IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-56-

Are Organisations in South Africa Ready to Comply with Personal Data Protection or Privacy Legislation and Regulations?

Ntsako BALOYI[1], Paula KOTZÉ[1,2]
[1]CSIR Meraka Institute, PO Box 395, Pretoria, 0001, South Africa
Tel: +27 12 8412594, Fax: +27 12 8414270 Email: NBaloyi1@csir.co.za
Tel: +27 12 8412268, Fax: +27 12 8414270, Email: paula.kotze@meraka.org.za
[2]Department of Informatics, University of Pretoria, Private Bag X20, Hatfield, 0028, South Africa

Abstract: This paper reports on a survey conducted to determine the readiness of organisations in South Africa to comply with personal data protection or privacy legislation and regulations. Issues addressed include employee knowledge of personal data classification, policies, the POPI Act, standards, and training or awareness campaigns within organisations. The study also looked at the significance of viewing personal data protection beyond the South African context, including the use of cloud services. To present a balanced view, the study involved both management and technical employees of organisations. It was found that most of the organisations involved in the study are not data privacy compliance ready. The study aims to contribute by assisting organisations to gauge their readiness for data privacy compliance and sensitise them of the need for readiness.

Keywords: Personal data, data protection, POPI Act, responsible party, operator.

1. Introduction

In recent history, there has been a prevalence of reports on data breaches within various organisations [1]. A study conducted in the United States of America (USA) or US) investigating 529 security breach cases, found 1.9 billion compromised records, the majority of which were within corporates [1]. Although one would think that only large corporates would suffer this fate; more and more governments, universities and healthcare providers have become prime targets of data breaches.

When it comes to personal data privacy or protection, businesses are seen as culprits for non-compliance [1], whilst governments are viewed as abusing surveillance provisions in the name of national security [2]. Snowden, Assange and Manning are known for exposing privacy violations through surveillance by government [2]. These revelations have led to increased debates about privacy and surveillance [2].

The lack of trust in public and private institutions should be a course for concern. All organisations, whether they are government, business or non-profit entities, require the confidence of ordinary people. Organisations require people's trust and in turn, people are entitled to demand, as far as practicable and lawful, certain privileges from these organisations, such as the right to data protection or privacy. The power imbalance between organisations and natural persons when concluding contracts makes it incumbent on businesses to go the extra mile in protecting people's personal data, as their data collection practices might be found to be wanting under judicial scrutiny of informed consent, purpose specification and processing limitation principles, amongst others [3].

1.1 Data Protection Regulations and Enforcement

There is a worldwide rush of enacting data privacy legislation. A 2016 report indicated that there are about 108 counties that have enacted data privacy legislation [4]. The rush to enact data protection legislation is partly due to the fear to be cut off from economic activities as a result of restrictions on international data transfers, where there are no 'adequate' levels of personal data protection [5, 6]. This could have dire consequences for businesses.

The European Union (EU) Directive [5] was a game changer. It resulted in the conclusion of the EU-US Safe Harbour arrangement [7] to facilitate transfer of personal data by organisations subscribed to the arrangement. The Safe Harbour arrangement was, however, declared to be in violation of the EU Directive by the Court of Justice for the EU [8], and a new agreement called the Privacy Shield [4] has since been put in place. The EU has now enacted an even more advanced data protection law, called the General Data Protection Regulation (GDPR) [9], which starts operating in May 2018.

The South African Protection of Personal Information Act (POPI) [3] has been influenced by the EU Directive and Organisation for Co-operation and Development (OECD) Guideline [10]. The OECD Guideline contains the most commonly used data protection principles and is referred to in the drafting of many legal instruments. The South African POPI Act was thought to provide adequate protection in terms of the standard set out by the EU Directive [10]. Whether there will be potential amendments to the POPI Act, due to recent updates to EU data protection legislation, is yet to be seen. It is, however, important to note that whilst most data protection legislation protect only natural persons, the South African legal position extends protection to legal persons [3]. Although the POPI Act requires responsible parties to ensure appropriate organisational and technical safeguards for personal information in a wider context, this paper's focus is only on data privacy.

Legislation is only as strong as its actual enforcement. Having personal data privacy laws does not mean much, unless it proves to be effective in practice through established enforcement mechanisms. People can only enforce their privacy rights concerning data protection violations if they are confident that they will get actual recourse. The USA is known to be amongst countries with some of the worst data protection laws in the world (due to fragmentation), but comes out top on enforcement [11]. Under the EU-US Safe Harbour arrangement, the Federal Trade Commission (FTC) made data privacy findings against many organisations, but did not actually fine any [4, 12]. Some other countries on the other hand are known to have great personal data protection frameworks, but have little to no evidence of their actual enforcement [4, 11]. Data protection applies to, and should be observed by, both juristic and natural persons, including governments, with specific exceptions.

