




Enforcement of the *Protection of Personal Information (POPI) Act*: Perspective of data management professionals

**Authors:**Agbor T. Kandeh¹ Reinhardt A. Botha¹ Lynn A. Futcher¹ **Affiliations:**

¹Centre for Research in Information and Cyber Security, Department of Information Technology, Nelson Mandela University, South Africa

Corresponding author:

Agbor Kandeh,
agborcom@gmail.com

Dates:

Received: 14 Sept. 2017

Accepted: 23 May 2018

Published: 09 Oct. 2018

How to cite this article:

Kandeh, A.T., Botha, R.A. & Futcher, L.A., 2018, 'Enforcement of the *Protection of Personal Information (POPI) Act*: Perspective of data management professionals', *South African Journal of Information Management* 20(1), a917. <https://doi.org/10.4102/sajim.v20i1.917>

Copyright:

© 2018. The Authors.
Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Read online:

Scan this QR code with your smart phone or mobile device to read online.

Background: The urgency to enforce the *Protection of Personal Information (POPI) Act* is building up within South Africa, triggered by the appointment of the Information Regulator for POPI on 01 December 2016. However, for data management practitioners, the absence of a practical guideline on how to legally process personal information of employees, customers or other juristic persons in line with the *POPI Act* poses a day-to-day technical challenge, especially for those embarking on a maiden journey to comply with the *POPI Act*.

Objectives: The objective of this article is to explore and analyse the unique perspectives of data management professionals who are vested with the responsibility of driving the successful enforcement of the *POPI Act* within their respective organisations, with the end goal of formulating a practical guideline for the enforcement of the *POPI Act*.

Method: To achieve the objectives of this research article, semi-structured interviews were conducted with a purposive, convenience sample of 16 data management professionals within companies in South Africa. A recording of their views was obtained through one-on-one interviews and a group interview.

Results: From the semi-structured interviews, group interview and response to the questions, several findings and learnings were elicited. Zooming into these findings showed close similarities in the actions taken by data management professionals operating in a similar industry. Based on these results, a high-level sequence of steps on how to enforce the *POPI Act* was formulated.

Conclusion: Based on the formulated sequence of steps, it is safe to conclude that the actions of data management professionals can be used to create a practical guideline to enforce the *POPI Act*. However, to standardise these guidelines across the data management function, there is a need to perform testing with a wider spectrum of data management professionals.

Introduction

The need to comply with the *Protection of Personal Information (POPI) Act* is gaining momentum in South Africa, following the appointment of the information regulator by the President of South Africa on 01 December 2016 (SAICA 2017). Unlike similar legislations such as the *Financial Intelligence Centre (FIC) Amendment Act* No. 1 of 2017 which is finance and payments industry specific, the *POPI Act* cuts across all industry types (public and private), and it is constantly being disrupted by the adoption of new technologies, which changes how personal information is stored, processed and transmitted. The concepts of *Privacy* and *Technology* are closely related and their impact on each other has been an ongoing research subject for many years now. This relationship goes as far back as 1890 when Warren and Brandeis (1890) articulated their disagreement on the Harvard Law Review regarding the intrusiveness of journalism and the need to protect privacy, triggered by the growth of newspaper publications and photography. According to Van den Hoven et al. (2014), the information privacy debate has evolved with the introduction of new information technologies over the years. In this debate, though information technology is often seen as the cause of information privacy problems, conversely, information technology is also presented as the solution to information privacy problems. Recent information technology trends and developments such as the Internet of Things (IoT), social media, big data, mobile devices, Geo-location and e-government have further raised the urgency for information privacy protection to be enforced and the effect on data management professionals to be examined. Table 1 is adapted from Westin (2003) showing the evolution of information privacy with the advent of new information technology trends.

TABLE 1: Evolution of the Information Privacy Concept following the evolution of information technology.

Period	Characteristics
Privacy Baseline, 1945–1960.	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection, processing and storing.
First Era of Contemporary Privacy Development, 1961–1979.	Rise of information privacy as an explicit social, political and legal issue. Early recognition of potential dark sides of the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIP) Framework and establishing government regulatory mechanisms established such as the <i>Privacy Act</i> of 1974.
Second Era of Privacy Development, 1980–1989.	Rise of computer and network systems, database capabilities and federal legislation designed to channel the new technologies into FIP, including the <i>Privacy Protection Act</i> of 1984. European nations move to national data protection laws for both the private and public sectors.
Third Era of Privacy Development, 1990–present.	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.
Fourth Era of Information Privacy Compliance Laws, for example, The <i>POPI Act</i> .	Internet of Things (IoT), Bring Your Own Device (BYOD), big data, cloud computing, social media, e-government, etc.

Source: Adapted from Westin, F., 2003, 'Social and political dimensions of privacy', *Journal of Social Issues* 59(2), 431–453. <https://doi.org/10.1111/1540-4560.00072>

POPI, protection of personal information.

