A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws

J. Botha[1, 2], M.M. Grobler[1, 4], J. Hahn[3], M.M. Eloff[2]
[1]Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2]Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa
[3]Boston University, Boston, United States of America
[4]University of Johannesburg, Johannesburg, South Africa

[1]jbotha1@csir.co.za
[1]mgrobler1@csir.co.za
[3]jadehqc@bu.edu
[2]eloffmm@unisa.ac.za

Abstract: Data protection and management of personal information has become an integral aspect for organisations and individuals in conducting business in the modern era. It has also become a major issue for legislators, regulators and consumers worldwide due to the widespread repercussions when personal information is negligently or maliciously used. Despite increased attention on personal information and the existence of data protection legislation internationally, data breaches remain a common occurrence. It has become crucial now, more than ever, for organisations to manage and safeguard personal information. As a nation, South Africa has addressed the need for increased protection - the Protection of Personal Information (PoPI) Act was signed into law in November 2013. This paper presents a comparison between the South African PoPI Act and other international data protection laws in order to highlight similarities and differences. These privacy legislations will be compared based on the principles set out by the PoPI Act. Other areas to be considered include data protection officers, enforcement, electronic marketing, online privacy and the year enacted. Data protection compliance is not straightforward and having the correct measurements and procedures in place is of utmost importance. These findings can be applied in future work to examine where South Africans can make use of already established international best practices to best enforce their privacy regulation.

Keywords: Data Breach; Compliance; Personal Information; PII, PoPI Act; Privacy Laws

1. Introduction/Background

The risk of breaching data protection legislation and regulation has grown significantly with the increase of the amounts of personal data being kept by various organisations and individuals (The Privacy Advisor, 2008). Since it is a global right for individuals to have their personal information protected against any unlawful collection, retention, dissemination and use, a significant number of data protection laws have been enacted internationally. Europe, for example, adopted the European Union's (EU) Data Protection Directive (DPD) already in 1995 (Birnhack, 2008). This Directive has been revised in 2015 and unified into a law known as the General Data Protection Regulation (GDPR). The United Kingdom (UK) adopted the Data Protection Act (DPA) in 1998 (United Kingdom Government Gazette, 1998), together with the EU DPD and was implemented in 2000. The United States does not have a specific data protection legislation, but has enacted a number of privacy laws since 2001 (Information Shield, N.D.).

In South Africa, the Protection of Personal Information (PoPI) Act has been signed on November 26th 2013 (South African Government Gazette, 2013), although the full enforcement date of the PoPI Act is still to be determined by the country's privacy regulator. South Africa is in the process of complying with the Act, but is facing implementation challenges. The objective of this paper is thus to perform a comparison between the PoPI Act and selected available international data protection laws in order to assess the PoPI Act's comparability with international laws. Although the positions and criticism raised against the PoPI Act are controversial (Heyink, 2015; Luck, 2014), this comparative research study aims to show that the PoPI Act is not a step back in terms of law evolution, but rather a step towards the worldwide tendency to modern personal information protection. It is undeniable that regulating the digital world is difficult as it evolves faster than

legislation can be passed, but it should be noted that technology does not have to complicate regulation, it can also be harnessed to assist regulators in their efforts.

2. Methodology

A brief overview is presented on international data protection laws and the PoPI Act, based on a desktop study. The principles of the PoPI Act are compared at a high level with African and non-African data protection laws (see sections 4 and 5). A basic literature review is conducted to gain a better understanding in terms of the PoPI Act and similar Acts globally. This will give a sense of the actions required for PoPI compliance. Data has been collected using existing literature as well as governmental and private industry reports.

3. An overview of International Data Protection Laws and the South African PoPI Act

Globally more than 100 countries, independent jurisdictions and territories have adopted comprehensive data protection/privacy laws to protect personal data held by governments and private companies (Banisar, 2016). Figure 1 presents a map indicating which jurisdictions have adopted laws and which are currently addressing this need: countries highlighted in blue have enacted comprehensive data protection laws, whereas countries in red have a pending obligation to enact such a law. The countries highlighted in white either have no initiatives to enact a specific singular data protection law or no information about such laws is available online. South Africa is the 15th African country to implement a data protection law (Fichet, 2015). The PoPI Act will not be compared to all the countries highlighted in Figure 1, but only to a selected few countries, chosen primarily for their territorial location, large economies and mature regulations.