1.2 Businesses and Their Use of Personal Data

Many organisations pride themselves on doing smart things through technology whilst utilizing customer personal information. Some have developed cunning ways of obtaining personal data, such as competitions, reward programmes, etc. [13]. People might sometimes not even be aware of the collection, tracking or processing of their personal data. As an example, a top executive at Ford said that Ford collects personal information and conducts tracking activities on their customers [14]. With the advent of smart phones and other technologies, software applications collecting personal information have become prevalent in individuals' daily lives. Many of these applications collect more personal data than they require [15] and hardly comply with the data minimization principle [16]. Privacy notices might also be too technical, ambiguous or broad in their wording, making it difficult for customers or ordinary people to understand their implications.

The POPI Act [3] makes specific mention of how responsible parties (data controllers) and operators (processors) should conduct their data processing operations. Responsible parties determine the purpose and use of personal data, whilst operators process data on behalf of responsible parties. It is in the nature of every business to collect and process personal data, the least of which could be personal data relating to an employment relationship. Businesses also outsource certain functions, such as pension fund related activities, which require businesses (responsible party) to disclose certain personal data to an external party (operator or responsible party). Businesses also work with other businesses or institutions as suppliers, consumers or service providers. Personal data of legal persons satisfying the definition of personal data should be treated in line with the POPI Act [3]. Responsible parties and operators are more likely to be legal persons. It is therefore incumbent on organisations to know what is expected from responsible parties and operators.

Multinational organisations and those providing services to customers outside the borders of South Africa will also have to be aware of the data protection laws of those countries, in order to ensure compliance. It is important for businesses and institutions to not only comply with South African personal data protection legislation, but to also provide protection in line with international laws or benchmarks.

2. Objectives

This paper reports on a study to determine current personal data protection readiness within organisations in South Africa by determining employee knowledge of personal data protection and their organisation's practices and policies. More specifically, this study seeks to determine:

- Knowledge of the POPI Act and its implications for non-compliance.
- Compliance with certain personal data protection or privacy standards and frameworks.
- Knowledge and availability of training and awareness programmes aimed at ensuring information privacy.
- Knowledge of personal data protection policies.
- Potential positions of influence towards personal data protection practices.

The work presented in this paper is part of a wider research effort to establish the readiness of organisations within South Africa to address and deal with personal data protection in line with current and developing personal data privacy frameworks and legislation. This paper only considers employees of an organisation, particularly those dealing with personal data or systems handling personal data. Employees in this study are not treated as data subjects themselves, but as users of personal data within organisations. A separate paper covers data protection and data privacy of individuals as data subjects [17].

Section 3 outlines the methodology followed to collect and analyse the data for the study. The findings of the study are presented in section 4 and concluding remarks are made in section 5.

3. Methodology

The study was quantitative in nature. As part of a wider research effort, as described above, an online survey was conducted among employees of a number of South African organisations.

The survey was made up of 14 questions, with responses captured through Google Forms. The majority of the questions were 'yes/no' type questions, with three questions including the third option 'don't know', and one question presenting participants with an option to select multiple answers. The survey consisted of questions covering areas such as the participant's primary work role, personal data related work, organisational practices and

policies, etc. The criteria used to determine organisational readiness was based on employee knowledge of personal data classification, policies, the POPI Act, standards compliance, and training or awareness campaigns within organisations.

Snowball sampling was used, where participants directly targeted were requested to further disseminate the survey to other suitable participants. Participants were either from South Africa or had some employment link to South Africa. The first group of participants targeted were professionals (management and technical personnel) from the information and communications technology (ICT), telecommunications, pharmaceutical, healthcare, and banking industries, as well as government, ICT research and academia. The choice of industries was based on the authors' contacts, but participants were urged to pass the survey to other professionals across industries.

The rationale behind selecting both management and technical personnel was that they are most likely the people to influence decisions on how systems using personal information are built or purchased. Furthermore, they are expected to deal not only with such systems, but also with the handling of personal data and compliance with regulatory and legal prescripts related to personal data protection and privacy.

