance and the POPI Act is shown in the following quote: "King IV Code requires that all governing bodies must ensure that their organisations are protecting the privacy of personal information" (Cilliers, 2017, para.3). Based on the definition presented in chapter 2 of data governance the POPI Act is a key tool in ensuring a high standard of data governance. As the governance code is voluntary and data governance dependent on what a given organisation deems necessary, the POPI Act could function as a binding minimum standard across all organisations.

A further component of governance is the internal audit function. Often seen as a financial function, this can be harnessed to provide oversight for compliance for the organisation also. Jones (2013, p.18) suggests that "typically, the internal audit function will lead the compliance audits and ensure that the organization is compliant with laws and regulatory provisions". Schneider (2008) adds that the internal audit function assesses the organisations risk and determines if adequate controls are in place and that they are effective.

Inertia is a reasonably well-known term conveying a state of being at a state of rest or of resisting change (The Physics Classroom, n.d.). With regard to the organisation Pfeffer (1997, p.86) defines inertia as "the inability for organizations to change as rapidly as the environment". Change can result in this inertia being overcome and this can be by means of internal or external forces or changes (Huber, Glick & Sutcliffe, 1993). Legislation could be considered an external force or change that requires compliance such as the POPI Act. There will be a high probability of structural changes needing to be made to adequately comply with the Act. This may however only be possible in larger organisations who can budget for new

functions and roles being created in the organisation structure. If an organisation were to begin or create an internal audit or compliance function this would affect the organisation in terms of its structure and implies the need for additional roles and tasks. An organisational change to accommodate legislative compliance is a major undertaking. As seen in data presented this role or function could be placed anywhere in the organisation up to board level and could result in considerable cost.

This falls under the ambit or organisational theory due to structural changes as presented in chapter 2. Jones (2013, p.6) confirms the notion of structure change with the following "In order for organizations to respond to the environmental changes and forces, it is often necessary to revamp the strategy and reorganize the structure".

### 5.2. Assessing pertinent factors in staff preparation for compliance

Elements of the analytical framework regarding staff were 1.) Identify interested parties' requirements, 2.) Leadership commitment, independent compliance functions, responsibilities at all levels, support functions. Data presented showed that all staff had a role to play in preparation for compliance even if just for informational purposes. IT orientated roles would be affected quite heavily as they would acquire additional tasks. Preparation for compliance was seen to be a top down initiative as a senior decision maker should ensure the organisation would take the necessary steps to prepare for compliance. Some suggestions from interviewees are that a board level or executive level appointment would be necessary. Thus, leadership commitment to the process would be ensured. This aligns with the King code of governance which makes governance structures in an organisation accountable for protection of personal information. Leadership should be actively involved in compliance with the POPI Act and senior staff are to drive the process. As seen earlier the King code suggests that data protection should be on the Boards agenda.

Data suggested that a compliance function could take responsibility for preparation for compliance with the POPI Act and thus this could be seen as independent. All teams and individuals would need to ensure that their area of responsibilities is compliant with the Act and not just IT. Literature and data collected are in agreement with this. This falls within the bounds of the analytical framework also as well as organisational theory and structural change.

## 5.3. Assessing the cost factor in preparation for compliance

The factors pertinent to cost from the analytical framework are 1.) Compliance costs, 2.) Direct labour costs, 3.) Implementation costs, 4.) Equipment costs and 5.) External service costs. Various anticipated costs were presented that agree to the analytical framework. Compliance costs were seen as being inhibiting to many organisations. Direct labour costs and external service costs are seen with regard to staff where new roles would be required for preparation for compliance and rectification of currently held information which is anticipated to be staff intensive. Consultants are external professionals that should be engaged in drawing up a plan for preparation for compliance and even to perform certain tasks that internal staff were not skilled to or did not have capacity to undertake. Implementation speaks to the new systems and processes required for preparation for compliance with the Act. Along with this is an anticipated requirement for new hardware for this specific application. Data presented shows that costs are a determining factor is preparation for compliance as costs could be prohibitive. This is especially so for staff and external service providers i.e. consultants. Consultants are seen to have the rounded knowledge on the various factors for a compliance program and insight into the Act. While costly, consultants typically have previous compliance experience as well as perspective on a number of industries and contexts (unless specialised in particular sectors) and this could provide valuable insight into the effort of preparation for compliance.

## 5.4. Simple model for compliance

The following simple model for compliance with the Act is drawn up from the relevant literature and data presented in this study. There are two main legs to this model. Firstly overarching concerns and secondly specific measures.

In terms of overarching concerns related to compliance an appropriately senior person should be identified in order to drive the compliance process and project, this will ensure access to key decision makers within the organisation and allow for changes to be made organisation wide as needed. Further a compliance team should be assembled to represent all stakeholders in the process of compliance from all areas of the organisation that are affected by the Act.

Specific measures to ensure compliance reside in two key streams. These are getting current information compliant and ensuring compliance of any new information being collected. The factors that this is relevant to are consent, the necessary information, security, purpose of collection, correctness of the information and lastly regarding operators, third parties and cloud storage.

Consent should be sought for information currently held (or deleted or de-identified should it not be possible) and any new information collected should have the appropriate consent collected at time of collection and data should be collected directly from the data subject. Only the necessary information should only be collected for the specified purpose. Current information that is not necessary for the purpose required it should be deleted or de-identified. New information should be kept to the minimum required for the purpose specified. Regarding security all information should be adequately protected from both within and without the organisation and limited to only persons who require access to this.

The purpose that information was collected for determines the period information should be kept for, if the purpose has come to an end then the information should be deleted or de-identified. The correctness of information should be checked at regular intervals and some mechanism for users to verify their information should be in place. Lastly should operators, third parties or cloud solutions be employed a verification of their services should be conducted to ensure that the data in their care is appropriately dealt with and that data subjects are made aware of the chain of processing undertaken to their personal information.