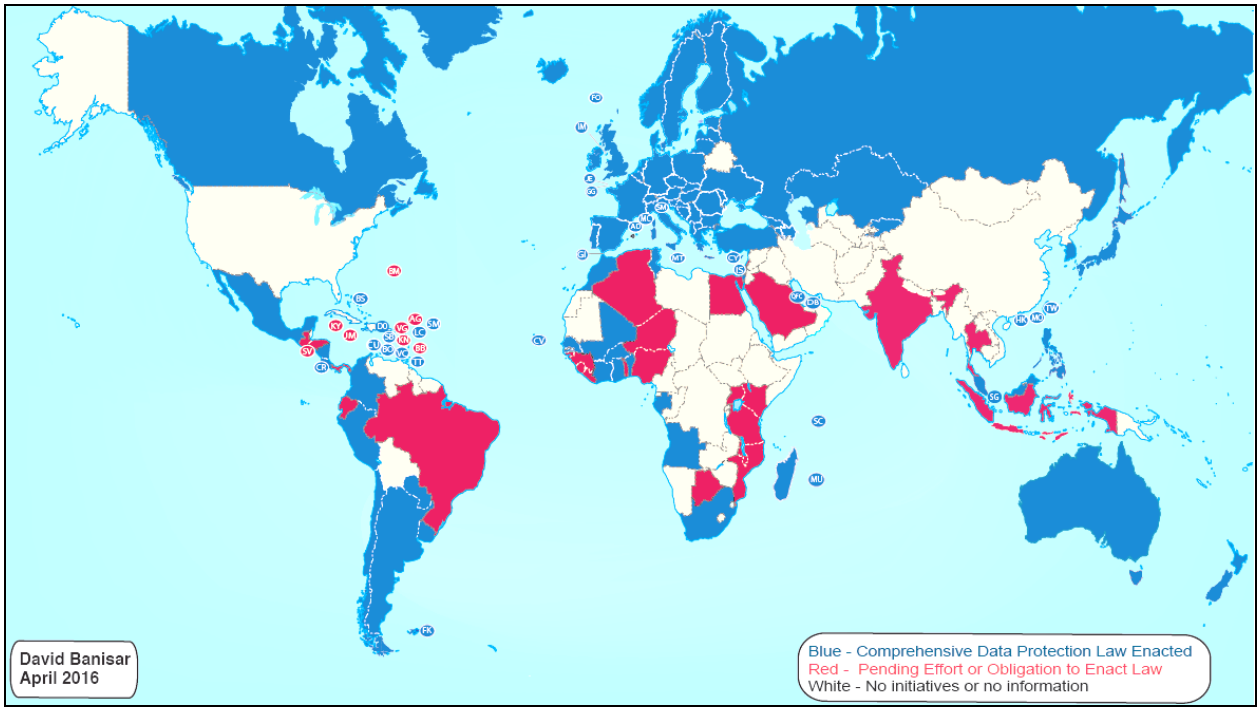

Figure 1: National Comprehensive Data Protection/Privacy Laws and Bills 2016 (Banisar, 2016)

The PoPI Act presents a set of conditions and principles that prescribe the way in which personal information may be processed (Michalsons, 2014). The Act was created based on the EU DPD (Birnhack, 2008; DataGuidance, 2013) and the Organisation for Economic Co-operation and Development (OECD) principles (PLI, 2016). It was further inspired by models of data privacy from the United States (US), Canada, Australia and the UK (Kokutse, 2011). The intention was to have personal information privacy regulated in South Africa in harmony with international laws in order to stimulate business and cross-border transfer (Pillay, 2016). According to the Norton Cybercrime Report, South Africa ranks third in the world for cybercrime victims (Business Media Live, 2015). South Africa was only surpassed by China and Russia (Lamprecht, 2013). The high ranking in cybercrime clearly raises the need for enforcing data protection laws and raising compliance awareness. Crime however is not the only reason companies should endeavour to comply with the PoPI Act.

When dealing with personal identifiable information (PII), the PoPI Act mandates significant changes in both governmental departments and commercial organisations. Legislated penalties for failing to comply with the Act are significant and can even lead to incarceration for negligent corporate officers. Having this legislation in place opens new implications for disclosing PII (South African Government Gazette, 2013). Organisations will not be allowed to use, store or process PII without individuals' consent and will face consequences for non-compliance to this Act. Consequences include but may not be limited to:

- Damage to a company's reputation.
- Losing customers.
- Inability to attract new customers.
- Pay-outs in damages as a result of civil class action.
- Fines of up to R10 million.
- Facing jail time of up to 10 years.

These consequences, as well as the organisations' will to protect individuals' sensitive information, enforce the need for organisations to conduct themselves in a responsible manner regarding PII. It is predicted that PoPI will become enforceable towards the end of 2017. Organisations should therefore focus on conducting PoPI audits and putting PoPI policies in place to prevent these consequences. It is believed that implementing the PoPI Act would aid global competitiveness, cybercrime and the right to privacy (Gunning, 2016).