The survey was distributed via email and various social media platforms. The purpose of the survey was explained and users were afforded the opportunity and ability to view survey statistics. Participants were made aware of the confidential and voluntary nature of the survey. They were also alerted that the survey results would be used for research purposes only and that no personal identifying information would be collected, in line with the ethos of the study. In total 56 responses were received.

The strength of the relationship between the responses to various questions was analysed using the Pearson correlation coefficient analysis [18]. For a data set of n=56, any coefficient value (r), with an absolute value above 0.27 indicates a significant relationship. The Evans' guide [19] was used to classify the relationship strength (*very weak: 0.00-0.19, weak: 0.20-0.39, moderate: 0.40-0.59, strong: 0.60-0.79 and very strong: 0.80-1.00*).

This study does not claim to be exhaustive of personal data protection related issues in organisations or to be a fully representative sample.

4. Findings

This section presents the results of the survey as well as a brief discussion of the findings.

4.1 Work Level Demographics

Participants were requested to indicate if their primary work role is managerial or technical. The authors are aware that technical employees may sometimes assume management roles; likewise, management may sometimes take on technical tasks, hence reference to primary work role.

There was a near even distribution between technical (48.2%) and management (51.8%) participants in the survey, as depicted in Figure 1. This distribution will allow us to highlight the difference in the level of knowledge and priorities for the two typical work roles.

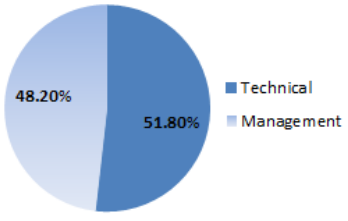


Figure 1: Management versus technical staff distribution of survey population

4.2 *Working with Personal Information*

Certain responsibilities require staff to work with people's personal information. The survey found that 73.2% of the participants, as depicted in Figure 2, work with people's personal information as part of their duties. This is a huge percentage and is evidence of the significance of the study conducted.

The survey results show a higher percentage of people in management (92.59%) roles working with personal data than those in technical roles (55.17%). Responses to the question under discussion were found to have a moderate relationship (r=0.42) with the primary work level.

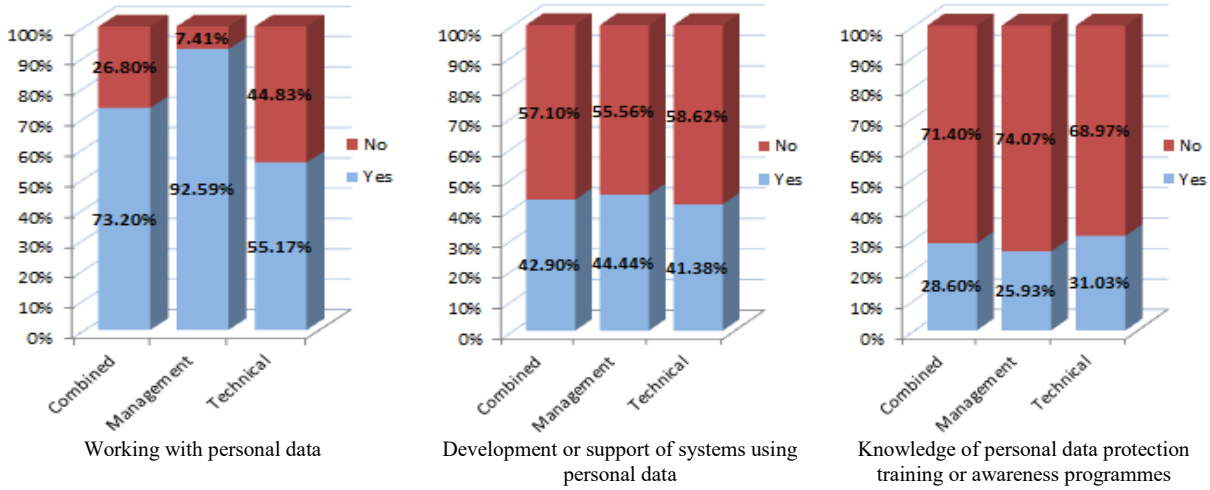


Figure 2: Working with personal data, systems collecting/storing personal data and related training

4.3 *Developing or Supporting Systems that Process Personal Information*

People who perform technical work, such as information technology specialists, may do work that involves the development or support of systems that process people's personal information. Management would normally oversee such work. Such people may actually be in a position to influence how systems are designed, and to ensure that principles such as privacy by default or privacy by design [12] are adopted. Their knowledge of the significance of data protection is thus important.

