Aligning South African Data and Cloud Policy with the PoPI Act

Emma Raaff, Nicole Rothwell and Aidan Wynne
CAIR, School for Data Science and Computational Thinking, Stellenbosch University, South Africa
elraaff@gmail.com
ngrothwell00@gmail.com
aidanwynne.27@gmail.com

Abstract: On 1 April 2021, the South African government released the Draft National Data and Cloud Policy for public comment. This policy aims to support the digital economy in South Africa by implementing initiatives to augment the development of digital infrastructure and skills, with a specific focus on cloud computing. The adoption of the policy would help position the country as a data-driven economy. However, the implementation of such a policy is predicated on the existence of supporting digital infrastructure and aligned inter-departmental goals. Currently, there are many technological and legal considerations that must be addressed in order for such a policy to be implemented successfully. One particularly important consideration is how this policy relates to South Africa's Protection of Personal Information Act, which came into effect on 1 July 2021. The Act sets out legal imperatives for the collection, storage and use of personal information belonging to South African citizens. The aim of this paper is to analyze how the Draft National Data and Cloud Policy relates to the Protection of Personal Information Act in terms of what is proposed in the Policy and what is legislatively imperative in the Act. The overarching context for this evaluation is data governance in the cloud with an emphasis on the security of personal information. Macroeconomic threats and a shortage of critical ICT skills presupposes technical challenges for the implementation of a cloud service. Formal Concept Analysis is utilized to conceptualize and understand the relationships between the Draft National Data and Cloud Policy and the Protection of Personal Information Act. Classification, Confidentiality and Open Data are presented as technological challenges to cloud implementation. This paper aims to contribute towards an understanding of these challenges and how they are affected by South Africa's legislation and policies. We therefore investigate how the Draft National Data and Cloud Policy is situated in the broader context of data protection in South Africa.

Keywords: Cloud data governance, Cloud computing, Digital security, The PoPI Act, Data and Cloud Policy

1. Introduction

The current landscape of cloud computing in South Africa necessitates appropriate governance strategies to materialise the benefits associated with the Fourth Industrial Revolution. The Draft National Data and Cloud Policy (Draft Policy) presents an opportunity to investigate how the establishment of an open digital economy will align with existing policies, legislation and regulations. This research paper aims to analyse the current data protection landscape in South Africa to determine whether it is able to accommodate what is proposed by the Draft Policy. Insights drawn from a Formal Concept Analysis (FCA) lattice will be utilized to evaluate the relationship between the Draft Policy and the PoPI Act. This paper aims to offer recommendations for the restructuring of the Draft Policy to aid in its implementation.

The next section provides some background to contextualise the paper. Section 3 outlines the research design, after which Section 4 displays the results of the FCA process. Thereafter, Section 5 provides critical evaluation and discussion of results.

2. Background

Data governance encompasses the rights and responsibilities associated with the management of data assets (Al-Ruithe, Benkhalifa & Hameed, 2018). Forward-thinking organizations consider the implementation of effective data governance as a means to solve data-related issues (Al-Ruithe, Benkhalifa & Hameed, 2018). Cloud governance involves policies relating to the security, privacy, availability, compliance and location of cloud services. Since data governance is under-researched and often applied informally, regulations surrounding the management of data require enhanced clarity if they are to be effectively implemented.

The association between data and cloud computing is becoming increasingly prominent with the global drive towards digitisation. To protect individuals, organizations and governments, the creation of functional data and cloud governance policies and frameworks is imperative. However, there is limited research on cloud governance. A well-constructed governance strategy provides vision, establishes accountability, and encourages desirable behaviour from role-players in the data and cloud domain (Al Ruithe, Benkhalifa & Hameed, 2018).

2.1 Landscape on Cloud Computing South Africa

According to Kumar & Kumar (2016), “cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.” It depends on a well-established ICT ecosystem, contingent on broadband infrastructure, to ensure the availability and reliability benefits of cloud computing.

Cloud computing has the potential to reduce expenditure on physical ICT infrastructure and can augment government initiatives to provide more affordable service delivery (Gillwald & Moyo, 2017). Since 1994, the South African government has made significant progress in addressing ICT issues in the country. Effort has been made to achieve greater coordination between government departments and to align ICT with business processes (Gillwald & Moyo, 2017:44). However, challenges to the implementation of an effective data and cloud policy are still present.