Table 1 gives a short description of each of the eight principles that guide the PoPI Act. In addition to these principles, there are other important definitions and structures set by the PoPI Act. For example, the Act entitles an independent Information Regulator to promote and monitor the compliance with the law. Similar to the EU DPD, the PoPI Act also applies to a non-resident in the country as long as the automated or non-automated processing is within the country's borders (Svantesson, 2014).

Table 1: Principles of the PoPI Act

PoPI Principle	Description
Accountability	The responsible party must ensure that the principles are adhered to.
Processing Limitation	There must be limits to the processing of information; processing must be lawful and not excessive.
Purpose Specification	Personal information must be collected for a specific, defined and lawful purpose that is related to the responsible party's activity; the subject should be aware of this purpose.
Further Processing Limitation	Any further processing must be compatible with the purpose that the information was collected for.
Information Quality	The responsible party must ensure that the personal information is complete, accurate and not misleading; the information can be updated if necessary.
Openness	A notification must be given to the Information Protection Regulator before the information is processed the subject must be notified that data is being collected about them.
Security Safeguards	The responsible party must ensure that the integrity of the collected personal information is maintained.
Data Subject Participation	The subject has the right to ask and be given the details of any information on him/her that the responsible party might have, at no cost.

(South African Government Gazette, 2013)

Since the PoPI Act requires changes in the way organisations conduct themselves in terms of the use and processing of PII, a comparative study was conducted to determine how the PoPI Act compares with international data protection laws. Table 2 compares the PoPI Act first to other African countries, whilst Table 3 compares it to other well established non-African countries. Each country's Act will first be compared to the principles set out by the PoPI Act, before comparing it to the following criteria (selected based on a number of online resources found comparing data protection laws):

- Data Protection Officer (DPO) required;
- Breach notification;
- International data transfer permitted under certain conditions (country specific);

- Electronic marketing prohibited;
- Online privacy addressed;
- Enacted date.

The next sections present a high-level comparison of selected data protection laws.

4. Comparison to African Countries

The prevalence of data protection laws in Africa is increasing, probably as a result of many organisations in Africa doing business globally. As a result of Africa's fast mobile technology adoption and increase in technological exposure and engagement (ENECA, 2014), personal information is often transferred across the borders of various African countries and also from African countries to other international regions. As such, organisations doing business across multiple regions should be familiar with privacy laws applicable in the various African countries and whether they have adequate protection levels.

The laws in different countries vary and both criminal and civil sanctions may apply for violations. When doing business with these countries one must take into account the laws and relevant territories to consider its risks and costs (Michalsons, 2015). Up to date, 16 African countries have adopted data protection legislation, five have instantiated data protection bills and nine are rumoured to instantiate such a bill (Fichet, 2015). Since June 2014 when the African Union (AU) adopted a Convention on Cybersecurity and Personal Data Protection, more African countries have made some progress in terms of data protection legislation (Ncube, 2016). As with South Africa, in several African countries, the process has been initiated but not fully completed. The remainder of this section will present some common elements found among those countries.

Table 2 presents a comparison of the PoPI Act to data protection laws in Africa. The countries listed are African countries that have a specific data protection law in place, refer to Figure 2. Some countries such as Egypt, Nigeria and Zimbabwe, cater for privacy in other laws and do not have a specific data protection law in place (Craig, Mcormack, Halpert, Lucente, & Cheuk, 2012); these countries will not be included in the comparison.