It was found that 42.9% of participants actually develop or support systems that process personal information, as illustrated in Figure 2. The results show almost similar percentages of management and technical people (44.44% and 41.38%, respectively) supporting/developing systems that process personal information.

4.4 *Training and Awareness [rogrammes*

Since 73.2% of the participants work with personal data, whilst 42.9% develop or support systems that process personal data. It becomes important to know whether such people are aware of any training or awareness programmes about personal data protection significance, regulations and potential non-compliance ramifications.

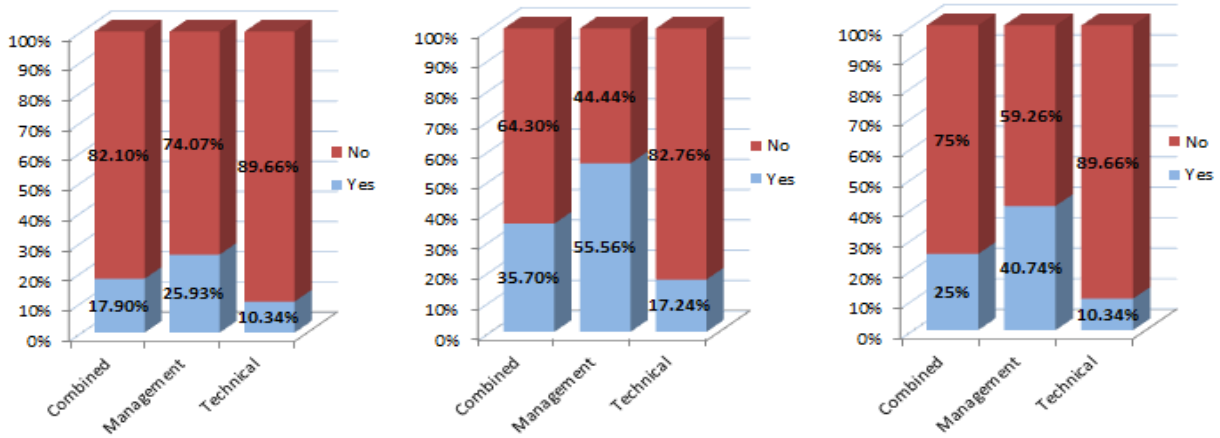
According to Figure 2, only 28.6% of all the participants were aware of such training or awareness programmes, whilst 71.4% were not. The question was not even about whether participants were trained, or made aware of how to handle personal data, but whether they were aware of the existence of any such services. The results were alarming. There is no question that a significant portion of management participants (74.07% to be exact) forms part of those not aware of such services, let alone being trained on personal data protection. This would make it difficult for management to recommend training on data protection for their employees, as most of management are not aware about the existence of such training

or awareness programmes in their workplaces, if there is any at all. This could be an indication that some South African organisations have not taken data protection or privacy as a business imperative yet. Interestingly, a higher percentage of technical staff (31.03%) knows about training and/or awareness programmes than management staff (25.93%).

4.5 Transborder Processing or Transfer of Personal Information

Many data protection legislation make provision for cross border transfers of personal information. The common standard for allowing data transfer is 'adequate level of protection' on the receiving country, but there are exceptions such as contract, consent, and so forth [3, 5]. Participants were asked whether they know of any transfer, storage or processing of personal data by their organisations outside South Africa.

Figure 3 shows that 17.9% of the participants indicated that they were aware of such transborder transfers or processing, whilst the majority (82.1%) were not aware of any. This is not surprising as most such operations would be confidential. This study has confirmed that some South African organisations do transfer or process personal data beyond the borders of South Africa. The results further show a higher percentage of management (25.93%) knowing about transborder transfers than technical (10.34%) employees. This is probably due to management's higher level of access to information and participation in decision-making.



Transborder processing or transfer of personal data

Processing personal data using cloud services

Sharing personal data with 3rd parties

Figure 3: Transborder transfer and cloud processing or sharing of personal data

4.6 Cloud Processing of Personal Information

The use of cloud services continues to gain popularity across industries [20]. This is to be expected as cloud services can offer great benefits to organisations, including cost savings [20]. The use of and control over cloud services can be challenging, as the physical equipment might be located in various jurisdictions with varying levels of protection for personal information. What is more interesting is that some people might not view this as a potential area of transborder transfer or processing of personal data. Participants were asked whether they knew of any storage, backup, processing or transfer peoples' information to the cloud or using cloud services by their organisations.