### 5.5. Conclusion of analysis

Data collected was presented in Chapter Four and analysed in Chapter Five in relation to the analytical framework. As with Chapter Four, this chapter was structured to mirror the research question and sub questions.

Analysis was conducted on the conditions for lawful processing of information due to the analytical framework providing a number of elements related to compliance. The conditions were noted as being adequate for compliance. The analytical framework also made provision for risks to be assessed and addressed. The retrospective effect of the POPI Act was presented as a risk and the application of this to the conditions for lawful processing of information was presented. Corporate and data governance for the organisation was traversed also in this analysis. It was concluded that the POPI Act would be an enforceable standard for data protection as it was the only legally binding mechanism (when it is in effect), as the codes of governance are not legal instruments that could be enforced.

The analytical framework with regard to staff presented two elements, the first being the identification of interested parties' requirements and leaderships responsibility for compliance. All staff have a role to play in preparation for compliance and should evaluate the Act in terms

of their responsibilities and compliance should be conducted by a multi-disciplinary team that is able to ensure requires for the whole organisation are met. The King IV code of governance stresses that data protection should be on the boards agenda as such this makes a strong case for leadership to be intricately involved in preparation for compliance and on an ongoing basis.

Regarding anticipated cost for compliance the analytical framework made provision for a number of factors including costs of staff (wages), external services, implementation, equipment and compliance costs. Data showed that staff costs are an area where attention would need to be given and stands to affect the organisation in its compliance effort. The cost of external service providers while possibly exorbitant are worthwhile due to the range of expertise brought to the table in compliance with the Act.

Based on data collected and analysis presented the chapter concluded with a simple model for compliance being put forward. This shows the POPI Act being complied with in two streams, firstly addressing information currently stored and factors for compliance that affect current databases and secondly measures to be addressed for new data collected. Current data is said to be the starting point by Jacobsen (2013). Other sources begin with the take on of new data. The Researcher believes both are equally important in preparation for compliance with the POPI Act.

## CHAPTER 6: CONCLUSION - RECAPPING THE RESEARCH

This chapter discusses the research undertaken and notes areas for further study. There are six chapters in all. The first chapter introduced the study. The second chapter assessed relevant literature, highlighted relevant concepts and the theoretical framework. The third chapter describes the research methodology, which includes the methods undertaken in carrying out the research and the choice of the data collection tool. The fourth chapter presented the data collected and is structured to mirror the research question. The fifth chapter analyses the data collected. The conditions for lawful processing are related to process changes (internal and external), retrospective effect of the POPI Act is noted as a risk. The Acts relevance to juristic persons is assessed. Lastly, the present chapter concludes the study, highlighting the main findings and areas for further study.

### 6. Revisiting the research

This study sought to understand the effect of preparing to comply with POPI on organisations, on staff involved in preparation for compliance and the costs anticipated in preparation for compliance.

Qualitative research methods were employed in conducting this exploratory study specifically constructivism. The tool for gathering data was the formal semi-structured interview. Twenty-four interviews were conducted, with three main types of interviewee – legal professional, consultants offering services related to the POPI Act and operational staff involved in compliance. Interview lengths ranged from twenty minutes to an hour-and-a-half. Seventeen were conducted face-to-face, and seven by Skype calls.

Significant effects are expected internally and externally in preparation for compliance with the POPI Act. These include how information is collected from data subjects, and then processed and stored. The conditions of lawful processing are a major concern: process changes must be implemented to prevent falling foul of the law.

Retrospective compliance is a concern in preparation; not in the true sense of retrospective laws, but rather the retrospective effect of the POPI Act where data collected before its commencement will still need to comply. This could essentially invalidate an entire database of personal information as it risks being unusable. This is seen as a risk factor.

## 6.1. Addressing of the research problem

This study set out to identify pertinent factors in preparation for compliance with the POPI Act with regard to the organisations, staff and cost anticipated in compliance and the effect of these due to a lack of deep understanding evident in the literature and in practice. The analytical framework adopted to guide this study was a combination of two ISO standards – 19600 and 27002, these being compliance management systems and information security. A third component was added to address costs of compliance with use of OECD's Cost Compliance Assessment being included.

A mapping of the research question and sub-questions to the elements of the analytical frameworks employed in this study was presented in chapter 2 and 3. In summary, the ISO 19600 compliance management system standard encompasses elements such as the identification of internal and external issues, determining scope of compliance, addressing risks and various security safeguards from ISO 27002 dealing with security procedures, technical services and mechanisms. These are pertinent to the organisation and sub-question 1.

Sub-question 2 was addressed by ISO standards also. ISO 19600 elements were identification of interested parties requirements and leaderships role in compliance, having an independent compliance function and responsibilities at all levels of the organisation, these are pertinent to staff.

Lastly sub-question 3 was guided by the OECD's Compliance Cost Assessment (CCA). The elements of this that are pertinent to this study are compliance costs, direct labour costs, implementation costs, equipment costs and the cost of external service costs.

## 6.2. Addressing the research question and sub questions

The effect of the factors pertinent in preparation for compliance with the POPI Act on the organisation, staff and anticipated costs are seen to be substantial. From the analytical framework it was presented that the conditions for lawful processing of information are central to preparation from compliance in terms of the identifying compliance measures. Another component of the framework in this regard is the identification of risks and due to the retrospective effect of these conditions are a substantial risk that should be mitigated in preparation for compliance. Internal and external factors were identified specifically, and this aligns to the analytical framework. Internal factors are seen to be more taxing than those external. Internal factors are staff, security, process and system changes to comply with the

Act. The external factors are related to clients and service providers and the interaction of the organisation with them. Security is vital to privacy and an additional element was added to the analytical framework for this. More data was collected regarding security than any other of the conditions for lawful processing of information. Plans should be enacted to counter these factors depending on the applicability to each individual organisation.