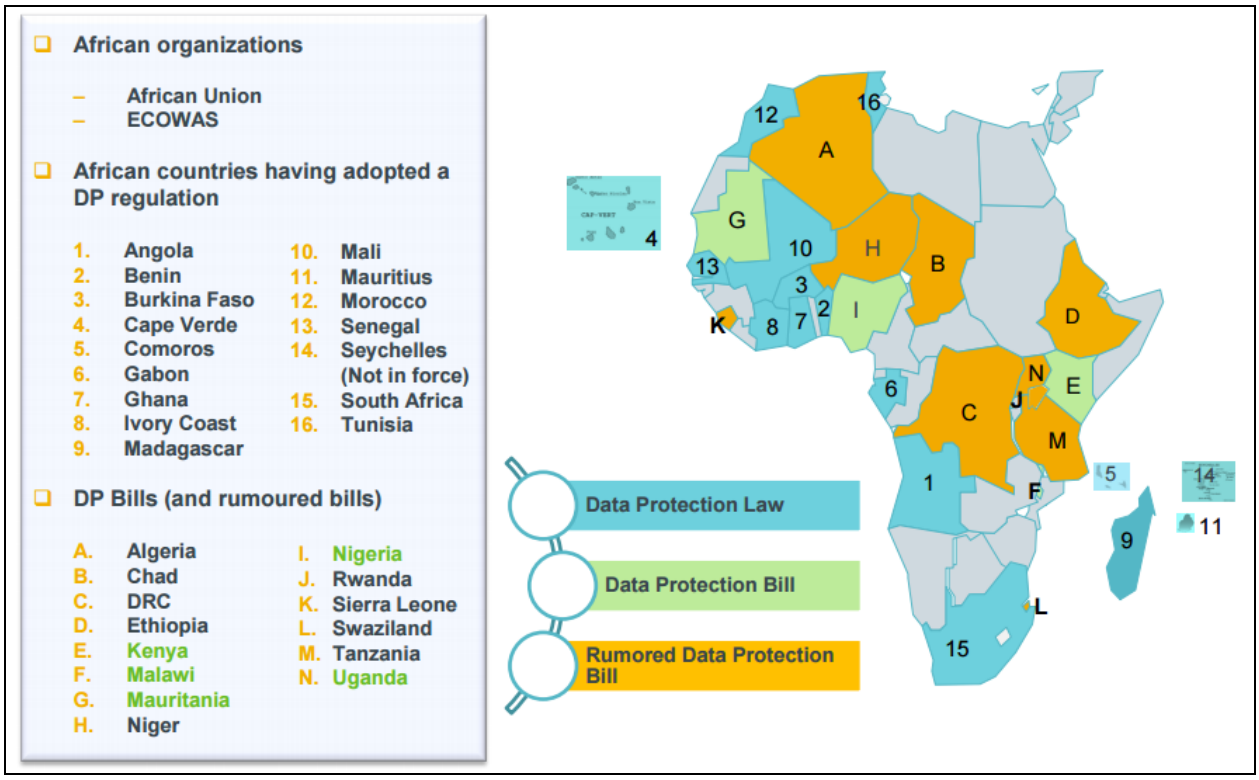

Figure 2. Data Protection Laws in Africa (Fichet, 2015)

4.1 PoPI Principles

The PoPI Act principles are in line with most of the African data protection laws, according to the results in Table 2. In most of the African countries, the data protection laws are referred to as the Protection of Personal Data (PPD) Act, or some variation thereof. Angola refers to the Personal Data Law (PDL), whereas Ghana refers to the Data Protection Act (DPA). In Morocco, the law is called the Protection of Individuals in Relation to the Processing of Personal Data (PIRPPD). Not enough information could be found on the Comorian data protection law and will therefore not be included in the comparison. Based on the results of Table 2, all of the laws have processing limitations, purpose specification and information quality in common. All of the laws require organisations to retain the personal information for the time required to achieve the purpose of the processing. However, in most cases, the specific time periods are not defined in these laws. In addition, South Africa is the only country that states accountability as one of the principles (Rich, 2014). Although other African countries might not have accountability as a principle, they might make provision for this in the context of the legislation. In every jurisdiction, there are security obligations that are enforced. There is also some sort of notice requirements for organisations to disclose the kind of personal information that is being collected, why it is collected, whether it is shared and for what time period. Moreover, organisations are required to prove that the securing of data integrity is being respected (Rich, 2014). All laws state that the data subject has rights (access, rectification and opposition) and should be fully informed of the data processing related to him/her (Fichet, 2015). These common elements enforce the applicability of data privacy regulation within the African countries.

Table 2. The PoPI Act Compared to Selected African Privacy Laws

Country	Act	PoPI Principles								Other Areas					
		Accountability	Processing Limitation	Purpose Specification	Further Processing Limitation	Information Quality	Openness	Security Safeguards	Data Subject Participation	DPO Required	Breach Notification	Cross-border Data Transfer Limitations	Electronic Marketing	Online Privacy	Enacted Year
South Africa	PoPI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		2013
Angola	PDL		✓	✓		✓		✓	✓			✓		✓	2011
Benin	PPD		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		2009
Burkina Faso	PPD		✓	✓		✓		✓	✓			✓			2004
Cape Verde	PPD		✓	✓		✓		✓	✓			✓	✓	✓	2013
Gabon	PPD		✓	✓		✓		✓	✓			✓			2011
Ghana	DPA		✓	✓	✓	✓	✓	✓	✓		✓				2012
Ivory Coast	PPD		✓	✓		✓		✓	✓	✓		✓			2013
Madagascar	PPD		✓	✓		✓		✓	✓	✓		✓			2015
Mali	PPD		✓	✓		✓		✓	✓			✓			2013
Mauritius	DPA		✓	✓	✓	✓	✓	✓	✓			✓			2004
Morocco	PIRPPD		✓	✓		✓		✓	✓			✓	✓		2009
Senegal	PPD		✓	✓		✓		✓	✓			✓			2008
Seychelles	DPA		✓	✓	✓	✓	✓	✓	✓			✓			2003
Tunisia	DPA		✓	✓	✓	✓	✓	✓	✓	✓		✓			2004

(Craig et al., 2012; Fichet, 2015; Rich, 2014)

4.2 Breach Notification

South Africa is the second African country to adopt the breach notification requirement, after Ghana (Rich, 2014). When it comes to notice obligation, all the laws in Africa are uniform in requiring the organisation to disclose the type of personal information being collected, the reason for that and with whom it is shared. Consent is still not uniform though. In Benin, only sensitive personal information requires consent (Rich, 2014); while the PoPI Act dictates consent for any personal data. None of the other African data protection laws requires notification of breaches (Craig et al., 2012).