Based on Table 1, we are in the fourth era whereby privacy laws are dictating how personal identifiable information is handled. This fourth era is unique as it presents challenges that are very different from those mentioned in the initial privacy baseline era. For example, in the privacy baseline era, there was limited technology to collect, process and store personal identifiable information. Progressing from the baseline era through the first, second, third and fourth privacy eras, there has been a significant advancement in information technology which has created privacy concerns both for the subjects whose personal information is being processed, as well as for the entity responsible to hold the personal information. To address these concerns and to protect its citizens now in the fourth era, Governments have passed laws regulating privacy such as the *POPI Act*. According to Solove (2006), hundreds of laws pertaining to privacy exist, mostly originating from the common law, torts, criminal law, evidentiary privileges and constitutional law. To understand the laws of information privacy, it is necessary to look at its origins and growth (Solove 2006). Greenleaf (2012), in his paper entitled 'Global Data Privacy Laws: 89 Countries, and Accelerating', confirms that over 89 countries and independent territories have now adopted comprehensive data protection laws including nearly every country in Europe, and many in Latin America, the Caribbean, Asia and Africa. Five years on, this number would have grown significantly based on the assumption that more countries are adopting some form of information privacy law to protect the information of their citizens. In the context of South Africa, the Constitution of 1996, Chapter 2 (Bill of Rights) Section 14, subsections a, b, c and d allude to the importance of the privacy of the citizens in a very broad manner, with a focus on the privacy around communications, property, home searches and possessions. The provisions of these subsections do not prescribe any means of enforcing information privacy protection. However, it makes provision for subsequent legislations on the protection of privacy. Further to this, the

Electronic Communications and Transactions Act, of 2002, popularly known as the *ECT Act*, highlights the need to protect privacy in the context of consumer rights, as well as in the context of security, when transacting electronically. Similarly, the *ECT Act* does not cover the POPI extensively. To date, information privacy is being protected by a combination of the common law and the *POPI Act* signed into law by the President of South Africa on 19 November 2013. According to Botha, Eloff and Grobler (2016), the *POPI Act* is something that organisations cannot ignore and the office of the newly appointed information regulator will be looking to make examples of organisations not complying. The next section introduces the data management professionals responsible for ensuring compliance with the *POPI Act*.

Data management professionals

A data management professional is defined as: 'any professional involved in the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets' (DAMA 2015). This definition is quite broad and encompasses a number of professions, which may not have direct contact with the lower-level aspects of data management. Hence, for the context of this study, a more focused definition of data resource management is provided by DAMA (2015), as 'the development and execution of architectures, policies, practices and procedures that properly manage the full data lifecycle needs of an enterprise'. Interpreting this definition from a technology perspective will include any information technology professional involved in the collection, storage, transmission and analysis of data, for example, data analysts, information technology (IT) security officers, IT compliance officers, IT risk officers, network engineers, IT auditors and software developers. Hence, the role of a data management professional is fully aligned with the POPI requirements mandated by the *POPI Act*. However, the majority of the available *POPI Act* literature is focused on the challenges faced by organisations as a whole to enforce the *POPI Act*. Conversely, the challenges faced by the individual DM professionals responsible for the enforcement of the *POPI Act* are not well documented. Hence the problem: *The absence of a practical and actionable guideline formulated by data management professionals to assist other data management professionals to simplify the implementation of the POPI Act within their respective organisations.* Following this problem is the question: *How can the observations of data management professionals on how personal information is stored, processed and transferred using computer systems, employees and processes be used to create a guideline for the implementation of the POPI Act?* This question is posed to address the problem of what practical observations can be extracted from the experience of data management professionals to create a guideline for the implementation of the *POPI Act*.

This article explores the unique perspectives of DM professionals who are responsible for implementing the provisions of the *POPI Act* within their organisations, focusing on gathering and analysing their views with the goal

of formulating practical guidelines for the implementation of the *POPI Act* within the South Africa context and construct.

Background

According to KPMG (2016):

The POPI Act, is a piece of legislation designed to protect any personal information which is processed by both private and public bodies (including government). Some exceptions exist, but every person who collects, stores, and otherwise modifies or uses information (i.e. processes information) is responsible under the POPI Act to comply with the conditions required for the lawful processing of personal information.

As a result, all organisations in South Africa are faced with the need to comply with the *POPI Act*. In the context of South Africa, the *POPI Act* is the applicable South African legislation and any company operating within South Africa is mandated to comply with this law. According to Workpool (2017), the purpose of the *POPI Act* is to ensure that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing and transmitting personal identifiable information by holding them accountable, should they abuse or compromise the personal information in any way. All organisations within South Africa are required to enforce the *POPI Act* in their day-to-day operations. This will require significant effort and change in the 'modus operandi' of their businesses. The history of the *POPI Act* dates back to 2011 when the *POPI Act* was tabled at the Parliament of South Africa. Thereafter, the *POPI Act* was signed into law by the President of South Africa. However, the commencement date is yet to be announced by the President of South Africa; companies will be given a year to achieve compliance with the *POPI Act* once the commencement date is announced. Penalties for failing to comply with the *POPI Act* includes prosecution, with a possible prison term of up to 12 months and a fine of up to 10 million Rands (R10 Million).