Figure 3 shows that 35.7% of the participants were aware of cloud related processing of personal data by their organisations, against 64.3% who did not know of such activities. It is interesting that the percentage of those aware of cloud related processing is slightly higher than that of those aware of transborder processing or transfers. A higher percentage of management (55.56%) appears to be aware of cloud processing than technical staff (17.24%). A strong correlation was found between the responses to the questions on

transborder transfers and cloud processing (r=0.53), whilst a moderate relationship was found between the responses to cloud processing and work level (r=0.40).

4.7 Sharing of Personal Information by Organisations

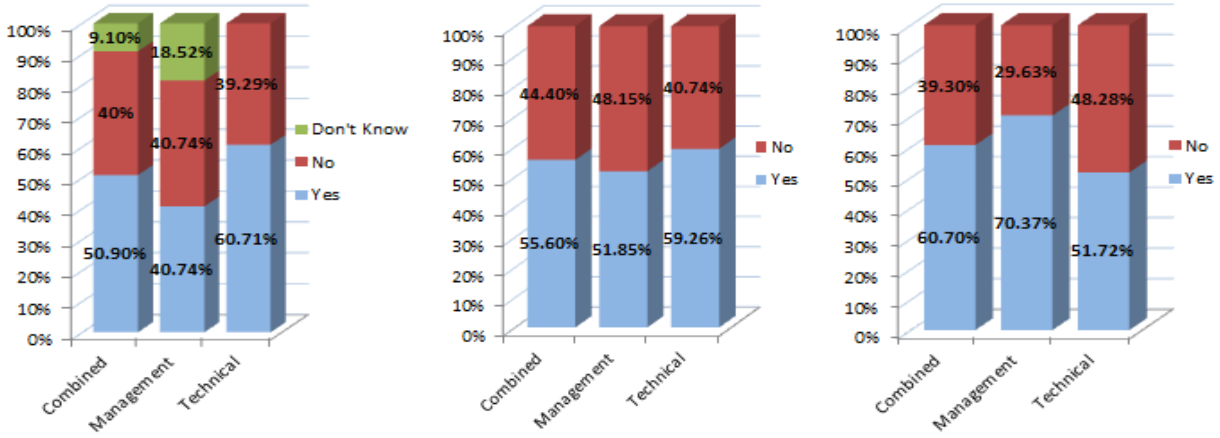
As argued in the introductory section, the processing of personal information is almost inevitable. In some cases, the same may be true for the sharing of personal data.

When asked whether participants knew of any sharing of personal data by their employers, 25% responded in the affirmative, whilst 75% said they were not aware of the sharing of any personal data as depicted in Figure 3. As can be expected from previous responses, a larger proportion of management (40.74%) knows about the sharing of personal data, than technical staff (10.34%).

4.8 Classifying Personal Data According to Sensitivity

Many data protection regulations make a distinction between personal data that is sensitive (special category or special personal information) and non-sensitive. It would indeed be interesting to know if organisations do make such a distinction when dealing with personal data. When participants were asked whether personal data was classified according to sensitivity in their organisations, 50.9% said it was, 40% said it was not, and 9.1% did not know whether it was or not, as presented in Figure 4.

It was found that those in technical work roles were more knowledgeable about the classification of personal data according to sensitivity (60.74%) than the management role (40.74%).



Personal data sensitivity classification | Personal data classification | Knowledge of personal data protection policies in organisations

Figure 4: Personal data policies and classifications

4.9 Classifying Personal Data into Categories

There are organisations that classify data according to confidentiality or some other criteria (e.g. top secret, secret, confidential, etc.). Participants were asked whether they knew of any classification applied to personal data in their organisations.

As can be seen in Figure 4, 55.6% indicated that they were aware of some classification applied to personal data, whilst 44.4% indicated that they were not aware of any classification. Management was almost evenly split on this question with 51.85% affirming to knowledge of classification and 48.15% negating. A higher percentage of technical staff knows about classification (59.26%) than management (51.85%).

4.10 Knowledge of Personal Data Protection Policies

To complement the question of data protection training/awareness, participants were asked whether they knew of the existence of any personal data protection policies in their

organisations. Whilst most participants were unable to vouch for such programmes, 60.7% of the participants were able to confirm knowledge of the existence of data protection policies in their organisations, whilst 39.3% could not (see Figure 4). Many organisations put together policies for various functions, and this finding could be an indication that just writing up policies without offering training/awareness programmes can be detrimental to organisations. It is worrying that 39.3% are not aware of any such policies.