4.3 DPO Required

In all legal systems, the challenge is to make a new law enforceable once it is promulgated. Having clear governance steps and punishment mechanisms in place is the common approach to this challenge, although the majority of African countries have not yet appointed a regulator. South Africa recently appointed a privacy regulator in May 2016. In Madagascar, the role of a data privacy officer was incorporated in legislation and a special commission is to be established as the independent regulator (Craig et al., 2012). In Ivory Coast, the enforcement mission was given to an independent administrative body of telecommunications (Rich, 2014). Mauritius has one of the most active enforcement regimes in terms of volume of imposed administrative fines (Rich, 2014). No other African country has appointed a privacy regulator (or no information is available online).

4.4 Cross-Border Data Transfer

The PoPI Act prohibits offshore transfers of personal data, but provides a number of exceptions where the Act includes rules and regulations for international data sharing (Kirby, Meiring, & Burger-Smidt, N.D.). All African countries, with the exception of Ghana, impose restrictions on cross-border data transfer. In Angola, the transfer of personal information to countries that do not ensure an adequate level of protection requires, as a rule, the individual's unambiguous, explicit and written consent, and prior authorisation from the DPA. In Burkina Faso, consent is not necessary as long as the receiving country presents the same level of protection (Rich, 2014). In Cape Verde, Gabon, Madagascar and Mauritius, the individual's consent overrules the lack of adequate protection offered by the receiving country. In contrast, the DPA in Seychelles has the whole power to define if a transfer would violate the principles (Rich, 2014).

4.5 Electronic Marketing

PoPI provides data subjects with certain rights with respect to unsolicited electronic communications and also prohibits automated processing of personal information. Benin, Cape Verde and Morocco also provide rights to electronic marketing whereas there is no provision for this in the remainder of the African countries (Craig et al., 2012).

4.6 Online Privacy

In terms of online privacy, only Angola and Cape Verde made certain provision (Angola City Government, N.D.). It might be a concern that the PoPI Act does not contain any provision for online privacy (Craig et al., 2012).

4.7 Enacted Year

With regards to maturity, the PoPI Act is relatively new, enacted in 2013. Madagascar's PPD is the most recent, enacted in 2015. Some African countries have data protection laws in place for over ten years. Seychelles has the oldest legislation, enacted already in 2003, but has not yet been in operation (Craig et al., 2012). Age, however, does not necessarily equate to maturity or completeness.

As the digital economy grows in Africa, adequate regulation requirements are getting tougher. Many African countries have yet to incorporate data protection legislation; those countries that have adopted data protection laws are facing difficulties in terms of implementation. However, all 53 African states agreed on a legal framework for regulating ICT activities such as electronic transactions, enhancing cyber security, control cybercrime and protecting personal data. This is a major step forward for Africa in terms of data protection (Fichet, 2015).

5. Comparison to Selected International Non-African Countries

This section compares the PoPI Act to selected non-African countries. The countries were selected based on their global influence and the maturity of their regimes. The purpose of comparing the PoPI Act to these countries is to assist in the identification of growth opportunities in data protection for South Africa, in terms of benchmarking against global influential countries.

The EU regulation has a great influence on data protection laws in Africa (Fichet, 2015). Since the EU DPD has been revised and unified into the GDPR (only to be enforced in 2018 (Ashford, 2016)), both these laws are included into the comparison in Table 3. The GDPR includes child privacy protections that are similar to the US Children's Online Privacy Protection Act (COPPA). The UK data protection law, the DPA, are in line with the EU DPD. The exception is the DPA's stronger legal protection for more sensitive information, including ethnic background, political opinions, religious beliefs, health, sexual health and criminal records (United Kingdom Government Gazette, 1998).

Canada has two federal laws. The Privacy Act (PA) covers the personal information-handling practises of federal government departments and agencies, whilst the Personal Information Protection and Electronic Documents Act (PIPEDA) cater for the private sector only (Privacy Commissioner of Canada, 2014). Data protection in Australia is currently a mix of Federal and State/Territory legislation (Craig et al., 2012). Australian States and territories (except for Western Australia and South Australia) each have their own data protection legislation applying to State Government agencies.

The US is the exception in this regard as it does not have a specific data protection law in place. It has roughly 20 sector specific or medium specific national privacy or data security laws, and hundreds of state-specific laws. California, for example, has more than 25 state privacy and data security laws (Craig et al., 2012). Due to its global influence, the US will be added to the comparison despite not having a specific data protection law.