Protection of personal information enforcement

Before presenting the views gathered from the DM professionals interviewed in this study, this article will answer the question of: *What is POPI Act enforcement?* According to the *POPI Act* as gazetted in Government Gazette No. 37067 of 26 November 2013 (Department of Justice 2013), the *POPI Act* presents eight conditions under which personally identifiable information (PII) can be legally stored, processed and transferred, namely:

- **Accountability:** This condition mandates the responsible party to ensure that all conditions for the lawful processing of personal information are respected.
- **Processing limitation:** This speaks to the following guidelines: lawfulness of processing, minimality, consent, justification and objection, and collection directly from data subjects.
- **Further processing limitation:** this condition ensures that any further processing is compatible with the purpose of collection.

- **Purpose specification:** This condition addresses the collection for a specific purpose, retention and restriction of records.
- **Information quality:** This requirement speaks to the quality and reliability of the information.
- **Openness:** This condition caters for the notification to the data subject when collecting personal information.
- **Security safeguards:** This requirement targets security measures to ensure the integrity and confidentiality of personal information.
- **Data subject participation:** This requirement guarantees the continuous access to personal information of the data subject.

Based on Mprem (2016), personal identifiable information includes information about a data subject's religious or philosophical beliefs; race or ethnic origin; trade union membership; political persuasion; health or sex life; and criminal behaviour or biometric information. This list is not exhaustive but provides a view into how broad and diverse the sources of personal identifiable information are. In line with the eight conditions listed above, the POPI information regulator can grant exemptions under certain conditions like when the information being processed is for the national security interest of South Africa. Further to this, the *POPI Act* also identifies some key stakeholders. Table 2 summarises the key stakeholders and their roles as defined by the *POPI Act* in the Government Gazette.

In essence, to enforce the *POPI Act*, businesses will have to read and understand the provisions stipulated in the *POPI Act*; translate these provisions into the context of their business; and start taking measures and instituting controls around their processes, employees and technology. Over and above the possible fine to be levied on the *POPI Act* defaulters, or a possible prison sentence which can be given to offenders, the POPI regulator is also empowered, after investigation, to issue an 'enforcement notice' requesting the defaulter to stop processing personal identifiable information. The scope of the order can vary from one individual's information to all personal information processed by the organisation. It can be restricted to a department, division, or cover an entire business and conceivably even a group. Naturally, such an order has the potential to disrupt and even to precipitate the closure of a business (Ernst & Young 2013). Another important power vested on the POPI regulator is to initiate a civil action on behalf of an individual or group of individuals whose information has been mishandled. In view of all these threats,

TABLE 2: Key Protection of Personal Information Act stakeholders and roles.

Key actors	Definition of role
1. Data subject	The person(s) to whom personal information relates.
2. Responsible party	A private or public body or any other person, which alone, or in conjunction with others, determines the purpose of and means for processing personal information.
3. Operator	An operator is 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.
4. Regulator	The body responsible to enforce compliance to the POPI regulations.

Source: 'Authors' own work

technical, governance and risk professionals within companies have no choice but to comply with provisions of the *POPI Act* within their organisations or face the consequences that may ensue from non-compliance to the Act.

Methodology

To achieve the objectives of this research article, semi-structured interviews were conducted with purposive, convenience sampling. For purposive sampling reasons, DM professionals were consulted for this study. And for convenience sampling reasons, the researcher's existing relationship and network of professional colleagues were interviewed. The context of this research approach was inspired by the position taken by industry professionals and supported by statements such as that of Matthes (2014:1), stating that:

... the information technology focus of the *POPI Act* should be on the knowledge of how logical and physical access is maintained and managed for the systems and areas housing personal information.

This resulted in questions like: Should organisations intensify physical security around personal information to prevent the information from getting into the wrong hands? Should organisations streamline processes and systems to identify the following?

- Where is the personal identifiable information stored?
- How is the personal identifiable information processed electronically?
- Who is allowed to access the personal identifiable information?
- For what purpose is the information to be stored, processed or transmitted?

To conduct the semi-structured interviews, the sample for this study comprises 16 DM professionals, from a network of 35 DM professionals structured along their job titles as presented in Table 3. Table 3 also provides a brief description of their roles in the context of the *POPI Act*.

A recording of the views and opinions of all 16 research participants was obtained through one-on-one interviews,

while a group interview was conducted with 5 IT security professionals from the 16 participants taking part in this study. The audio recordings of these interviews were transcribed for further analysis using the relational content analysis methodology. According to Palmquist et al. (1997), relational content analysis seeks to go beyond the mere presence, by exploring the relationships between the concepts identified, and establishing a meaningful relationship. In so doing and in the context of this study, the opinions and remarks raised by this group of data management professionals was then compared against existing literature on the *POPI Act* using an automated and manual keyword search. The intention of comparison was to establish whether there are any relationships between the data emanating from these two sources of information (semi-structured interview of data management professionals and available literature on the *POPI Act*). The next section presents the views of the DM professionals, sampled through the semi-structured interview, and a focus group with five data management professionals responsible for information security.

The 'Conceptual framework' and 'Summary of the interview questions' sections cover the semi-structured interview questions to be used for this study and present the outcome of the interviews conducted with the 16 DM professionals sampled in this study.

Conceptual framework

According to Jabareen (2009), a conceptual framework is defined as a network or a 'plane' of linked concepts. This definition sets the tone for leveraging on a conceptual framework as a mechanism to analyse related concepts. In terms of this study, the following three related concepts will be evaluated in line with the research problem, research questions and research objectives as defined in the section on 'Data management professionals'

- Problem context: This focuses on the key problem to be addressed in this study, which is to formulate a guideline to assist DM professionals to enforce the *POPI Act*.
- The privacy context: Herewith, the privacy rules on how personal identifiable information is stored, processed and transmitted using information systems and other technologies is covered.