Contrasting this to 73.2% of participants that work with personal data, it is clear that there are people that are working with personal data, without using any policies for guidance and most likely not trained to handle personal data. A higher percentage of management participants (70.37%) are knowledgeable about personal data protection policies than technical staff (51.72%).

4.11 Knowledge of POPI Act

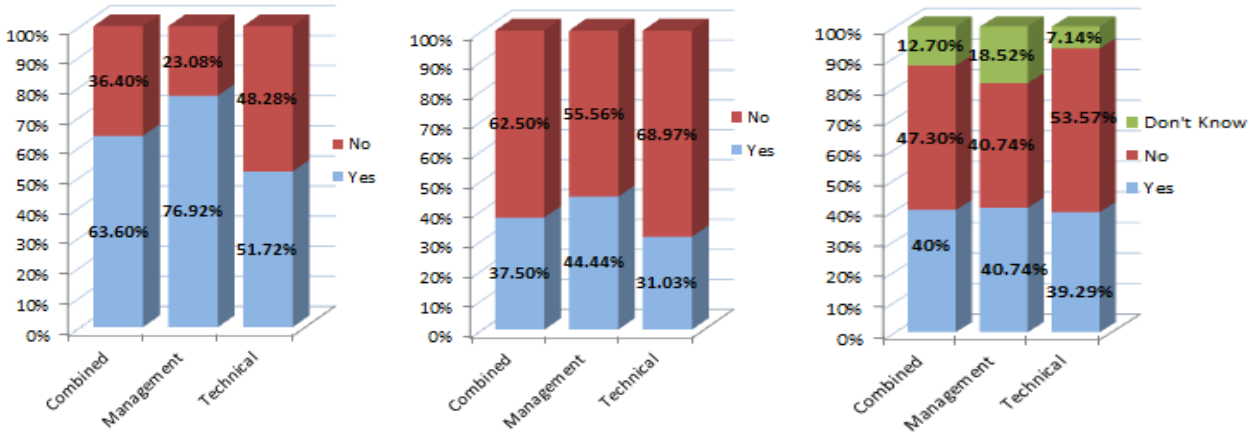
It is hoped that personal data protection policies would embody the most relevant and important provisions of current personal data protection laws. This might not necessarily be the case, and it is accordingly important to know if people are aware of the POPI Act [3] and its requirements relating to organisations.

When asked whether participants knew of the POPI Act and its requirements, 63.6% indicated that they did know, with 36.4% indicating that they did not, as depicted in **Error! Reference source not found.**. This may not be a problem provided that policies are updated to reflect current legislation. Just as with knowledge of policies, a higher percentage of management is knowledgeable (76.92%) about POPI Act than technical staff (51.72%).

4.12 Knowledge of POPI Act Non-Compliance Implications

Knowledge of the POPI Act may not necessarily translate into knowledge of adverse effects for organisations emanating from non-compliance with the POPI Act [3]. Participants were asked whether they knew of legislative effects or implications of non-compliance with POPI Act for organisations.

It was found that 37.5% of the participants were aware of non-compliance implications, whilst the majority (62.5%) were not aware, as illustrated in **Error! Reference source not found.**. This is a worrying finding in that not being aware of non-compliance implications may take away the seriousness of compliance, and may indicate ignorance of ramifications this could have for organisations and potentially individuals. A higher percentage of management participants (44.44%) are familiar with implications for non-compliance than technical staff (31.03%).



Knowledge of POPI Act and its requirements

Knowledge of POPI Act non-compliance implications

Organisation's policy compliance with POPI Act

Figure 5: POPI Act and policy compliance

These statistics are not surprising taking into account the proportions of familiarity with the POPI Act and the fact that management bare a greater burden of responsibility. A moderate correlation was found between responses to the question on knowledge of POPI Act and knowledge of non-compliance implications (r=0.59). A moderate correlation was also found between responses to this question and those for the one on knowledge of training or awareness programmes (r=0.41).

4.13 Data Protection Policy Compliance with POPI Act

Responsible parties are required to comply with requests for information, reasons, alterations, etc. of data subjects with regard to their personal data according to both the POPI Act [3] and Promotion of Access to Information Act [21]. In any regulatory landscape, business policies will only be as good as their compliance to national laws. However, actual compliance in practice and not policy compliance is what is important.

Participants were asked whether they thought their organisation's personal data protection policies are compliant with the POPI Act. **Error! Reference source not found.** shows that 40% of the participants thought their organisation's policies were compliant with the POPI Act, 47.3% thought their organisations personal data protection policies were not compliant, and 12.7% said they did not know of their organisations' position.