Table 3 presents the high-level comparison between the PoPI Act and selected non-African countries. The remainder of the section details the compared legislation in support of the PoPI discussion in Section 3. This section will therefore not compare the PoPI Act with all categories for the second time.

Table 3. The PoPI Act Compared to Privacy Laws in Leading Countries

Country	Act	PoPI Principles								Other Areas					
		Accountability	Processing Limitation	Purpose Specification	Further Processing Limitation	Information Quality	Openness	Security Safeguards	Data Subject Participation	DPO Required	Breach Notification	Cross-border Data Transfer Limitations	Electronic Marketing	Online Privacy	Enacted Year
South Africa	PoPI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		2013
Australia	PA		✓	✓		✓	✓	✓	✓	✓		✓			1988
Canada	PA / PIPEDA	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2000
Europe	EU DPD		✓	✓	✓	✓	✓	✓	✓	✓		✓			1995
Europe	GDPR	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	2016
UK	DPA		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	2000
USA	*		✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	*

(Bird & Bird, 2016; Botha, Eloff, & Swart, 2015; Craig et al., 2012; Australian Government, 2014; United Kingdom Government Gazette, 1998)

* The United States does not have a specific data protection legislation, but has enacted a number of privacy laws since 2001 (Information Shield, N.D.). As such this row will not be populated based on a single act.

5.1 PoPI Principles

Based on the results in Table 3, the PoPI Act is largely in line with data protection legislation from selected international countries. The PoPI Act, PIPEDA and the GDPR are the only data protection laws that make provision for accountability as a principle. All of the laws compared require a DPO. The UK does not specifically state data subject participation as a principle, but it does state that information should be handled according to people's data protection rights (United Kingdom Government Gazette, 1998). The PIPEDA allows individuals to challenge an organisation's compliance on any of its privacy principles. Although Table 3 shows an alignment between the GDPR and the PoPI Act, there is a concern that the PoPI Act might have to be amended (Michalsons, 2016). The GDPR also introduces new concepts such as 'the right to be forgotten' and data portability (Bird & Bird, 2016).

5.2 Breach Notification

The Australian PA does not currently cater for mandatory data breach notification, but this is likely to be incorporated soon (Park & Griffin, 2016). The EU DPD does not cater for breach notification; but the newly implemented GDPR introduce this concept (Bird & Bird, 2016). The UK is currently under no obligation with the DPA to notify authorities of a data breach (Hasan, 2016). In the US, security breach notifications have been enacted in a number of laws in most of the states.

5.3 Cross-Border Data Transfer

In Australia the cross-border transfer of data is permitted but the sending agency or organisation remains largely accountable for that personal information (Australian Government, N.D.). Cross-border data transfers are permitted by both the EU DPD and the GDPR on the basis of ad hoc clauses. The EU has identified a small number of countries with adequate protection for personal information. Although the US is not included in this list, US businesses meeting the 'adequate' standard for privacy protection can certify with the US-EU Safe Harbor program (Packal & Haggerty, 2014).

5.4 Electronic Marketing

Electronic marketing is governed by the Canadian PA and PIPEDA, as well as Canada's Anti-Spam Legislation (CASL). The EU DPD does not specifically address electronic marketing. The GDPR forces the consent terms to be defined more clearly when collecting and processing personal information for the purpose of electronic marketing (Smart Insights, N.D.). The UK DPA does not prohibit the use of personal information for electronic marketing purposes. The US has extensive regulations on electronic marketing (Craig et al., 2012).

5.5 Online Privacy

In Australia there is no law specifically relating to online privacy. The Canadian regulatory authorities have been very active in addressing online privacy. No information could be found that the EU DPD specifically caters for online privacy. However, some European countries do cater for this in a certain way in different laws. Similarly in the UK, the DPA does not cater for online privacy but it is catered for in other UK regulations (Craig et al., 2012). The GDPR does make provision for online privacy in a number of ways such as the e-Privacy Directive (Beaumont, 2016). In the US, online privacy is catered for in a number of laws as well as online privacy for children with COPPA (Jay, 2015).

5.6 Enacted Year

The Australian PA 1988 was amended in 2012 and came in to force in 2014. The Canadian PA has evolved, since the first instance in 1977, to include data privacy in 2000 and has also been amended in 2015. The PIPEDA received approval in April 2000 (Privacy Commissioner of Canada, 2014). Based on the countries in Table 3, the GDPR is the youngest Act, adopted in 2016 and will supersede the EU DPD in 2018 (Bird & Bird, 2016). The UK DPA has been updated since 2000 and all changes will be in force from 20 October 2016 (United Kingdom Government Gazette, 1998).