TABLE 3: Job titles and description of job roles.

Job title	Description	Description role in the context of <i>POPI Act</i>	Participants
Data analyst	Collects, processes and performs statistical analysis on datasets	Collects data, processes and performs statistical analysis on datasets	2
IT security professional	Plans and implements security measures to protect data	Implements and monitors data protection controls as required by the <i>POPI Act</i>	5
IT compliance officer	Ensures that IT operates within the regulatory frameworks	Evaluates and monitors compliance with the <i>POPI Act</i> and other regulatory frameworks. (Access to all personal data and controls)	2
IT risk officer	Accesses the IT risk exposures to ensure they are in line with the company's risk appetite	Conducts a full risk assessment on compliance to the <i>POPI Act</i> (access to all personal data and controls)	2
Network engineer	Designs, implements and supports data networks	Accesses data in transit across the network links	1
IT auditor	Reviews information systems controls for compliance with policies, procedures and best practices	Access to stored data, configuration data, system data and data processing controls	2
Software developer	Builds computer systems and applications based on a set of requirements	Designs database to store personal data. Accesses personal data, processes personal data and transfers personal data	3

Source: Adapted from Doyle, A., 2017, 'List of Information Technology (IT) job titles', The Balance, viewed 01 March 2017, from <https://www.thebalance.com/list-of-information-technology-it-job-titles-2061498>

POPI, protection of personal information; IT, information technology.

- **Research sample:** The research sample involves the list of information technology professionals responsible to enforce compliance with the *POPI Act* in their respective organisations.

These three concepts are linked in the following ways:

- Problem context is linked by 'rules on processing personal information' to the 'Privacy Context'.
- Privacy context is linked by 'implement rules defined by *POPI*' to the 'Research Sample'.
- Research sample is linked by 'step to enforce *POPI*' to the 'Problem Context'.

Figure 1 illustrates the different contexts in scope for this study and their relationships.

Based on the conceptual framework, this study will explore the claim that the practical observations of a purposive and/or convenient sample of DM professionals can be standardised to formulate a high-level sequence of steps (guidelines) to assist other DM professionals to enforce the *POPI Act* in their company.

The next section deals with the semi-structured interview question to be used for this study.

Summary of the interview questions

The participants of this study responded to the list of three questions. The questions were structured to target the various aspects of the *POPI Act*:

- **Question 1:** deals with the awareness of the *POPI Act* and its significance to the job profile of the participants. The question reads: *What is your understanding of the POPI Act and how does it affect your scope of work?*
- **Question 2:** focuses on the individual activities undertaken by the participants to enforce the *POPI Act*. The question reads: *Describe some of the measures you have taken in your current role to comply with the POPI Act.*

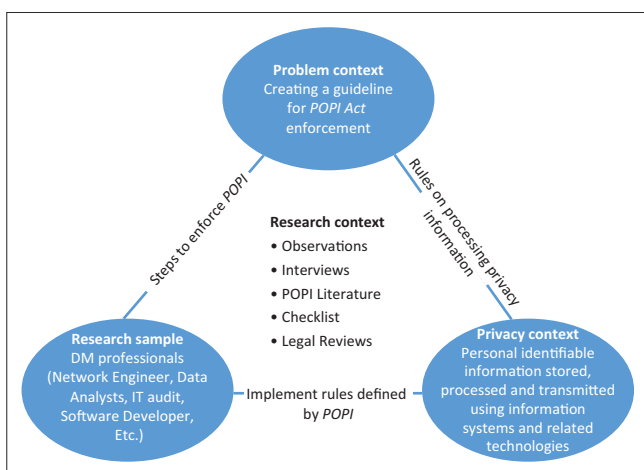


FIGURE 1: Conceptual framework.

- **Question 3:** targets the consequence and implication of non-compliance with the *POPI Act* by the participants. The question reads: *To what extent will the failure to comply with the POPI Act affect your performance ratings in your current role?*

Findings and comments

Awareness of the *Protection of Personal Information Act*

Responding to the question regarding the awareness of the *POPI Act*, 14 of the 16 research participants acknowledged their awareness of the *POPI Act* and its stringent compliance requirements. Two of the participants who specialise in 'software development' were not aware of the *POPI Act*. Further to this, while conducting the group interview with the five IT security professionals, it was revealed that there is a significant overlap between the *POPI Act* and the ISO 27001 information security standard and best practice. The IT security professionals stressed that implementing ISO 27001 will raise awareness about many baseline security controls required by the *POPI Act*. In addition, the IT security professionals also raised the following comments regarding the awareness of the compliance requirements of the *POPI Act* as urgent advice to other data management professionals:

- Data classification with respect to unstructured data such as images of documents, photos, videos and paper records should be stored in a designated secure area to ensure end-to-end *POPI Act* compliance.
- Considering that the current scope of vulnerability and penetration testing does not cover privacy-specific data sets and controls, it is necessary that the scope of vulnerability management and penetration testing be expanded to accommodate privacy-specific data sets and controls in line with the provisions of the *POPI Act*.
- The disposal and recycling of IT assets should be freed of any personal information that can compromise the data subject.