The next element of the analytical framework and sub question 2 relates to staff. Every staff member should have a minimum level of knowledge of the POPI Act. A number of roles where the preparation of compliance will affect directly are noted. Particular emphasis was on IT professionals who work with data once collected and are required to ensure correct usage and security measures are in place to comply with the Acts provisions.

Cost is key to compliance with the POPI Act as such the OECD Cost Compliance Assessment was included as part of this studies analytical framework. Larger organisations could layout millions of Rand to budget for compliance, but small companies were said to only be able to pay as much as for a mobile phone contract. Staff and security measures will cost to implement and maintain compliance with the Act. Cost for external service are potentially well spent due to well-rounded expertise that could be expected from a consultant or consultancy.

## 6.3. Contributions to the body of knowledge

Aspects of the study have made additions to the body of knowledge:

### 6.3.1. Selection of interviewees

While many legal experts in the ICT Law sector participated in interviews for this study, there was value in also interviewing drafters of the POPI Act. This shaped the conclusions, some of them contradicting the majority view but carrying higher weight due to having been involved with actually writing the POPI Act and brought a deeper understanding of the effect of the Act. An effort should be made to look deeper into minority views expressed, as the majority could well be incorrect in some instances.

### 6.3.2. Analysis of data

A number of tools exist for the coding and grouping of data such as QDA, Miner and Atlas.Ti. These have varying costs associated with usage. The Researcher would suggest that a spreadsheet be used in the same manner as in this study. Many have the Microsoft Office suite of products and this makes collaborative work more easily done without needing to worry about other software packages, operating systems and compatibility. Spreadsheets are simple to use

for most people so there should not be a steep learning curve in harnessing this in the research process.

### 6.3.3. Simple compliance model

A simple model for compliance with the POPI Act was presented which covers the main areas that emerge as key to an organisations compliance. While not extensive this captures the main concerns and areas in preparation for compliance with the Act.

The salient points of this model are that it is preferable for a senior staff member to drive the compliance effort and that a team or committee should be formed to guide the process thereby ensuring that all teams requirements are considered. This constitutes the overarching concerns related to compliance.

The next section of the model deals with the handling of data currently held and data that will be collected. This has implications for consent, only necessary information should be stored (current and future), this information can only be used for a specific purpose and only kept for as long as this purpose was valid and lastly information security should be adequate.

## 6.4. Applicability of the research

This research is applicable to a wide audience. The POPI Act has very few exceptions in its application. The study presented data suggesting that all staff be familiar with the POPI Acts provisions in order to be aware of possible transgressions, and also noted many industries that would experience repercussions of preparation to complying.

## 6.5. Limitations of this study

Respondents who participated in the interviews that informed this study were categorised into three groups, each group would provide a particular emphasis based on their perceptions and experience with the POPI Act. The three groups were legal professionals who advised clients in some way or other on compliance with the Act, consulting professionals who provided technical services in complying with the Act and lastly operational professionals involved with compliance for their respective organisations.

Regarding the legal professionals two were part of the South African Law Reform Commission project team who drew up the Act. This group was well represented in that members of large law firms, IT Law specialist practises and smaller legal consultancies participated. However when looking at the consulting professionals group many were from smaller consultancies and not the well-known consulting houses (yet some were part of large consultancies earlier in their

careers). This is a limitation as their experience in large compliance projects or at large organisations could been seen to provide greater insight into the preparation for compliance with the Act. For operational professionals this was similar. Three respondents were from NGO's, two from an insurance company, another from a university and two from specialist technology companies, none were from large organisations that could provide insight on some of the complexities in those environments.

Secondly, the study focussed on South Africa and only respondents based in the country were requested to participate. The law is comparable with international standards and similar compliance measure could be employed but due to limiting this to the local context this could not be expanded on.

Lastly the model proposed is a basic model for compliance and covers the main areas of compliance with the POPI Act.

### 6.6. Suggestions for future research

Because the POPI Act is new, it will no doubt be the subject of many future studies. This study raises a number of possible topics. The provisions of the POPI Act might be studied in terms of other jurisdictions laws, thus determining its international validity. Already a growing common privacy legislative base can be seen developing. Exceptions could be compared to determine whether a better standard could be applied. This will be seen where provisions are adjudicated in a similar way or not and in changes to other legislation an example is the GDPR tightening opt in provisions.

This study showed that compliance with the POPI Act would hinge on the conditions for lawful processing of information. Further studies could confirm if this is in fact the case once the regulator has been up and running for a period. Future studies can also be undertaken when the POPI Act is fully in forced to understand how the POPI Act is being applied to juristic persons.

The POPI Act may seemingly lead to innovation and cost saving and as such this would be a beneficial areas of future study. This emerged in this study anecdotally and a future study may be able to verify if this is the case and to what degree it was possible.

On a general note, a potentially fruitful area of future study would be an attempt to reach consensus on a single, commonly-held definition of privacy, in contrast to the present spectrum of understanding of the concept. This could be of incredible benefit and value to future legislation by having a comprehensive definition.

## REFERENCES


Abuor, M.A. (2016). *Urban poverty and the child's right to privacy: a case study of Kibera - Nairobi*. University of Nairobi. Retrieved from http://erepository.uonbi.ac.ke/

Abraham, J., & van Welie, R. (2016). Global B2C E-commerce Report 2016. The Ecommerce Foundation.

Agre, P. E., & Rotenberg, M. (1997). *Technology and Privacy: The New Landscape.* MIT Press.

Armerding, T. (2018, January 26). *The 17 biggest data breaches of the 21st century.* Retrieved from https://www.csoonline.com

Australian Law Reform Commission [ALRC]. (n.d.). *Introduction to the Inquiry, The meaning of Privacy.* Retrieved from https://www.alrc.gov.au/publications/1.%20Introduction%20to%20the%20Inquiry/meaning-privacy

Bace, J., Rozwell, C., Feiman, J. & Kirwin, B. (2006). Understanding the costs of compliance. *Gartner Research*, ID Number: G00138098.