4.14 Compliance with Standards and Frameworks

There are various standards and frameworks that specifically deal with, or mention, personal data protection. Participants were asked which standards or frameworks their organisation's data protection policies comply with. This question allowed participants to select more than one answer; as a result, each bar in Figure 6 indicates the percentage of participants that selected each particular option.

Up to 76.4% of participants indicated that they did not know which standards their organisations complied with, 3.6% indicated that their organisations did not comply with any standards, and 3.6% indicated that their organisations complied with other standards than those on the options provided. Participants that indicated that their organisations complied with ISO standards for personal data protection were 10.9%, 3.6% indicated compliance with ITIL, 14.5% indicated compliance with King III, and 7.3% indicated compliance with COBIT [20]. It was interesting to note that management staff were more likely to select the governance framework (King III), than technical standards, in contrast to technical staff which selected the more technical standards like ISO and COBIT.

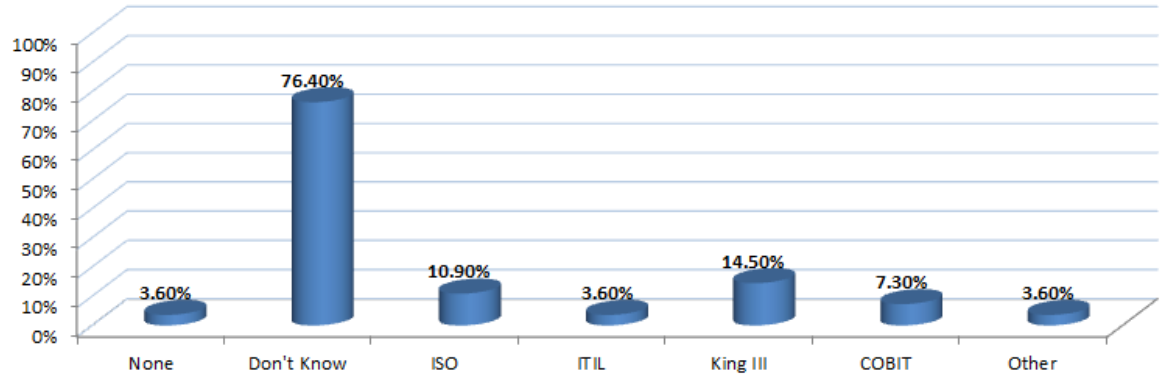


Figure 6: Data protection related frameworks and standards

4.15 Additional Analysis

Supplementary to the correlation results presented above, further significant but weak relationships are:

- Working with personal information against the development/support of systems handling personal data (r=0.28).

- Working with personal information and organisational compliance with POPI Act (r=-0.31).
- Knowledge of classifying data according to sensitivity and according to specific categories (r=0.36).
- Knowledge about classifying data according to sensitivity and not sharing personal data with third parties (r=-0.32).
- Classification according to a specific category is also related to knowledge of the existence of policies in the organisation (r=0.36) and privacy policy compliance to the POPI Act (r=0.33).
- Knowledge of the existence of privacy policies correlates with knowledge of existence of training or awareness programmes (r=0.35).
- Knowledge of the POPI Act correlates with knowledge of transborder transfers or processing personal information (r=0.31) and knowledge of training and/or awareness programmes (r=0.34).
- Knowledge of the POPI Act non-compliance implications correlates with knowledge of transborder transfers (r=0.31) and awareness of cloud processing (r=0.27).

5. Conclusions

The study found that within the personal data protection space, major work still needs to be done by many organisations. Most of the work required relates to the dissemination of information about personal data protection and privacy to those that work with personal data. A large number of participants indicated that they work with personal data in different contexts, whilst some develop systems that collect or process personal data. These people are supposed to know about personal data protection and data privacy, although many were not knowledgeable about it.

Many participants were not familiar with the POPI Act and even worse its non-compliance implications. Knowledge of compliance with data protection related standards and/or frameworks were also very low. Employees should understand the consequences of non-compliance, since privacy is a fundamental human right and personal data protection forms part of this right.

It also became clear that some employees are not aware of personal data protection policies in their organisations. Where no such policies exist, policies that are compliant with the POPI Act and other relevant laws should be developed. Organisations that have data privacy and protection policies in place should complement them with training programmes and/or awareness campaigns.