2.2 Draft Policy Overview

Digitization presents South Africa with an opportunity to address its socio-economic challenges (Draft National Policy on Data and Cloud, 2021). Government and private sector organizations are increasingly shifting their service delivery models to the digital domain to provide accessible services to citizens and customers. The creation of the Draft Policy has been motivated by the acknowledgement that South Africa’s success in overcoming economic challenges is largely dependent on exploiting opportunities in the digital economy.

Currently, data generated by government is stored mostly in privately-owned databases. The lack of policy to guide data acquisition, ownership, storage, use and analytics pose a threat to national security and economic growth. There are numerous legal, policy, and regulatory documents situated in separate government departments, resulting in a lack of coordination. The Draft Policy aims to align the disparate documents in such a way that enables the country to develop a competitive digital economy.

The Draft Policy stipulates that the State Information Technology Agency (SITA) should act as the cloud champion. The Policy also emphasizes skills and infrastructure development. Therefore, the Policy targets some of the crucial developmental issues that South Africa faces.

2.3 The Landscape of Data Protection

New threats to the integrity and confidentiality of personal information are introduced by the Internet of Things (IoT), cloud computing and Big Data, and data protection initiatives are required as a result (Botha et al, 2017). Globally, over one hundred countries have implemented data protection laws. The General Data Protection Regulation (GDPR) is arguably considered the gold standard of privacy legislation. South Africa’s PoPI Act has been formed based on GDPR principles, alongside models from the USA, Canada, Australia and the UK (Botha et al, 2017).

2.4 The PoPI Act Regulation

The PoPI Act provides directives for the storage and processing of personal information belonging to South African citizens and juristic entities. Every responsible party that collects, stores, modifies or uses information must comply with the PoPI Act and will be held accountable for non-compliance. The legislation aims to protect Personal Information (PI), prevent theft, and uphold the fundamental human right to privacy (Nel, 2021). For the Act to effectively meet its aims, there are legal consequences for non-compliance, including civil class action, fines of up to R10 million and jail time of up to 10 years (Botha et al., 2017).

The PoPI Act outlines key stakeholders, defined in Table 1 (Republic of South Africa, 2013).

Table 1: Key Role Players in the PoPI Act

Key Role Players in the PoPI Act	
Actors	Role definition
Information Regulator	A government institution that investigates and fines responsible parties, enforcing compliance with the Act
Data Subject	Any party to whom personal information belongs
Responsible Party	A public or private body who decides why and how to process information
Data Processor/Operator	A party that processes personal information on behalf of the responsible party

3. Research Design

What the Draft Policy envisions appears to challenge what is prescribed by the PoPI Act and what is practically possible to implement within the South African context. Four research questions were formulated to guide the discussion surrounding data governance in South Africa. The aim of these questions is to understand the most important considerations for data governance and cloud security by making explicit the relationships between the PoPI Act and the Draft Policy. These questions contribute towards the overarching aim of understanding the current data protection landscape and evaluating whether South Africa is in a position to accommodate what is proposed in the Draft Policy.

3.1 Research Questions

The questions guiding the research problem include the following:
Q1: Does the Draft Policy have implications for the confidentiality of data?

Q2: What does the Draft Policy stipulate regarding the regulation of data and how does this relate to the PoPI Act?

Q3: Are there contradictions in what the Draft Policy proposes and how does the PoPI Act impact these discrepancies?

Q4: How does the Draft Policy propose the security of digital information assets and adhere to the PoPI Act?

3.2 Methodology

The research method utilised is Formal Concept Analysis (FCA), which is primarily used for graphical knowledge representation and exploration (Priss, 2007). FCA involves the representation of objects and attributes in a formal concept lattice, which can be analysed to discover concepts and relationships from the data. This paper utilises FCA to understand relationships between the Draft Policy and the PoPI Act.

Objects, attributes and the relationships between them are captured in a cross table, known as the formal context. The cross table is then used to build a formal concept lattice. In the lattice, each node represents a formal concept, consisting of a single object or several closely related objects and their shared attributes. Connections between concepts are represented by lines. For the purposes of this paper, aspects of the Draft Policy were encoded as objects and the principles from the PoPI Act were encoded as attributes. The lattice visually depicts the relationships between objects from the Draft Policy and attributes from the PoPI Act.