Backman, P., & Levin, K. (2011, January 31). *Privacy breaches – impact, notification and strategic plans.* Retrieved from http://www.lexology.com

Banisar, D., & Davies, S. (1999). Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. *John Marshall Journal of Computer & Information Law Volume XVIII.*

Bennet, C. J. (1992). Regulating Privacy: Data Protection and Public Policy in Europe and the United States. *Cornell University Press*

Bennett, S. (2013). *A Brief History Of Social Media (1969-2012*). Retrieved from http://www.adweek.com

Bish, J.J. (2016, January 11). *Population growth in Africa: grasping the scale of the challenge.* Retrieved from http://theguardian.com

Bleker, S., & Hortensius, D. (2014). ISO 19600: The development of a global standard on compliance management. *Business Compliance* 02/2014. *Baltzer Science Publishers*

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3,* 77-101.

Britnell, L. (2008). *The Changing Face of Identity Theft.* Retrieved from https://www.ftc.gov

Britz, J. J. (1996). Technology as a Threat to Privacy: Ethical Challenges and Guidelines for the Information Professional. *Microcomputers for Information Management, volume13* p175-93.

Brown, R.B. (2006). Doing Your Dissertation in Business and Management: The Reality of Research and Writing. *Sage Publications,* p.43.

Buecker, A., Amado, J., Druker, D., Lorenz, C., Muehlenbrock, F., & Tan, R. (2010). IT Security Compliance Management Design Guide with IBM Tivoli Security. *IBM Redbooks* pg. 417

Burchell, J. M. (1998). Personality Rights and Freedom of Expression: The Modern Actio Injuriarum. *Juta and Co Limited.*

Burchell, J. (2008). The Legal Protection of Privacy in South Africa: A Transplantable Hybrid. *Electronic Journal of Comparative Law, vol. 13*.1.

Cain, A. (2016, June 1). 60% of hiring managers look up candidates online — here's how to make sure your Facebook profile doesn't cost you a job. Retrieved from http://www.businessinsider.com

Cilliers, H. (2017, August 21). *King IV and data security*. Retrieved from https://accountingweekly.com

Clarke, R. (2013, July 24). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms.* Retrieved from http://www.rogerclarke.com/

Cohen, S. (2017, November 17). *Privacy Risk with Social Media*. Retrieved from http://www.huffingtonpost.co.za

Coral, C., & Bokelmann, W. (2017). *The Role of Analytical Frameworks for Systemic Research Design, Explained in the Analysis of Drivers and Dynamics of Historic Land-Use Changes*. Department of Agricultural Economics, Thaer-Institute, Humboldt-University Berlin, 10099 Berlin, Germany

Crest Advisory Services. (2017, September 16). *Professor Mervyn King on POPI and Corporate Governance.* Retrieved from: http://crestadvisoryafrica.com/wp/index.php/2017/09/16/professor-mervyn-king-on-popi-and-corporate-governance/

Creswell, J. W. (1994). Research design: Qualitative and quantitative approaches. *Thousand Oaks, CA: Sage Publications.*

Creswell, J. W. 2003. Research Design: Qualitative, quantitative and mixed methods approaches. 2nd ed. *Thousand Oaks, CA: Sage Publications.*

Croft, N.H. (2017). *The Role of ISO Standards in Governance, Risk and Compliance Management for Today's Business*. Retrieved from http://www.hkqaa.org

Crossman, A. (2017, March 18). *Understanding Purposive Sampling.* Retrieved from https://www.thoughtco.com/

Currie, I. (2010). *The Protection of Personal Information Act and Its Impact on Freedom of Information.* Retrieved from University of the Witwatersrand (WITS): http://www.wits.ac.za

Davies, M. (2017, October 17). *Data breach: Millions of South Africans' personal info exposed.* Retrieved from http://www.huffingtonpost.co.za

De Stadler, E. (2013, November 7). *Direct marketing: Does POPI or the CPA apply*? Retrieved from http://www.sibergramme.co.za

Dhont, K., & Woodcock, K. (n.d.). *South Africa Enacts New Data Protection Law.* Retrieved from http://www.lorenz-law.com

Dixon, P. (2008, January 4). *A Brief Introduction to Fair Information Practices.* Retrieved from https://www.worldprivacyforum.org

DLA Piper (n.d.). *Data Protection, Privacy and Security*. Retrieved from https://www.dlapiper.com/en/czech/services/intellectual-property-and-technology/data-protection-and-privacy/

Eger, J. (2006, April 2). Controlling Government Abuse of Our Right to Privacy. Retrieved from http://www.govtech.com

Ellis, C. 2004. The Ethnographic I: A Methodological Novel about Auto-ethnography. *Walnut Creek, CA: AltaMira Press.*

EPIC. (2002). *Privacy and Human Rights*. EPIC, DC.

Ericsson (2015, November). *Mobility Report*. Retrieved from https://www.ericsson.com/

Etzioni, A. (2008). The Limits of Privacy. *Basic Books.*

EY, (n.d.). *ISO 19600 International standard for compliance management.* Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-iso-19600-international-standard-for-compliance-management/$FILE/EY-iso-19600-international-standard-for-compliance-management.pdf

Farha, R., Sekeris, E., & Hermansson, D. (2017). *The hidden cost of reputation risk.* Retrieved from http://www.oliverwyman.com.

Ferris, J.M. (2012). *The ISO PIA Standard for Financial Services.* In: D. Wright, P. De Hert. (Eds.), Privacy Impact Assessment. Law, Governance and Technology Series, vol 6. Springer, Dordrecht

Flynn, M. W. (2013, February 15). *Ex Post Facto.* Retrieved from https://www.quickanddirtytips.com

Food and Agriculture Organisation [FAO]. (n.d. a). *Session 1. Organizational theories*. Retrieved from http://www.fao.org/docrep/w7503e/w7503e03.htm

Food and Agriculture Organisation [FAO]. (n.d. b). *Tool 9: Semi-structured interviews*. Retrieved from http://www.fao.org/

Foord, K. (2000). Defining Privacy. *Victorian Law Reform Commission.*

Glenn, D. (2012). *The History of Social Media from 1978-2012*. Retrieved from http://www.adweek.com

Graziani, R. (2012). IPv6 Fundamentals: *A Straightforward Approach to Understanding IPv6*. CISCO Press.