Based on the literature review, provisions are made for most or all of the criteria measured on in Table 3. Data protection can no longer afford to be ignored as it is becoming a major issue for legislators, regulators and

consumers worldwide. Using this comparison as benchmark, South Africa can be regarded as on par with international privacy laws.

6. Conclusion

The amounts of personal data stored by individuals and organisations have grown significantly. This can result in potential high data breach risks and other unlawful activities. In an attempt to provide protection to citizens, a significant number of data protection laws have been enacted internationally. With these laws in place, it can be regarded as a right for individuals to have their personal information protected against unlawful collection, retention, dissemination and use. The world's privacy landscape has evolved as a result.

The privacy landscape in Africa has also evolved, with South Africa adopting the PoPI Act in 2013. Based on the comparisons presented in Table 2 and Table 3, the PoPI Act's principles are on par with selected African and non-African data protection laws. South Africa seems to be one of only four African countries that appointed a privacy officer/regulator. In this regard, the PoPI Act is ahead of other African countries without a DPO. Compared to other countries outside of Africa, though, appointing a privacy officer/regulator is the norm. In Africa, only three countries mandates data breach notification, including South Africa. Australia and the UK do not cater for data breach notifications. Europe did not include this in the EU DPD but did make provision for this in the GDPR. Most countries agree that the cross-border transfer is prohibited if the destination country has no adequate protection in place. This fact gives sustainability to the conclusion that having regulation in place, as South Africa is aiming to do, facilitates international commerce. Rights against electronic marketing are implemented in the PoPI Act and only three other African countries. Comparing this to the selected non-African countries, only Australia and the EU DPD does not make provision for electronic marketing. The GDPR does cater for this. Online privacy is only included in the laws of Angola and Cape Verde in the African countries. All the non-African countries considered, include online privacy legislation.

According to the comparisons done in this paper, the PoPI Act compares relatively well with other countries more mature in terms of data privacy legislation. This comparison is valuable in terms of reflecting a true need of international work on future harmonisation of laws.

References

Angola City Government. (N.D.). City of Angola - Privacy Policy. Retrieved from http://www.angolain.org/privacy/ [Accessed Oct/4, 2016]

Ashford, W. (2016). EU data protection rules affect everyone, say legal experts. Retrieved from http://www.computerweekly.com/news/4500270456/EU-data-protection-rules-affect-everyone-say-legal-experts [Accessed Aug/27, 2016]

Australian Government (2014). Privacy fact sheet 17: Australian privacy principles. Retrieved from https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-17-australian-privacy-principles_2.pdf [Accessed Oct/7, 2016]

Australian Government. (N.D.). Cross-border data flows. Retrieved from http://www.alrc.gov.au/publications/31.%20Cross-border%20Data%20Flows%20/summary-%E2%80%98cross-border-data-flows%E2%80%99-principle [Accessed Oct/7, 2016]

Banisar, D. (2016). National comprehensive data protection/privacy laws and bills 2016 Map. *Privacy Laws and Bills.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 [Accessed Oct/6 2016]

Beaumont, R. (2016). The GDPR, cookie consent and customer centric. Retrieved from https://www.cookielaw.org/blog/2016/5/13/the-gdpr,-cookie-consent-and-customer-centric-privacy/ [Accessed Oct/7, 2016]

Bird & Bird. (2016). Guide to the general data protection regulation. Retrieved from http://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en [Accessed Oct/6, 2016]

Birnhack, M. D. (2008). The EU data protection directive: An engine of a global regime. *Computer Law & Security Review, 24*(6), 508-520.

Botha, J., Eloff, M., & Swart, I. (2015). Evaluation of online resources on the implementation of the protection of personal information act in South Africa. Paper presented at the *ICCWS 2015-the Proceedings of the 10th International Conference on Cyber Warfare and Security,* South Africa. 39.

Business Media Live. (2015). SA ranks world's third highest cybercrime victims. Retrieved from http://www.businessmedialive.co.za/sa-ranks-worlds-third-highest-cybercrime-victims-2/ [Accessed Aug/5, 2016]

Craig, C., Mcormack, P., Halpert, J., Lucente, K. & Cheuk, A. (2012). DLA Piper's data protection laws of the world. Retrieved from http://www.edrm.net/resources/data-privacy-protection/data-protection-laws [Accessed Jun/28, 2016]

DataGuidance. (2013). South Africa: New privacy law will have 'significant impact 'on businesses. Retrieved from http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2104 [Accessed November/28, 2014]

ENECA. (2014). Tackling the challenges of cybersecurity in Africa. Retrieved from http://www.uneca.org/publications/tackling-challenges-cybersecurity-africa [Accessed Sep/15, 2016]

Fichet, C. (2015). Emerging data protection regulations in Africa. Retrieved from http://www.elexica.com/~/media/Files/Training/2015/05%20May/Emerging%20data%20protection%20regulations%20in%20Africa.pdf [Accessed Aug/12, 2016]