3.3 Application of FCA to the Draft Policy and the PoPI Act

3.3.1 Data Processing

The first step involved extracting the most significant concepts and principles from the Draft Policy and the PoPI Act. This was achieved by encoding policy interventions in the Draft Policy as objects, and key principles in the PoPI Act as attributes. A cross table of objects and attributes was created which formed the formal context.

3.3.2 Data Mapping

The formal context was used to build a formal concept lattice, which was created automatically by the selected FCA tool, ConExp. The lattice visually depicts the relationships between objects and attributes by systematically arranging them in such a way that clearly displays the paths between concepts. Figure 1 depicts the concept lattice that was created using the formal context.

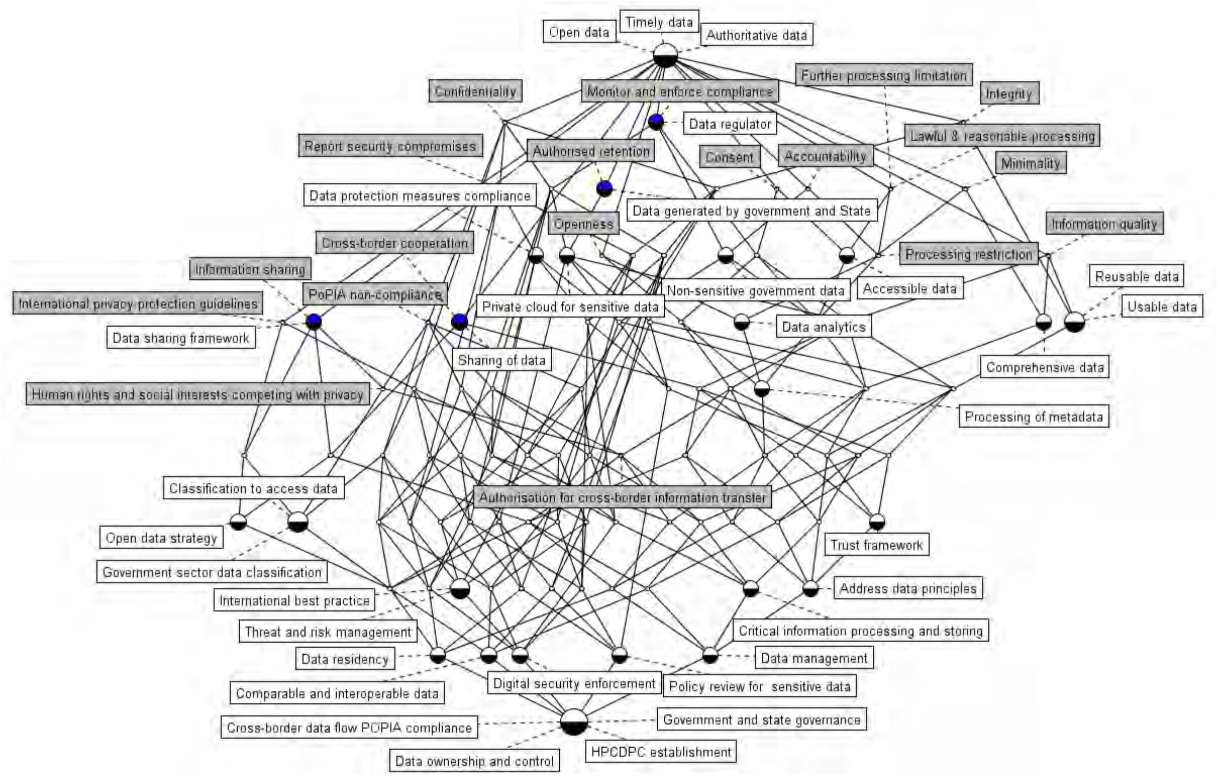
Open data
Timely data
Authoritative data
Confidentiality
Monitor and enforce compliance
Further processing limitation
Integrity
Data regulator
Report security compromises
Authorised retention
Consent
Accountability
Lawful & reasonable processing
Minimality
Data protection measures compliance
Openness
Data generated by government and State
Information quality
Cross-border cooperation
Processing restriction
Information sharing
PoPIA non-compliance
Non-sensitive government data
Accessible data
Reusable data
International privacy protection guidelines
Private cloud for sensitive data
Usable data
Data analytics
Data sharing framework
Sharing of data
Comprehensive data
Human rights and social interests competing with privacy
Processing of metadata
Classification to access data
Authorisation for cross-border information transfer
Open data strategy
Trust framework
Government sector data classification
Address data principles
International best practice
Threat and risk management
Critical information processing and storing
Data residency
Data management
Digital security enforcement
Policy review for sensitive data
Comparable and interoperable data
Cross-border data flow POPIA compliance
Government and state governance
Data ownership and control
HPCDPC establishment