No customer consent form and data enrichment

Responding to Question 2 regarding the measures being taken by data management professionals to comply with the *POPI Act*, the data analysts interviewed in this study confirmed that it is not common to find a data request accompanied by a consent form from the data subject, be it an internal employee or an external customer. One of the data analysts stated that, *normally the business operator just log a form stating the data type and the fields of data he or she wants from the organisational database*. Further to this, the requirement to enrich data was also highlighted. According to the data analysts, for enrichment, data belonging to a data subject is cleaned and modified without the involvement or consent of the data subject and it is a common practice within the organisations for which the two data analysts interviewed, have worked in the past. In terms of Question 3 regarding the consequence of non-compliance with *POPI*, one of the data analysts confirmed the fact that the policy guiding data management solutions within

their organisation is still being developed and the support of an expert in information privacy is required to guide analysis performed on personal identifiable information. Finally, from a system perspective, it was also revealed by participants that the call logging system used to manage the request and distribution of data within the organisation has no privacy control inbuilt.

Similarity of the Protection of Personal Information Act and ISO 27001

As per the discussion with the focus group of data management professionals responsible for information security, responding to Question 2, four out of the five participants were of the opinion that by implementing ISO 27001, businesses will ensure that they have effective control in place to manage risk and protect personal information. One of the participants argued that POPI goes beyond security controls and governance measures. In addition, the security professionals interviewed pointed out that *on top of the security controls to be implemented, organisations should be more responsible and enforce ethical practices in their business operating models. This view is in line with Van den Hoven (2008), who stressed that information technology creates ethical privacy issues.* When pressed further, a common practice in insurance companies was cited, whereby information collected for one purpose is used by the subsidiaries of these companies to offer similar or sometimes completely different products or services. Responding to this insight, one of the participants suggested that data leak protection (DLP) technologies should be employed by organisations to manage their employees' end user devices and portable equipment, namely, laptops, tablets and cell phones, and so on.

Responding to Question 3, four of the five participants confirmed that organisation-specific policies on information privacy and data classification are still being developed within their respective organisations, and therefore they are not enforceable.

The Protection of Personal Information Act and organisational culture

Responding to Question 2, there was a consensus from the two IT compliance officers interviewed that enforcing the *POPI Act* goes far beyond just putting systems and control measures in place; it requires a fundamental change in how organisations and their employees conduct business. One of the respondents further specified that inherently organisations will have to change their culture on how they consume and transmit personally identifiable data. The participant stated that organisations will have to undergo major changes both in their business policies, processes and structure. These changes might be costly and disruptive for its employees and shareholders. In the words of one of the IT compliance respondents, 'the biggest challenge to enforce the *POPI Act* is the cost of building the compliance landscape'. When this respondent was further probed, his opinion was that the impact of non-compliance to the *POPI Act* is the same for big or small enterprises both in the public and private sectors.

With regard to Question 3, one of the participants mentioned that there is a general *lacklustre attitude towards the POPI Act*. When pressed further regarding the attitude towards the *POPI Act*, the respondent confirmed that the complacency is top down. Meaning that top management seems not to take the *POPI Act* enforcement seriously and this attitude has cascaded down to their subordinates and other junior staff. In addition, one of the participants mentioned that the fact that the commencement date has not yet been communicated by the President is not helping in 'accelerating' the compliance efforts. Analysing this further with the compliance officers, to an extent, the slow progress in enforcing the *POPI Act* can also be attributed to the fact that organisation-specific processes and procedures are missing. More so, the efforts directed at individuals responsible to safeguard data should be reviewed so as to cater for the vast scope and multiple locations of personal information facilitated by Internet technologies. To support this view, according to Mprem (2016), the biggest challenge in the implementation of the *POPI Act* is in the scope of the definition of the phrase 'processing of personal information'.

Change in the information technology compliance landscape

In the interview with the information technology risk officers, responding to Question 2, one of the IT risk participants raised the concern that from the assessment done by a consulting firm contracted to their organisation, the task to enforce POPI is scattered across different technical teams and that makes it difficult to hold any specific team accountable. Furthermore, the consulting firm also suggested change in the existing IT risk framework to cover the risk associated with the *POPI Act*. From this recommendation, the participant mentioned that most of the activities undertaken by the IT risk team have been around reviewing the risk framework and getting the supporting IT teams to incorporate risk, related to *POPI Act*, in their risk registers and putting controls in place to mitigate these risks. Beside this, with the broadening compliance scope caused by the *POPI Act*, the one-year legislated compliance period might not be sufficient. Finally, in response to Question 3, both IT risk participants stated that until the organisation approves the revised IT risk framework and confirms the risk appetite, the threat of non-compliance with the *POPI Act* would stay a high risk.

The Protection of Personal Information Act and span of technical control

In the engagement with the network engineer, it was revealed in his response to Question 2 that the span of control to enforce the *POPI Act* is very broad and complex. For instance, the reason given being that:

... most of the wide area network (WAN) links are sitting with the major service providers (Telkom, MTN, BCX, Neotel, and Vodacom). And the contracts with these major carriers do not cover specifically personal information as mandated by the *POPI Act*.