Guba, E., & Lincoln, Y. (1989). Fourth generation evaluation. *Newbury Park, CA: Sage.*

Hafetz, J. L. (2002). “A Man's Home is His Castle?": Reflections on the Home, the Family, and Privacy During the Late Nineteenth and Early Twentieth Centuries. *William & Mary Journal of Women & Law Volume 8 Issue 2*

Hale, B. (2015). The History of Social Media: Social Networking Evolution! *History Cooperative.*

Hancock, B. (1998). An Introduction to Qualitative Research. *Trent Focus Group.*

Harvard University. (n.d.). *Research Methods: Some Notes To Orient You*. Retrieved from http://isites.harvard.edu

Hirsch, D. D. (2011). The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? *Seattle University Law Review Volume 34 Number 2.*

Henderson, A. (2017). *The 10 steps to achieving a data privacy compliance framework.* Retrieved from https://insights.redflaggroup.com

Henderson, C. (n.d.). *The history of communication technology: telephone*. Retrieved from http://www.personal.psu.edu

Hendriks, D. (2013, May 8). *Complete History of Social Media: Then And Now*. Retrieved from https://smallbiztrends.com

Heywood, D. (2014, November). *Google Spain and the 'right to be forgotten'*. Retrieved from https://united-kingdom.taylorwessing.com/

Huber, G. P., Glick, W.H., Sutcliffe, K.M. (1993). *Organizational Change and Redesign: Understanding and predicting organizational change*. New York: Oxford University Press.

Hughes, A. (2014). *Human dignity and fundamental rights in South Africa and Ireland*. PULP

International Standards Organisation [ISO] (n.d.). Retrieved from https://www.iso.org/about-us.html

Internet World Stats. (2015). *Internet Usage Statistics for Africa*. Retrieved from http://www.internetworldstats.com

Jacob, S. A., & Furgerson, S. P. (2012). Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research. *The Qualitative Report, 17(42), 1-10.*

Jacobsen, P. (2013). *POPI compliance is a steep, uphill climb for direct marketers*. Retrieved from http://webtechlaw.com

Jacobsen, P. (2014). *Don't place too much emphasis on the Protection of Personal Information Act.* Retrieved from http://webtechlaw.com

Jones, K. K. (2013). *The Impact of Legislation on the Organization: Evaluating the Impact of Corporate Governance Regulation on the Internal Audit Function.* Dissertation, Georgia State University.

Jordaan, N. (2016). *JSC recommends special leave for Facebook judge after social media uproar*. Retrieved from http://www.timeslive.co.za

Kendall, M., & Dijkman, J. (2007, September). Regulations regarding the Promotion of Access to Information Act. *SAICA Techtalk Issue 140.* Retrieved from https://www.saica.co.za/

Kolver, L. (2014, March 6). *SA businesses not ready for POPI implementation – Grant Thornton*. Retrieved from http://www.engineeringnews.co.za

Kowalczyk, D. (2015). *Purposes of Research: Exploratory, Descriptive & Explanatory.* Retrieved from https://study.com

KPMG. (2013). A practical business response to POPI. Retrieved from http://www.kpmg.com/ZA/en/IssuesAndInsights/ArticlesPublications/Protection-of-Personal-Information-Bill/Documents/Practical%20Response%20to%20POPI-final.pdf

Kroi, I. (2016, April 18). *Practical tips on how to keep up with regulatory changes*. Retrieved from https://www.linkedin.com

Kroi, I. (2017, March 24). *Data protection, a challenge for the legislators, for the entities and for the persons.* Retrieved from https://www.linkedin.com

Kurland, P. B., & Lerner, R. (1987). Amendment 4. *The Founders Constitution Volume 5.*

Kvale, S. (1996). *Interviews: An Introduction to Qualitative Research Interviewing*. Sage Publications.

Liebowitz, S.J., & Margolis, S.E. (1994). Network Externality: An Uncommon Tragedy. *Journal of Economic Perspectives, Volume 8, Number 2.* Page. 133-150.

Leizerov, S. (2013). *Privacy trends 2013, The uphill climb continues.* Retrieved from http://www.ey.com

Licklider, J. C. R., & Clark, W. (1962). On-Line Man Computer Communication. *AIEE-IRE '62 (Spring).*

Linder, D. (2016). *Exploring Constitutional Law*. University of Missouri, Kansas. Retrieved from http://law2.umkc.edu

Lovatt, I. (2016, July 7). *Does GDPR apply to organizations outside the EU?* Retrieved from https://www.bluevenn.com

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society July-September 2014.*

MacKessy, J. (2010, September 23). *Knowledge of Good and Evil: A Brief History of Compliance*. Retrieved from http://post.nyssa.org

Mahoney, A. (2014, August 22). Trade Secret Laws: Competitive Advantages at Work. Retrieved from https://lawstreetmedia.com

Maldoff, G. (2016, January 12). *Top 10 operational impacts of the GDPR: Part 3 – consent*. Retrieved from https://iapp.org/news

Marsh, R. M. (2009). legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet. *Michigan Telecommunications and Technology Law Review, University of Michigan Law School Volume 15 Issue 2.*

Marshall, J. (2012). *A Practical Guide to Writing Clients and Servers.* University of Kentucky. Retrieved from http://www.cs.uky.edu

Masters, J. (2014). What is Internet Governance? Council on Foreign Relations. Retrieved from https://www.cfr.org

Mathison, S. (1988). *Why triangulate? Educational Researcher.* Sage Publications. Retrieved from http://journals.sagepub.com

Maxwell, J.A. (1992). Understanding and Validity in Qualitative Research. *Harvard Educational Review; Fall 1992.*

McCarthy, J.T. (2005). The Rights of Publicity and Privacy. *Minneapolis MN. Thompson West.*

McDowell, H. (2017, April 13). *Banks spent close to $100 billion on compliance last year*. Retrieved from https://www.thetradenews.com

McFarland, M. (2012). *Privacy Norms*. Retrieved from https://www.scu.edu

McNamara, C. (1999). General Guidelines for Conducting Interviews. *Minnesota*.