Figure 1: The Concept Lattice built using ConExp.

3.3.3 Lattice Analysis

The final step in the process involved the evaluation of specific areas of the concept lattice to explore the research questions presented. The analysis was completed by identifying the key formal concepts and relationships relevant to the specific research questions presented in Section 3.1.

4. Results

4.1 Question 1: Confidentiality

One of the primary benefits of cloud computing is the increased availability of data. However, balancing availability with confidentiality and privacy is a challenge (AI-Ruithe et al., 2018). The concept lattice provides guidance on how the Draft Policy relates to the PoPI Act's requirements for confidentiality. The attribute of Confidentiality is related to three of the most significant objects in the lattice which are Open Data, Timely Data and Authoritative Data, and is also related to numerous other objects. Some of the more notable objects to which confidentiality is related are Private cloud for sensitive data, Policy Review for Sensitive Data, Classification to Access Data, Government Sector Data Classification and Data Residency.

The PoPI Act sets out strict requirements for responsible parties to ensure the confidentiality and integrity of personal data remains protected. S19(1) and S19(2) instruct a responsible party to put "reasonable technical and organisational measures" in place to prevent damage or unlawful access to personal information. The responsible party is obligated to identify "foreseeable internal and external risks to personal information" and implement safeguards against them, including post-implementation monitoring of the safeguards (Republic of South Africa, 2013). The Draft Policy is a means to augment the digital economy and enhance global competitiveness. However, establishing a high-availability cloud computing environment where sensitive data is stored and processed raises potential issues. While the Draft Policy does acknowledge the potential challenge of cloud adoption, it is unclear whether the country has the resources required to establish an adequate risk management strategy to ensure that the PoPI Act's requirements for confidentiality are upheld.

4.2 Question 2: Regulation

S 10(10.6.2) of the Draft Policy proposes reviewing "existing regulatory authorities' mandates" with the intention to establish a "single data regulator" to oversee all aspects of data governance (Draft National Policy on Data and Cloud, 2021). This could aid in coordinating legislation on data governance. However, the establishment of a Data Regulator would raise implications for the continued existence of other regulatory authorities. The PoPI Act has its own Information Regulator, and therefore a significant issue in the Draft Policy's mandate relates to how the PoPI Act will be upheld with the new role of a Data Regulator.

The lattice provides insight into the importance of the Data Regulator in the Draft Policy. The Data Regulator object is positioned close to the top of the lattice, subsuming many objects below it. Therefore, the Data Regulator is connected to, and has implications for, many interventions in the Draft Policy. However, despite being of high importance within the Policy, there is little discussion regarding the details of the Data Regulator's appointment and mandate in terms of the PoPI Act, especially regarding implications for the Information Regulator. Monitor and Enforce Compliance is the only attribute attached to the formal concept associated with the object of the Data Regulator in the lattice. Monitor and Enforce Compliance is synonymous with the role of the Information Regulator. An observation from the lattice is therefore the conservative association of the Data Regulator's responsibilities with the PoPI Act. This illustrates the importance of clarifying exactly how the Policy, and particularly the Data Regulator, relates to the PoPI Act's Information Regulator. The Draft Policy's proposition for a Data Regulator is to consolidate the regulatory bodies stipulated in relevant legislation, suggesting that the Data Regulator could replace these bodies completely. However, there is little information provided on how exactly the Data Regulator would integrate with the PoPI Act and whether this new body would, in fact, entirely replace the Information Regulator.