In addition, the network engineer revealed that links connecting financial institutions and government links carrying sensitive

data are difficult to compromise as regulations, such as the Payment Card Industry–Data Security Standard (PCI-DSS) mandates some key techniques to make the data in transit difficult to be compromised or to read when compromised. Some of the techniques mentioned by the participant and used by his WAN service provider are encryption, hashing and the establishment of virtual private networks (VPN). Furthermore, the network engineer confirmed that it is easy to protect data flowing through a proprietary network as opposed to an open network such as the Internet. To substantiate this point, the participant stated that in proprietary networks such as the government network, managed by the state information technology agency (SITA), the attack surface is small and rudimentary, so that security technologies such as encryption, compression, segregation and authentication are adequate to secure personal information. In response to Question 3, the network engineer stated that compliance with the *POPI Act* is not part of his key performance area (KPA).

Compliance with the *Protection of Personal Information Act* mandates a new information technology audit universe

The two IT audit professionals interviewed, in response to Question 2, were not sure of the scope of the audit universe to be audited to ensure compliance with the *POPI Act*. One of the participants mentioned the following environment to be in scope (systems, databases, networks, personal computers, servers, mobile devices) but conceded that this is not an exhaustive scope and will vary from one business unit to the other. Another challenge raised by one of the audit professionals is the complexity and diverse nature of the company policy and procedures to handle personal information. He states that *the policies and procedures to handle the different types of personal information is not clear, and silent on some areas like third party handling of company data*. Hence, he finds it very difficult to perform comprehensive audits according to the *POPI*. Finally, in responding to Question 3, the participants both confirmed that the absence of data classification and information sensitivity awareness in their organisation creates a high risk of non-compliance with the *POPI Act*.

Enforcing the *Protection of Personal Information Act* requires customisation of commercial off-the-shelf software

In the interview with the three software developers, two out of the three developers were of the opinion that the *POPI Act* is a governance issue, which does not concern them. However, one of the participants admitted that developers should be involved in enforcing compliance to the *POPI Act*, but raised the concern that translating the *POPI Act* into technical requirements to implement into systems will be a very difficult exercise, especially for systems that are already in production environments. To justify this point, the software developer stated that:

... off-the-shelf systems mostly from international software houses such as Oracle, SAP, and Microsoft are not tailored built with *POPI* in mind. Hence, it will require some level of customisation to be compliant.

Finally in terms of Question 3, the software developers all agreed that they developed systems and applications based on functional and non-functional requirements provided by the business owners; so if information privacy requirement is not explicitly specified as a formal requirement, then they cannot be held accountable. One of the developers conceded that in the development process they use test data which, if not handled properly, can compromise the data subject, for example, contact details (address and telephone), bank account numbers to mention a few. Commenting on this finding, it is noteworthy to highlight that for the software developers who are not aware of the *POPI Act*, like any other law, the *POPI Act* does not absolve offenders based on their ignorance. Therefore, the provisions of the *POPI Act* are binding whether you are aware of it or not.

Summary of findings and guideline for *Protection of Personal Information Act* enforcement

Table 4 summarises the findings and enumerates the key observations, which can be used as a possible guideline for the implementation of the *POPI Act*.

Based on Table 4, the following steps could constitute a guideline for the *POPI Act* implementation by data management professionals. However, the exact sequence to follow will necessitate a separate study:

- **Step 1:** *Raise awareness of the POPI Act with all the data management professionals.* This will ensure that all DM professionals know about the *POPI Act* and the risk of its non-compliance.
- **Step 2:** *Change the rules governing data requests and enrichment to comply with the POPI Act.* This step will ensure that all personal information extraction and manipulation is done in compliance with the *POPI Act*.
- **Step 3:** *Implement ISO 27001 baseline security controls.* This measure will establish the baseline information security controls required to protect personal information.
- **Step 4:** *Adopt a POPI Act compliance culture. It cannot be treated as a far-off thing.* This will change the attitude of all data management professionals towards the *POPI Act*. It will also emphasise the need for urgency to comply with the *POPI Act*.
- **Step 5:** *Align IT compliance and Risk policies, processes and procedures to the POPI Act.* This measure will change all the internal operating guides, gearing them up towards the *POPI Act* compliance.
- **Step 6:** *Take accountability even for personal data residing with external service providers.* This will ensure that all personal information owned by the organisation whether residing internally or externally is treated in a similar manner.
- **Step 7:** *Conduct POPI Act compliance assessment before procuring COTS software.* This measure will ensure that all IT system procurement is compliant with the requirements of the *POPI Act*.
- **Step 8:** *Build POPI Act compliance into the key performance areas (KPA) and key performance indicators (KPI) contracts of*

TABLE 4: Summary of findings and guidelines for *Protection of Personal Information Act* enforcement.