Meier, G. (2014, July 5). *How POPI Affects Email Marketing.* Retrieved from http://www.bluemagnet.co.za

Michael, R.S. (n.d.). *Measurement: Reliability and Validity, Y520 Strategies for Educational Inquiry*. Retrieved from http://www.indiana.edu

Michalsons Law Firm.(2008, September 25). *Guide to the ECT Act in South Africa.* Retrieved from https://www.michalsons.com

Miller, G. C. (1998). Printing and Publication. In J.M.Stellman. (Ed.), *Encyclopaedia of Occupational Health and Safety, Volume 3.* International Labour Organisation, Geneva.

Miller, G. P. (2017). The Law of Governance, Risk Management, and Compliance. *Wolters Kluwer Law & Business.*

Mills, J., Bonner, A., & Francis, K. (2006). The Development of Constructivist Grounded Theory. *International Journal of Qualitative Methods 5 (1).*

Mitchell, J. (2001). Convergent Communications, Fragmented Regulation and Consumer Needs. In W.H.Melody (Ed.), *Telecom Reform Principles, Policies and Regulatory Practices* (pp. 433-442).

Morris, S. (2015). *4 Phases of a Compliance Management System (CMS).* Retrieved from https://kirkpatrickprice.com

Moyo, A. (2013). *POPI to make life easier for IT*. IT Web. Retrieved from https://www.itweb.co.za

Myhre, J. (2013, August 20). *Technology is invading our privacy.* Retrieved from http://www.dmnews.com

Nargundkar, R. (2008). *Marketing Research: Text and Cases.* 3rd edition, p.38.

Narsee, A. J. (2016). *WhatsApp with the Moegoeng diss, judge?* Times Live Retrieved from https://www.timeslive.co.za

Naude, A. (2014). Data Protection in South Africa : The Impact of the Protection of Personal Information Act and Recent International Developments. *LLM Mini-dissertation, University of Pretoria.*

Ncube, C. (2004). A Comparative Analysis of Zimbabwean and South African Data Protection Systems. *International Journal of Law and Information Technology*

Neethling, J., Potgieter, J. M., & Visser, P. J. (1996). Neethlings Law of Personality. *Butterworths.*

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing,* 18(2), 34-5. DOI: 10.1136/eb-2015-102054

OECD (2014), *OECD Regulatory Compliance Cost Assessment Guidance*, OECD Publishing. Retrieved from http://dx.doi.org/10.1787/9789264209657-en

Ostrom, E. (2009). A general framework for analyzing sustainability of social-ecological systems. *Science*, 325, 419–422.

Parsons, M., & Colegate, P. (2015). 2015 The Turning Point for Data Privacy Regulation in Asia. *Hovell Lovells Chronicle of Data Protection.*

Perez, M. E. (2014). *Presentation, Analysis and Interpretation of Data*. Retrieved from https://www.slideshare.net

Pfeffer, J. (1997). *New Directions For Organization Theory*. New York: Oxford University Press.

Petronio, S. (2015). Communication Privacy Management Theory. *The International Encyclopaedia of Interpersonal Communication. 1–9.*

Pilgrim, T. (2016). *Privacy, Data & De-Identification.* Australian Government, Office of the Information Commissioner. Retrieved from https://www.oaic.gov.au

Posner, R. A.(1981). The Economics of Privacy. *The American Economic Review Volume 71, No. 2 page 405-409.*

Post, R. C. (2001). Three Concepts of Privacy. 89 *Georgetown Law Journal* 2087.

Praxiom. (n.d.). *A brief history of ISO 27002 and ISO 17799.* Retrieved from http://www.praxiom.com/iso-17799-2000.htm

Privacy Rights Clearing House. (2002). Public Records in the Internet: A Privacy Dilemma. Retrieved from

Privacy Rights Clearinghouse. (2016). Social Networking Privacy: How to be Safe, Secure and Social. Retrieved from

Rajasekar, S., Philominathan, P., & Chinnathambi, V. (2013). Research Methodology. *Bharathidasan University.*

Republic of South Africa (RSA). (1996). *Constitution of the Republic of South Africa*.

Republic of South Africa (RSA). (2005). *Occupation Health and Safety Act*, Schedule of Electrical machinery regulations.

Republic of South Africa (RSA). (2009). *Occupational Health and Safety Act*, Electrical Installation Regulations.

Republic of South Africa (RSA). (2012). *ICT Policy Colloquium Discussion Document*. Government Gazette No 35255.

Republic of South Africa (RSA). (2013). *Protection of Personal Information Act* No 4 of 2013.

Republic of South Africa (RSA). (2015). *Guidance Notes to the Pressure Equipment Regulations.* Government Gazette No 38505

Richards, N. M. (2005). Reconciling Data Privacy and the First Amendment. *UCLA Law Review, Vol. 52*, p. 1149.

Robinson, E. (2003). *Case Study in Implementing Security for HIPAA Privacy Compliance*. Retrieved from https://www.sans.org

Roe, C. (2017, June 22). *What is data governance?* Retrieved from http://www.dataversity.net

Roebuck, K. (2011). Identity Management: High-Impact Strategies - What You Need to Know. *Lightning Source.*

Roos, A. (2007). Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position. *South African Law Journal, Volume 124, Issue 2,* Pages 400-437.