It is also unclear whether there is capacity to establish such a body when considering that the Information Regulator under the PoPI Act faced significant personnel shortfalls; even after its implementation in July 2021, the body did not have a Chief Executive Officer (Nel, 2021). There is also uncertainty surrounding the implementation of the PoPI Act, with organisations being unsure how to comply with the Act due to the fact that the responsibility for educating organisations on compliance falls to the Information Regulator. The challenges experienced by the Information Regulator are a concern when considering the establishment of the Data Regulator, as this body would require more resources and capability than the Information Regulator due to its responsibility for overseeing all aspects of data governance.

4.3 Question 3: Potential Contradictions

The primary rationale behind an open data economy model and an open data strategy is to provide an inclusive environment that promotes innovation and economic growth （Draft National Policy on Data and Cloud, 2021). The Draft Policy argues for data localization and residency, in order to ensure that the country receives value from local data processing. There are potential contradictions between the Draft Policy's stipulations regarding its open data policy and those regarding data localization and residency, which could infringe on the rights of citizens.

The concept lattice supports the idea of potential contradictions between the Draft Policy and the requirements of the PoPI Act. The attributes of International Privacy Protection Guidelines, Information Sharing, and Cross-Border Cooperation, from the PoPI Act, are all related to the three most significant objects, of which Open Data is the most relevant when evaluating the Open Data Strategy proposed by the Draft Policy. Open Data is an object of the most general formal concept in the lattice, having no attributes and subsuming all other concepts.

Data localization, which is the most restrictive policy measure referenced in the Draft Policy, stipulates that all data created within a nation are the property of that nation (Wong, 2020). This results in the nation having ownership over the data, whereby its governing laws dictate how the data will be treated and whether cross-border data flow is allowed. The PoPI Act's primary purpose is set out in Section 2. S 2(a)(ii) recognizes that privacy is a fundamental right, and that safeguards to protect this right must be in place.

Furthermore, S 2(b) of the Act aims to regulate how personal information is processed by establishing conditions that are in alignment with international standards and best practices. The purpose statements set out in S 2 of the PoPI Act support the Draft Policy's open data strategy and the free flow of information in South Africa and across its borders. The mandate also maintains regulatory consonance with international processing standards regarding personal information (Republic of South Africa, 2013). However, one can argue that the South African government could introduce a data localization framework that contradicts the open data strategy proposed in the Draft Policy. Restricting the free flow of data will create a closed data environment. Therefore, while aspects of the PoPI Act and Draft Policy support an open data strategy, the proposal of a data residency, sovereignty, and localization framework will conflict with the open data strategy as stipulated in the Draft Policy. Ambiguity surrounding this issue should be removed by providing clarity in the Draft Policy.

4.4 Question 4: Security Issues

As the nation undertakes digitalization through the development of state digital infrastructure, security threats are presented. Cybersecurity is an element that requires consideration by the South African Government due to the implications of the Draft Policy (Sutherland, 2017). South Africa has fallen behind in prioritizing cybersecurity legislation and lacks the skilled labor to meet the demands required of the nation. South Africa's cybersecurity landscape, coupled with the risks associated with cloud computing, raises the question of whether South Africa has the ability to sufficiently mitigate cyber threats.

The concept lattice indicates all objects and attributes related to the Digital Security Enforcement object. The lattice can be used to substantiate cybersecurity shortfalls that the Draft Policy and the PoPI Act present. This formal concept, Digital Security Enforcement, is a very specific concept which is subsumed by most of the other concepts in the lattice. The main attribute intents of Digital Security Enforcement that will be evaluated are Report Security Compromises, Monitor and Enforce Compliance, and International Privacy Protection Guidelines.

The Draft Policy identifies two important considerations under S 10.3, recognizing the role of the PoPI Act and its guiding principles while ensuring accurate monitoring and enforcement of compliance (Draft National Policy on Data and Cloud, 2021). The second issue, under S 10.5 recognizes that South Africa has among the worst "online crime" in the world (Draft National Policy on Data and Cloud, 2021). One of the main concerns of the Draft Policy's open data strategy is that the proposed data protection and cybersecurity policy interventions may not suffice in safeguarding the proposed digital infrastructure. The PoPI Act also carries implications for cybersecurity, given its broad exemptions for national security (Sutherland, 2017). Government and private entities have not expressed confidence in the current cybersecurity infrastructure to prevent cyber-attacks. This raises doubt regarding whether the Draft Policy and its associated open data strategy can be implemented without exacerbating vulnerabilities.