Question	Findings	Possible guideline for <i>POPI Act</i> implementation
What is your understanding of the <i>POPI Act</i> and how does it affect your scope of work?	<ul style="list-style-type: none"> • Fourteen out of the 16 participants are aware of the <i>POPI Act</i> and its stringent compliance requirements. • Two out of the 16 respondents were not aware of the <i>POPI Act</i>. 	<ul style="list-style-type: none"> • Generally, most of the DM professionals sampled in this study are aware of the <i>POPI Act</i>. However, for DM professionals who are not aware of the <i>POPI Act</i>, urgent awareness should be provided.
Describe some of the measures you have taken in your current role to comply with the <i>POPI Act</i> .	<ul style="list-style-type: none"> • Data request and enrichment are still being done without customer consent forms. • The implementation of ISO 27001 will help organisations to quickly comply with the <i>POPI Act</i>. • To ensure compliance, data management professionals need to adopt a <i>POPI Act</i> compliance culture within their organisations. • The <i>POPI Act</i> triggers a change in the IT compliance landscape and risk framework. • The <i>POPI Act</i> requires data management professionals to take more accountability for the span of technical controls. • Enforcing the <i>POPI Act</i> will require customisation of commercial off-the-shelf software. 	<ul style="list-style-type: none"> • The rules governing data requests and enrichment should be standardised to comply with the <i>POPI Act</i>. • Organisations should be encouraged to implement ISO 27001 as a major step towards the <i>POPI Act</i> compliance. • Data management professionals should adopt a <i>POPI Act</i> compliance culture. It cannot be treated as a far-off thing. • Data management professionals responsible for IT compliance and risk need to align policies, processes and procedures to the <i>POPI Act</i>. • Data management professionals are to take more accountability even for personal data residing with outsource partners or external service providers. • The <i>POPI Act</i> compliance assessment should be conducted before procuring COTS software.
To what extent will the failure to comply with the <i>POPI Act</i> affect your performance ratings in your current role?	<ul style="list-style-type: none"> • Compliance to the <i>POPI Act</i> is not a key KPA for technical professionals responsible for data management. • Policy and processes to enable the <i>POPI Act</i> compliance is still being developed. 	<ul style="list-style-type: none"> • <i>POPI Act</i> compliance should be built into the key performance areas (KPA) and key performance indicators (KPI) of all data management professionals. • Organisations should commit resources to develop internal policies required to enforce compliance to the <i>POPI Act</i>.

POPI, protection of personal information; DM, data management; COTS, commercial off-the-shelf.

all data management professionals. This step will make sure that all data management professionals prioritised *POPI Act* compliance in their day-to-day activities.

- **Step 9:** Finalise all requisite policies, processes and procedures to enable the *POPI Act* within the organisation. This measure will put in place all requisite governance practices to enable *POPI* compliance to be achieved within the organisation.

Conclusion

The insight provided by the data management professionals as recorded in the summary findings section of this study is diverse and presents many key observations for other DM professionals or organisations that are taking the initial steps towards complying with the *POPI Act*.

Firstly, although there is a general awareness of the *POPI Act* among the data management professionals sampled, the challenge and complexity to enforce the *POPI Act* seems to vary from organisation to organisation and largely depends on the type of personal information they use in their business operating model. However, some measures are being taken by most of the data management professionals sampled in this study to comply with the *POPI Act*. However, these measures might not be enough once the *POPI Act* comes into full force. In effect, the legislated duration of 1 year given to all organisations to comply with the *POPI Act* might not be sufficient. To support this assertion, PWC conducted a research in 2011 and over 35% of respondents were not sure how long it will take to implement the *POPI Act*, while another 35% of respondents said that it will take over 5 years and another 13% said it will take more than 1 year (PwC 2011). Hence, from these findings, it clear that 1 year is a very short timeframe to achieve full *POPI Act* compliance.

Secondly, from the perspective of the DM professionals gathered, and presented in Table 4, this study concludes that the compliance guidelines for data management professionals operating in a similar industry can be standardised to create a guideline for the implementation of the *POPI Act*.

To accomplish this, further technical analysis and testing will have to be conducted to fine-tune the implementation guidelines on a case-by-case basis.

Finally, the willingness to enforce the *POPI Act* will take some time to become engrained in the day-to-day activities of some of the DM professionals. For now, the need to comply with the provisions of the *POPI Act* is mostly seen as a far-off thing, especially for DM professionals working in companies that have not put in place internal measures such as policies to enforce the *POPI Act*. More so, the cost to build the *POPI Act* compliance capabilities was seen as a financial burden by the participants. To support this view, Kingwill (2016) of KPMG suggests a phased approach to *POPI* compliance which is based on a continual effort and each phase builds on the findings of the previous phases. This gradual approach will ease the operational burden placed on many organisations to comply with the *POPI Act*. In fact, most of the data management professionals sampled in this study concur with a phased approach. They are not keen on employing a full-scale enforcement of all the provisions of the *POPI Act* as this might disrupt their operations.

Acknowledgements

Agbor T. Kandeh would like to state that both Prof. Botha and Prof. Fatcher sponsored his Doctor of Philosophy (PhD) project with the Nelson Mandela University (NMU), with Prof. Botha being the lead supervisor.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors' contributions

R.A.B. played the role of a guide and mentor shaping my thinking and approach in conceptualising this article.

R.A.B. assisted A.T.K. in aligning the article with his PHD research project, focusing on 'Enabling information privacy and compliance by user configurable software objects'. In doing so, R.A.B. also helped in structuring the outline of the article and key areas of focus. L.A.F. assisted in a more technical role in reviewing the article, the semantics, language structure and flow and contributed in narrowing the research focus and in deciding on the research methodology and sample size.