Gunning, E. (2016). How to prepare for POPI. Retrieved from https://www.ensafrica.com/news/how-to-prepare-for-POPI?Id=2285&STitle=ENSight [Accessed Sep/27, 2016]

Hasan, I. (2016). New rules for data protection. Retrieved from http://www.lawgazette.co.uk/law/legal-updates/new-rules-for-data-protection/5054463.fullarticle [Accessed Oct/6, 2016]

Heyink, M. (2015). Why are South African lawyers remaining in the dark with POPI? Retrieved from http://www.derebus.org.za/why-are-south-african-lawyers-remaining-in-the-dark-with-popi/ [Accessed Sep/15, 2016]

Information Shield. (N.D.). International privacy laws. Retrieved from http://www.informationshield.com/intprivacylaws.html [Accessed July/7, 2014]

Jay, R. P. (2015). Data protection & privacy. Retrieved from https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf [Accessed Oct/7, 2016]

Kirby, N., Meiring, I. & Burger-Smidt, A. (N.D.). Protection of personal information. Retrieved from http://www.werksmans.com/keep-informed/current-legal-developments/protection-of-personal-information/ [Accessed Sep/22, 2016]

Kokutse, F. (2011). African nations moving slowly forward to establish data protection framework. (Electronic Commerce & Law Report). Bloomberg BNA. Retrieved from http://www.bna.com [Accessed Oct/6]

Lamprecht, I. (2013). Few organisations ready for PoPI. Retrieved from http://www.moneyweb.co.za/archive/few-organisations-ready-for-popi/ [Accessed Jun, 2016]

Luck, R. (2014). POPI – is South Africa keeping up with international trends? Retrieved from http://www.saflii.org/za/journals/DEREBUS/2014/84.html [Accessed Sep/15, 2016]

Michalsons. (2015). Data protection laws of Africa. Retrieved from http://www.michalsons.co.za/focus-areas/privacy-and-data-protection/data-protection-laws-africa [Accessed Aug/08, 2016]

Michalsons. (2014). Protection of personal information act – POPI. Retrieved from http://www.michalsons.co.za/protection-of-personal-information-act-popi/11105 [Accessed April/1, 2014]

Michalsons. (2016). What does the GDPR mean for the PoPI Act. Retrieved from https://www.michalsons.com/blog/gdpr-mean-popi-act/19959 [Accessed Oct/17, 2016]

Ncube, B. C. (2016). Recent developments in African regulation of cybercrime: An overview of proposed changes to the South African framework.

Packal, E. A., & Haggerty, P. H. (2014). Cross-border transfers: Cutting through the complexity. Retrieved from https://www.dataprivacymonitor.com/cybersecurity/cross-border-data-transfers-cutting-through-the-complexity/ [Accessed Oct/7, 2016]

Park, M., & Griffin, J. (2016). Australian mandatory data breach notification on the agenda again. Retrieved from http://www.dataprotectionreport.com/2016/09/australian-mandatory-data-breach-notification-on-the-agenda-again/ [Accessed 6/Oct, 2016]

Pillay, L. (2016). US safe harbor and PoPI. Retrieved from http://www.lexology.com/library/detail.aspx?g=2a10bacb-15df-4803-a7bf-debbff1e5e30 [Accessed Aug/23, 2016]

PLI. (2016). Cloud computing 2016: Key issues and practical guidance. PLI New York Center, New York. (800) 260-4754.

Privacy Commissioner of Canada. (2014). Privacy legislation in Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/ [Accessed Jun, 2016]

Rich, C. (2014). Privacy and security law report. (Law Report No. 13 PVLR 717). The Bureau of National Affairs Inc. (800-372-1033). Bloomberg BNA. Retrieved from http://www.bna.com [Accessed Oct/6]

Smart Insights. (N.D.). What does general data protection regulation actually mean for marketers? Retrieved from http://www.smartinsights.com/marketplace-analysis/digital-marketing-laws/what-general-data-protection-regulation-actually-means/ [Accessed Oct/7, 2016]

South African Government Gazette (2013). Protection of Personal Information Act. Retrieved from www.justice.gov.za/legislation/acts/2013-004.pdf. [Accessed Oct/7, 2016]

Svantesson, D. J. B. (2014). Extraterritoriality of EU Data Privacy Law-Its Theoretical Justification and Its Practical Effect on US Businesses, the. *Stanford Journal of International Law, 50*, 53.

The Privacy Advisor. (2008) An introduction to privacy enhancing technologies. Retrieved from https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/ [Accessed Aug/12, 2016]

United Kingdom Government Gazette (1998). Data Protection Act, Act. Retrieved from http://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed Oct/7, 2016]