5. Evaluation and Discussion

5.1 Question 1: Confidentiality

S 19 of the PoPI Act states that the integrity and confidentiality of personal information must be upheld while mitigating unauthorized access and unlawful processing. The Draft Policy proposes the instatement of a public High-Performance Computing and Data Processing Centre (HPCDPC). This will make data widely accessible, which fulfills the Policy's open data strategy. This public cloud will store all non-sensitive government and state data. Existing data protection laws and minimum-security standards will determine what is classified as non-sensitive data. Sensitive data will be stored in a private cloud to ensure adequate measures are in place to ensure confidentiality. Ensuring the confidentiality of data first requires accurate classification frameworks. The Draft Policy states that any handling of personal information will be in accordance with the PoPI Act. However, this rests on classification processes. Furthermore, if the Draft Policy were to be implemented, it would require classification activities to be conducted with collective responsibility and a high regard for best practice. There are concerns regarding the ability of current classification frameworks to uphold the PoPI Act if the Draft Policy were to be implemented. Before the Draft Policy is implemented, existing cybersecurity legislation, frameworks and initiatives surrounding classification should be evaluated to ensure that they offer adequate protection of confidential personal information.

5.2 Question 2: Regulation

A prominent point of ambiguity in the Draft Policy is found in s 10(10.6.2), which proposes a "review of existing regulatory authorities" and the subsequent establishment of a Data Regulator. It is unclear whether the Data Regulator would completely replace existing regulatory bodies stipulated in the PoPI Act and other legislation, or if it would extend and support existing bodies. There is also significant concern around the Data Regulator receiving sufficient funding for the responsibility placed on it, as it would oversee all aspects of data governance and management. This concern arises primarily out of difficulties faced by similar bodies such as the PoPI Act's Information Regulator.

A solution to these challenges is for the Draft Policy to provide a more explicit and detailed description of what exactly the Data Regulator would do and how it would integrate with existing security and data-related regulatory bodies. In addition, insight is needed into how the review of existing regulatory bodies would be conducted and therefore how the Data Regulator would come into existence. This would prevent ambiguity and uncertainty. The Draft Policy must also ensure that research is undertaken into the difficulties faced by similar regulatory bodies in order to reduce the challenges presented to the Data Regulator.

5.3 Question 3: Potential Contradictions

The Draft Policy states that data ownership and cross-border data flow will be in accordance with the PoPI Act (Draft National Policy on Data and Cloud, 2021). While this reduces the risk of ownership and data flow being in contradiction to the PoPI Act, there are issues to consider regarding the way that the PoPI Act and the Draft Policy deals with ownership and data flow. Malinga (2021) reports on these issues and raises the important point that static or raw data lacks economic value. Value is generated through processing and data flows. While the Draft Policy recognises the need to ensure that data increases in value through effective processing and transfer, there appears to be significant emphasis on keeping data processing local under the PoPI Act. Therefore, while there is no outright contradiction between the Draft Policy's aims and the PoPI Act's provisions regarding data ownership and flow, there is a risk that this approach to data ownership and cross-border flow, drawn from the PoPI Act, contradicts the Draft Policy's own aims to develop the digital economy to its full potential. The Draft Policy should then be clearer in how the capacity of local data processing will be improved to ensure that it can fulfil its aims of creating increased value to develop a digital economy.

With regards to non-personal information, it could prove effective to allow freer flow of data across borders and enable non-local data value generation instead of creating a situation of data localisation. As it stands, it seems that there is a risk for this under the Draft Policy. This could result in the loss of potential value that could be generated though non-local data processing and a freer flow of data across borders. Therefore, while the Draft Policy places emphasis on developing local data processing and value creation, it must be ensured that South African public and private institutions have the required faculty to generate this value. It should also be ensured that the opportunity for value creation provided by non-local processing and ownership of data is not overlooked.