It appears that many organisations may not have data privacy training or awareness programmes for their employees, or they may not be well publicised. Where there are no training or awareness programmes, developing such programmes, or outsourcing the function, can greatly assist organisations and ensure that employees are familiar with provisions of the POPI Act and implications of non-compliance, amongst other things.

Lastly, it was found that some organisations still lack a classification system for personal data. The POPI Act and other international regulations make a distinction between sensitive and non-sensitive data, a form of classification that organisations can adopt as a minimum regarding personal data.

The findings of the study brought to question the readiness of organisations for personal data protection and privacy compliance. It is in the interest of businesses/organisations to guarantee their stakeholders that they take personal data protection seriously and are committed to treating it in accordance with applicable legal prescripts. The study pointed out some weaknesses with the hope that organisations will be able to gauge their own positions against the presented results and improve or correct accordingly. Through

reflection, assessments or audits, organisations can be positioned advantageously pending the full implementation of the POPI Act.

Personal data protection is not just a South African requirement but is becoming a legal business imperative in many jurisdictions. Organisations having businesses across borders, exporting or importing personal data, will have to comply with the personal data protection laws of all the relevant countries. Failure to comply may cost organisations business, result in fines or even imprisonment for responsible officials. Customer confidence in businesses that do not protect personal data may also be eroded.

Different industries inherently treat personal data differently, primarily due to the presence or absence of professional training and various environmental sensitivity issues. As future work, industry specific studies are proposed to address the particular interventions required for relevant industries and/or various professional or work roles.

References

[1] Erickson, K. and P.N. Howard, A case of mistaken identity? News accounts of hacker, consumer, and organizational responsibility for compromised digital records. Journal of Computer-Mediated Communication, 2007. 12(4): p. 1229 - 1247

[2] Cole, D.D., Assessing the leakers: criminal or heroes. Journal of National Security Law & Policy, 2015. 8: p. 107 - 118.

[3] Government of South Africa, Protection of Personal Information Act. 2013.

[4] Tesfachew, T., Key challenges in the development and implementation of data protection laws, in Data Protection Regulations and International Data Flows: Implications for Trade and Development. 2016, United Nations: Geneva. p. 7 - 22.

[5] The European Parliament and the Council of the European Union, Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Communities, 1995. 281: p. 31 - 50.

[6] Gustke, C. Which countries are better at protecting privacy. 2013.

[7] Farrell, H., Constructing the international foundations of e-commerce—The EU-US Safe Harbor Arrangement. International Organization, 2003. 57(2): p. 277 - 306.

[8] Raul, A.C., Global overview, in The Privacy, Data Protection and Cybersecurity Law Review, A.C. Raul, Editor. 2015, Gideon Roberton: London. p. 1 - 4.

[9] The EU General Data Protection Regulation. 2016: Allen & Overy.

[10] Roos, A., Data privacy law, in Information Communications Technology Law, D. van der Merwe, Editor. 2016, LexisNexis (Pty) Ltd: Johannesburg. p. 363 - 487.

[11] Tesfachew, T., Global developments and lessons learned, in Data Protection Regulations and International Data Flows: Implications for Trade and Development. 2016, United Nations: Geneva. p. 23 - 29.

[12] Rotenberg, M. and D. Jacobs, Updating the law of information privacy: the new framework of the European Union. Harvard Journal of Law & Public Policy, 2013. 36(2): p. 605 - 652.

[13] Hagel, J. and J.F. Rayport, The coming battle for customer information. 1997, McKinsey Quarterly.

[14] Wheels24 Q&A: The data your car collects and who can use it. 2016.

[15] Li, Y., et al., Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers, 2016. 65(5): p. 1339 - 1349.

[16] Alhadeff, J., Optimizing societal benefit of emerging technologies in policy development related to data flows, data protection and trade, in Data Protection Regulations and International Data Flows: Implications for Trade and Development. 2016, United Nations: Switzerland. p. 107 - 110.

[17] Baloyi, N. and P. Kotzé, Do users know or care about what is done with their personal data: A South African study, in IST-Africa 2017 Conference. 2017, IEEE: Windhoek.

[18] Krehbiel, T.C., Correlation coefficient rule of thumb. Decision Sciences Journal of Innovative Education, 2004. 2(1): p. 97.

[19] Evans, J., Staightforward Statistics for the Behavioural Sciences. 1996, Pacific Grove: Brooks/Cole Publishing.

[20] Carroll, M., A Risk and Control Framework for Cloud Computing and Virtualization, in Information Systems. 2012, University of South Africa: Pretoria.

[21] Government of South Africa, Promotion of Access to Information Act. 2000.