SAFLII. (2007). Grütter v Lombard and Another (628/05) [2007] ZASCA 2; [2007] 3 All SA 311 (SCA) (20 February 2007).

SAICA. (n.d. a). What is corporate governance? Retrieved from https://www.saica.co.za/TechnicalInformation/LegalandGovernance/CorporateGovernance/tabid/867/language/en-ZA/Default.aspx

SAICA. (n.d. b). *Consumer Protection Act, No 68 of 2008.* Retrieved from https://www.saica.co.za/Technical/LegalandGovernance/Legislation/ConsumerProtectionActNo68of2008/tabid/1911/language/en-ZA/Default.aspx

Samarajiva, R. (2001). Telecom Regulation in the Information Age. In W.H.Melody (Ed.), *Telecom Reform Principles, Policies and Regulatory Practices* (pp. 415-432).

Schleiter, K. E. (2009). When Patient-Physician Confidentiality Conflicts with the Law. *US National Library of Medicine National Institutes of Health.* Retrieved from https://www.ncbi.nlm.nih.gov

Schmidt, S. (2016). Asia's Regulatory Awakening Reaches New Milestone. Demyst Data.

Schneider, A. (2008). The roles of internal audit in complying with the Sarbanes-Oxley Act. *Int J Discl Gov, 6*(1), 69-79.

Schutt, R.K. (2004). Qualitative Data Analysis. *Sage Publications.*

Shaffer, G. (2000). Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of US Data Privacy Standards. *Yale Journal of International Law, Volume 25.*

Shah, S. (2016, May 14). *The History of Social Networking.* Retrieved from https://www.digitaltrends.com

Sivaranjani, G., & Suganthi, G. V. (2014). A Novel Method for Privacy Preserving Data Publishing. *International Journal of Advanced Research in Computer Science & Technology Volume 2.*

Smith, M. (2015, December 16). *Letter: Road rules increase safety.* Retrieved from http://www.richmond-news.com

Smith, M. R. (1973). The Return of Papyrus. *Aramco Volume 24, Number 4.*

Solove, D.J. (2006). A Brief History of Information Privacy Law. *Proskauer on privacy, PLI*

South Africa Law Reform Commission [SALRC]. (2005). *Privacy and Data Protection Discussion Paper 109*. Retrieved from http://www.justice.gov.za/salrc/dpapers/dp109.pdf

SALRC. (2009). *Data and Privacy Report.* Retrieved from http://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf

Southekal, P.H. (2017). Data for business performance. *Technics Publications.* Page 199.

Srivastava, A., & Thomson, S.B. (2009). Framework analysis: A qualitative methodology for applied policy research. *Journal of Administration and Governance* 72

Stallings, W. (n.d.). *Standards for Information Security Management*. Retrieved https://www.cisco.com

Standler, R. B. (1997). *Privacy Law in the USA*. Retrieved from http://www.rbs2.com/

Stengg, W., Fitzpatrick, T., Pillar, S., & Pocztowska, J. (2008). *DG Markt Guide to Evaluating Legislation*. European Commission [EUC].

Surrey University. (n.d.). *Module 9: Introduction to Research, Analysing Qualitative Research Data*. Retrieved from http://libweb.surrey.ac.uk/library/skills/Introduction%20to%20Research%20and%20Managing%20Information%20Leicester/page_75.htm

Tabibi, Z., Grayeli, F., & Abdekhodaei, M. S. (2016). Self-reported compliance with traffic rules in a sample of Iranian pre-schoolers: Knowledge of rules, perception of danger, moral judgment, and self-regulation. *Swiss Journal of Psychology*, *75*(1), 25-33.

Taylor, D. (n.d.). *The Literature Review: A few tips on conducting it*. University of Toronto, Canada. Retrieved from http://advice.writing.utoronto.ca

Taylor, F.W. 1947. *Principles of Scientific Management.* New York, NY: Harper

The Physics Classroom. (n.d.). *Newton's Laws - Lesson 1 - Newton's First Law of Motion: Inertia and Mass.* Retrieved from http://www.physicsclassroom.com/class/newtlaws/Lesson-1/Inertia-and-Mass

Trochim, W.M.K. (2006, October 20). *Research Methods Knowledge Base.* Retrieved from https://www.socialresearchmethods.net/kb/reliablt.php

United Nations. (2015). *Universal Declaration of Human Rights.* Retrieved from http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

United States Department of Justice. (n.d.). *Privacy Act of 1974*. Retrieved from https://www.justice.gov/opcl/privacy-act-1974

Valenzuela, D., & Shrivastava, P. (2002). *Interview as a Method for Qualitative Research*. Presentation. Arizona State University. Retrieved from http://www.public.asu.edu

van den Hoven, J., Blaauw, M., Pieters, W., Warnier, M. (2014). Privacy and Information Technology. *Stanford Encyclopaedia of Philosophy.*

Wadhwa, V. (2014). Laws and Ethics Can't Keep Pace with Technology. *MIT Technology Review.*

Wakefield, A. (2015, August 28). *Case of super-spy machine sensitive – Hawks.* News24 Retrieved from https://www.news24.com

Walker, D., Ramashia, M. & Rambau, F. (2013). *Chapter 22: South Africa* in The corporate governance review. W.J.L.Calkoen (Ed.), 304-314.

Warren, S. D., & Brandeis, L, D. (1890). The right to privacy. *Harvard Law Review, vol. 4, no. 5.*

Waters, J. (2011, July 25). Could you pass a Facebook background check? Market Watch, Retrieved from https://www.marketwatch.com

Weiner, J. (2007). *Measurement: Reliability and Validity Measures*. John Hopkins University. Retrieved from http://ocw.jhsph.edu

Westin, A. (1967). *Privacy and Freedom.* Washington and Lee Law Review Volume 25 Issue 1

Wicks, J., & Areff, A. (2016, June 10). *Penny Sparrow ordered to pay R150k*. News24. Retrieved from https://www.news24.com

Yin, R. K. (2003). *Case Study Research Design and Methods*. London: Sage Publications.