A recommendation for solving the abovementioned issues is to balance local data processing and value creation with non-local data processing, flow and ownership. The Draft Policy should also ensure that sufficient research is conducted into the potential for South African institutions to process data and produce value, and use this research to inform how restrictions placed on cross-border data flow and ownership are formulated.

5.4 Question 4: Security Issues

The Draft Policy indicates a need for Cybersecurity Measure reform and improvement as the current cybersecurity ecosystem in South Africa is arguably unequipped to mitigate new threats. The protection of personal information from cybercrime is dependent on South Africa's capability to implement an appropriate risk mitigation infrastructure. This has been a priority for the country in recent years; Gillwald & Moyo (2017) note that SITA has been working to improve its security standards in efforts to mitigate cybercrime. However, due to limited capacity, it is unclear whether the state of cybersecurity in South Africa is currently prepared to mitigate cyber threats at the level required by the Draft Policy. The Cyber-security Bill is arguably considered as a turning point for South Africa's cybersecurity initiatives. However, it is not referred to explicitly in the Draft Policy. A recommendation is for the Cybersecurity Bill to be acknowledged while stating that the Draft Policy will be in accordance with the Bill to emphasize how cybersecurity legislation is being enforced, thereby ensuring that there is legislated protection against unlawful activity.

The South African government should first attempt to improve the state of cybersecurity in the nation before attempting to implement the Draft Policy. The Draft Policy places emphasis on this, stating that current cybersecurity measures should be updated. For example, s 10(10.5.2) and s 10(10.5.3) state that cybersecurity legislation such as the NCPF should be reviewed to ensure that it accounts for the threats and risks accompanying increased digitization, as well as ensuring capability to respond to risks. However, cybercrime is presented as a significant challenge and it is unclear whether there is sufficient capacity to develop the current cybersecurity infrastructure to a point where the Draft Policy can be implemented without exacerbating vulnerabilities. S 10(19.1.5) states that the HPCDPC will be cloned to establish two similar centres which will provide backup and ensure operation continuity in the case where the HPCDPC is a target of a cyberattack. The Draft Policy's contingency plan accounts for the current cybersecurity climate, however, legislation and frameworks should be reviewed as a precursor to the infrastructural development under the Policy to first create a secure cybersecurity ecosystem. A recommendation is that more should be invested into developing the country's cybersecurity infrastructure and skills before the Draft Policy is implemented, in order to ensure that South Africa is fully equipped to deal with the new threats and risks associated with cloud computing and increased digitization.

5.5 Establishing SITA as the Cloud Champion

The Draft Policy stipulates that SITA will become the champion of cloud computing in the country. A significant emphasis in the Draft Policy is the establishment of the High-Performance Computing and Data Processing Centre (HPCDPC) which will provide data processing facilities and cloud computing services. The Draft Policy places much of the responsibility for this Centre on SITA. However, implementing the HPCDPC will prove challenging, since SITA faces significant obstacles that could hinder its ability to successfully carry out its precept under the Draft Policy (Gillwald & Moyo, 2017). SITA's 2020-2025 Strategic Plan (n.d.:42) highlights the challenges still faced by the agency. Some of the key issues highlighted in the Strategic Plan relate to funding, leadership and corruption. Therefore, SITA will face challenges meeting the requirements associated with a cloud champion. In the past, SITA has prohibited the use of cloud computing services, which has resulted in the constriction of this technology at a national and provincial government level (Gillwald & Moyo, 2017). Thus, a fundamental shift is required by SITA if they are to become the primary custodian of cloud computing under the Draft Policy. A solution to ensure that the agency carries out their role effectively is to ensure accountability to an external body. If responsible parties, and organizations in particular, are going to entrust personal information for which they are responsible to SITA, there must first be stringent accountability and security practices in place. Therefore, SITA is a crucial component when evaluating the likelihood for success of the Draft Policy.

6. Conclusion

The Draft National Data and Cloud Policy is a promising development in South Africa's digital environment. While the policy is recognized as being valuable, there are many important considerations that have to be accounted for regarding its implementation. This paper has focused on several areas in which the Draft Policy relates to the PoPI Act, including availability and confidentiality, data regulation, data localisation and digital security. In addition, a discussion of SITA as the cloud champion was presented. An evaluation of potential challenges in those areas was conducted in an attempt to contribute to an understanding of data governance in the cloud. Suggested strategies to address the implications of the Draft Policy were presented. The evaluation presented in this paper was guided by Formal Concept Analysis and involved the examination of a concept lattice generated by ConExp. The Draft Policy promotes a modern data governance landscape in South Africa. However, more transparency and clarity in the policy is required to ensure that the principles of the PoPI Act are effectively complied with, along with the restructuring of the Draft Policy document to enable the benefits associated with cloud computing to be realized.