References

- Botha, J., Eloff, M. & Grobler, M., 2016, *IFIP advances in information and communication technology*, vol. 474, pp. 72. Springer, Boston.
- Brenton, M., 1964, *The Privacy Invaders*, Coward McCann, New York.
- DAMA, 2015, *The DAMA guide to the data management body of knowledge*, viewed 27 February 2017, from <https://dama.org/sites/default/files/download/DAMA-DMBOK2-Framework-V2-20140317-FINAL.pdf>
- Doyle, A., 2017, 'List of Information Technology (IT) job titles', *The Balance*, viewed 01 March 2017, from <https://www.thebalance.com/list-of-information-technology-it-job-titles-2061498>
- Electronic Communications and Transactions Act. 2002 c7*, viewed 27 February 2017, from <http://www.gov.za/sites/www.gov.za/files/a25-02.pdf>
- Ernst & Young, 2013, *What happens if we violate PoPI?*, Ernst & Young, viewed 10 March 2017, from [http://www.ey.com/Publication/vwLUAssets/What_happens_if_we_violate_PoPI/\\$FILE/130522%20Privacy%20Thought%20Leadership%20.pdf](http://www.ey.com/Publication/vwLUAssets/What_happens_if_we_violate_PoPI/$FILE/130522%20Privacy%20Thought%20Leadership%20.pdf)
- Government Printing Works, 2002, *Electronic Communications and Transactions Act*, No. 25 of 2002, Pretoria.
- Government Printing Works, 2013, *Protection of Personal Information Act*, No. 4 of 2013, Pretoria.
- Greenleaf, G., 2012, *Global Data Privacy Laws: 89 Countries, and accelerating*, Social Science Electronic Publishing, Inc. Sydney Australia.
- Jabareen, Y., 2009, *Building a conceptual framework: Philosophy, definitions, and procedure*, Sage Journals, viewed 10 March 2017, from <http://journals.sagepub.com/doi/pdf/10.1177/160940690900800406>
- Kingwill, N., 2016, *Practical steps to becoming POPI compliant*, KPMG, viewed 02 March 2017, from <https://home.kpmg.com/za/en/home/insights/2016/05/practical-steps-to-becoming-popi-compliant.html>
- KPMG, 2016, *What is the Protection of Personal Information Act (POPI) and how we can help your business with compliance*, viewed 06 February 2017, from <https://home.kpmg.com/za/en/home/insights/2016/05/what-is-popi-.html>
- Matthes, C., 2014, 'Unpacking the POPI Act: The ins and outs of protecting personal information', *ITWeb Technology News*, viewed 05 November 2016, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=71001
- Mprem, 2016, *Practical challenges of complying with POPI*, viewed 05 January 2017, from <http://mprem.co.za/Publications/post/practical-challenges-of-complying-with-popi>
- Palmquist, M.E., Carley, K.M., & Dale, T.A., 1997, 'Two applications of automated text analysis: Analyzing literary and non-literary texts', in C. Roberts (ed.), *Text Analysis for the Social Sciences: Methods for Drawing Statistical Inferences from Texts and Transcripts*, Lawrence Erlbaum Associates, Hillsdale, NJ.
- Protection of Personal Information Act, 2013 c3*, viewed 27 February 2017, from <http://www.justice.gov.za/legislation/acts/2013-004.pdf>
- Pwc, 2011, *The protection of personal information bill: The journey to implementation*, Pwc.co.za/popi viewed 17 February 2017, from <https://www.pwc.co.za/en/assets/pdf/popi-white-paper-2011.pdf>
- Republic of South Africa, 2013, *Protection of Personal Information Act*, Publishing No. 4 of 2013, Government Printers, Pretoria.
- SAICA, 2017, *Draft legislations: POPI*, SAICA, viewed 19 February 2017, from <https://www.pwc.co.za/en/assets/pdf/popi-white-paper-2011.pdf>
- Solove, D., 2006, *A taxonomy of privacy*, University of Pennsylvania Law Review, pp. 154, 477–564.
- The Bill of Rights of the Constitution of the Republic of South African, 1996, Government Gazette. (No. 17678).
- Van den Hoven, J., 2008, *Information technology, privacy, and the protection of personal data in information technology and moral philosophy*, Cambridge University Press, Cambridge, pp. 301–322.
- Van den Hoven, J., Blaauw, M., Pieters, W. & Warnier, M., 2014, 'Privacy and Information Technology', *The Stanford Encyclopaedia of Philosophy*, Spring 2014 edn., viewed 19 February 2017, from <https://plato.stanford.edu/archives/spr2016/entries/it-privacy/> Stanford, CA 94305, US.
- Warren, D. & Brandeis, D., 1890, 'The right to privacy', *Harvard Law Review* 4(5), 193–220. <https://doi.org/10.2307/1321160>
- Westin, F., 2003, 'Social and political dimensions of privacy', *Journal of Social Issues* 59(2), 431–453. <https://doi.org/10.1111/1540-4560.00072>
- Workpool, 2017, 'What is POPI: The Protection of Personal Information (POPI) act explained', *Workpool Site*, viewed 05 November 2016, from http://www.itweb.co.za/index.php?option=com_content&view=article&id=71001