## APPENDIX 1: INTERVIEW PROTOCOL


**Masters research: Information sheet, semi-structured interview guide and informed consent form**

**Title of research: Understanding the Impact of Implementing the Protection of Personal Information Act**

**Name of student: Amiel M Joshua, Student No. 406165, Mobile: 083 714 0978**

**Supervisor: Dr Kiru Pillay, LINK Centre, University of the Witwatersrand**

**Request:** You are invited to participate in this study by responding to a limited number of questions for the purposes of research for the MA in the field of ICT Policy and Regulation. The interviewer would like to conduct a one-on-one interview, which should take a maximum of one hour. Please read the following outline in order to consider your participation. An informed consent form is attached for your signature.

**Overview of the study:**

Data privacy has become a key concern in the information age. The Internet has made possible the capture and transmission of vast amounts of personal information across the globe in seconds. In the United States of America and parts of Europe various legislative regimes exist relating to privacy. South Africa has only recently begun to formally safeguard the right to online privacy of its citizens, despite privacy having become a constitutional right with the advent of democracy. Implementing these safeguards will potentially radically affect the process of collecting, storing, transmitting and accessing information collected from individuals. This study aims to assess three aspects regarding the impact of compliance with regulations designed to safeguard citizens of South Africa's privacy; the impact of the Act on: specific industry sectors and organisations; the transfer of data between countries; and the impact on data professionals in ensuring compliance.

**Deciding to participate:** Participation is entirely voluntary. You are free to withdraw at any stage without giving a reason. There are no risks to participation. The study may have several beneficial outcomes, as the topic is of interest to persons and institutions active in the ICT policy and regulation environment. A few quotations from selected interviews may be included in the final report, with the respondents details anonymised. The examined report will be published in the Wits open access repository WIReDSpace.

**Anonymity and confidentiality:** Any limited personal information collected about you will be kept confidential. Names will not be listed in the published report, unless specifically agreed to. The anonymised data generated in the course of the research will be kept securely in paper or electronic format.

**Designation and institutional component of Key Informant:**

**Date and Time of Interview:**

**Research Questions**

The study posed 2 main research questions. The first was addressed by means of analysis of legislation in other jurisdictions. This involved a combination of desk analysis and interviews.

The second research question was answered in terms of assessing readiness for compliance with respect to: (a) data privacy, (b) minimum security measures and (c) other principles of data management as laid out in the Act:

**Research Question 1:** To what extent do the provisions of the Act compare with its original intention, and also with accepted international norms?

- What, in your opinion, were the original intentions of the Act?
- What deficiencies in legislation at the time of the Act being promulgated was the Act meant to address?
- To what extent do you believe the Act succeeds in addressing these deficiencies?
- Mention specific sections of the Act and what they were intended to address.

*Sub Question 1:* How do the provisions of the Act compare to similar legislation in other jurisdictions?

- What other jurisdictional legislation was reviewed?
- Why these jurisdictions in particular?
- What was learned from these legislations?
- What specific sections were copied or used as a basis for the legislation under discussion?
- Are there any unique sections that the POPI? - i.e. not included in other legislations?
- If so, why? What specific circumstances in SA led to this/these component(s)?

*Sub Question 2:* What changes are anticipated by the promulgation of the Act in terms of how personal information is collected, stored and used?

- What specific operational changes do you foresee for organisations and individuals as a consequence of the Act?
- What such changes do you foresee specifically with respect to the collection, storage and use of personal information?
- How has personal information been collected, stored and used previously?
- What deficiencies have existed?
- How are these deficiencies addressed in the new legislation?
- How onerous do you believe the new Act will be in respect of collection, storage and usage of personal information?
- Are there aspects relating to collection, storage and usage that are not addressed by the Act?

*Sub Question 3:* To what extent will trans-border data flow be enhanced or impeded by the implementation of the Act?

- Do you consider there to be deficiencies in the Act?
- How does the Act affect trans-border flows?
- What particular aspects of trans-border flows was the Act meant to address?
- Do you believe that the Act addresses these adequately?

**Research Question 2:** What are the implications of the Act with respect to specific organisations and persons?

- Are any sectors affected more than others?
- Why is this so?
- Do these sectors use personal data more than other sectors?
- Are specific roles going to be impacted by implementing the Act?
- What is required of persons implementing the Act?

*Sub Question 1:* What internal and external changes does compliance with the Act force on companies that gather personal information?

- What aspects of the Act necessitate these changes?
- What current practices stand to be altered in order to comply with the Act?
- Do these include key business areas of the organisation?

*Sub Question 2:* What effect does the Act have on the processes of organisations that gather and store personal data and on the daily tasks of technology professionals?

- What processes are expected to be altered by implementation of the Act?
- What provisions of the Act require these changes?
- Is the organisation able to function without the processes should they not be able to comply with the Act?
- Why is this the case?
- Are external professionals required to comply with the changes that need be implemented in the organisation for compliance with the Act?

**Is there anything else you would like to share regarding the subject?**

**Would you be willing to respond to a short email follow up, if required?**

**Ends.**

**Masters research: INFORMED CONSENT FORM**

**Title: Understanding the Impact of Implementing the protection of Personal Information Act (POPI)**

**Please initial box**

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions. ☐

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason. ☐

3. I understand that the Researcher will not identify me by name in any reports using information obtained from this interview and that the views I express will remain confidential; **OR** ☐

4. I agree to my name being listed as a participant in this study in the annexure to the report, but not to be referenced in the main body of the report. ☐

   I agree to the interview being audio recorded. ☐

5. I agree to the use of anonymised quotes in the dissertation. ☐

6. I agree that data gathered from me in this study may be stored (after it has been anonymised) and may be used for future research. ☐

---

Name of Research ParticipantDate Signature

---

Name of Researcher Date Signature

## APPENDIX 2: DATA ANALYSIS SPREADSHEET