Future work could include the evaluation of relationships between the Draft Policy and other legislation such as the National Cybersecurity Policy Framework. As the Draft Policy is still in draft format, once implemented, future work could focus on the impact of the Policy in comparison to how other countries have undertaken the adoption of cloud computing.

Acknowledgements

We would like to sincerely thank Arina Britz and Bruce Watson for their guidance and support, while encouraging us throughout. This work is based on the research supported in part by the National Research Foundation of South Africa (Grant Number:136211) and the Centre for AI Research (CAIR).

References

Ahuja, S. and Mani, S., 2012. Availability of Services in the Era of Cloud Computing. *Network and Communication Technologies*, 1(1).

AI-Ruithe, M., Benkhalifa. and Hameed, K. (2018). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing* [Electronic], 23(5). Available: https://doi.org/10.1007/s00779-017-1104-3 [2021, October 5].

Botha, J., Grobler, M.M., Hahn., J. and Eloff, M.M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. *International Conference on Cyber Warfare and Security (ICCWS).*

Department of Communications and Digital Technologies. (2021). *Draft National Policy on Data and Cloud* [Online]. Available: https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf [2021, October 5].

Gillwald, A and Moyo, M. (2017). *Modernising the Public Sector through the Cloud.* [South Africa]: Africa Portal [Online]. Available: https://media.africaportal.org/documents/Cloud-Computing-in-the-public-sector-final-25052017_V03.pdf [2021, October 5].

Kandeh, A., Botha, R. and Futcher, L. (2018). Enforcement of the Protection of Personal Information (POPI) Act: Perspective of data management professionals. *SA Journal of Information Management*, 20(1).

Kumar, M and Kumar, N. (2016). Cloud Computing: Architect and Use of Technology in the Past, Present and Future. *International Journal of Research in Engineering, Technology and Science* [Electronic], 6. Available: http://www.ijrets.com/wp-content/uploads/2016/08/160314084-11.pdf [2021, October 5].

Malinga, S. (2021). *Several flaws in SA's draft data and cloud policy, say experts* [Online]. Available: https://www.itweb.co.za/content/xA9PO7NZ46Z7o4J8\ [2021, October 5].

Nel, P. (2021). Personal Interview. 22 July.

Priss, U. (2007). Formal Concept Analysis in Information Science. *Annual Review of Information Science and Technology* [Electronic], 40(1). Available: https://doi.org/10.1002/aris.1440400120 [2021, October 5].

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

State Information Technology Agency. (n.d.). *2020-2025 Strategic Plan.* [Pretoria]: SITA [Online]. Available: https://www.sita.co.za/sites/default/files/Strategic%20Plan%202020-2025.pdf [2021, October 6].

Sutherland, E. (2017). Governance of Cybersecurity – The Case of South Africa. *The African Journal of Information and Communication*, (20): 83-112.

Thamm, M. (2018). SAPS/SITA capture: FDA holds South Africa to ransom, threatens to 'collapse criminal justice system'. *Daily Maverick* [Electronic], 5 April. Available: https://www.dailymaverick.co.za/article/2018-04-05-sapssita-capture-fda-holds-south-africa-to-ransom-threatens-to-collapse-criminal-justice-system/ [2021, October 6].

Wolff, K.E. (1993). A First Course in Formal Concept Analysis How to Understand Line Diagrams. *SoftStat '93: Advances in Statistical Software 4, 429-438* [Electronic]. Available: https://sites.tufts.edu/ancientbirds/files/2018/06/a-first-course-in-formal-concept-analysis.pdf [2021, October 5].

Wong, B. (2020). Data Localization and ASEAN Economic Community. *Asian Journal of International Law* [Electronic], 10(1). Available: http://dx.doi.org.ez.sun.ac.za/10.1017/S2044251319000250 [2021, October 5].