A COMPARISON OF COMPLIANCE WITH DATA PRIVACY REQUIREMENTS IN TWO COUNTRIES

A case study in South Africa and the United Kingdom

Adéle da Veiga, University of South Africa, SA, dveiga@unisa.ac.za

Ruthea Vorster, University of South Africa, SA, rvorster@unisa.ac.za

Fudong Li, University of Portsmouth, UK, fudong.li@port.ac.uk

Nathan Clarke, University of Plymouth, UK, N.Clarke@plymouth.ac.uk

Steven Furnell, University of Plymouth, UK, S.Furnell@plymouth.ac.uk

Abstract

In the United Kingdom (UK), the Data Protection Act (DPA) has been in force since 1998, whereas South African (SA) organisations are preparing for compliance with the Protection of Personal Information Act (POPIA). The objective of this research is to compare aspects of data protection compliance between the UK and SA to establish if a country that has had data protection in place for a longer period of time has a higher level of compliance with data protection requirements in an online context compared to a country that is preparing for compliance, using the results to make recommendations for non-compliance aspects. To fulfil the research objective, an insurance industry multi-case study was conducted. Similar data privacy requirements from the DPA and POPIA were selected for the multi-case study and as such, consent for direct marketing, secure processing of personal information (PI), privacy policies and sharing of PI collected via websites were evaluated. For each country, PI of four created consumer profiles was deposited to 10 insurance company websites in each country to evaluate the requirements. The results showed that some of the websites did not honor the selected opt-out preferences as direct marketing material was sent to the SA and UK consumer profiles. Forty two unsolicited third party contacts were received by the SA consumer profiles indicating unconsented distribution of PI in SA. In comparison, no unsolicited contacts were received by any of the UK profiles. The results demonstrate that the UK, being regarded as a jurisdiction with a heavy stance towards privacy implementation and regulation, is more compliant than SA in terms of implementation of the evaluated data protection requirements included in the scope of this study. SA insurance organisations should ensure that the non-compliance aspects are addressed and can learn from the manner in which the UK insurance organisations implement the privacy requirements. Furthermore, the UK insurance organisations should focus on improved compliance for direct marking to aid with compliance to the DPA and upcoming General Data Protection Act.

Keywords: POPIA, Protection of Personal Information Act, privacy, DPA, Data Protection Act, GDPR, General Data Protection Regulation, personal information, consumer, direct marketing, opt-in, opt-out, compliance, legal.

1 Introduction

Personal data or information is regarded as the new oil in the digital world – a strategic asset, and even a product in itself (*The Economist*, 2017; Sarkhel and Alawadhi, 2017). Since there is an enormous amount of personal data collected in cyberspace, organisations are able to gain a competitive advantage through targeted marketing, product customisation (Spiekerman et al., 2015) and the use of value chains (European Commission DG Connect, 2013) to deliver tailored services and products to consumers. However, the processing and use of personal data must be conducted with due regard for the requirements of data protection regulations.

There are over 100 countries with enacted data protection regulations (Greenleaf, 2013). Although these regulations focus on the protection of personal data, the definitions of privacy as well as the conditions for processing and protection vary (Spiekerman et al., 2015). Furthermore, the regulations are enforced more robustly in some jurisdictions, and more moderately in others (DLA Piper, 2018).

The research study reported on in this paper focuses on the data protection jurisdictions of South Africa (SA) and United Kingdom (UK). The South African Protection of Personal Information Act (POPIA) (South Africa, 2013) was signed into law in 2013, and South Africa is regarded as a country in which regulation and enforcement are moderately applied (DLA Piper, 2018). The UK Data Protection Act (DPA) (Great Britain, 1998) has been in effect since 2000, and in the UK regulation and enforcement are considered to be robustly applied (DLA Piper, 2018). The Information Commissioner's Office (ICO) in the UK has issued various fines to organisations found to have sold personal information (PI) for marketing purposes, and to have sent unsolicited text messages or emails. In recent cases the ICO fined Home Logic UK Ltd (ICO, 2017a) £50,000 for making marketing calls and Moneysupermarket.com (ICO, 2017b) £80,000 for sending marketing emails which recipients did not consent to. The maturity and classification of the two approaches differ sufficiently to merit a comparison of practice.

Informed consent is a principle covered by both POPIA and the DPA. Many argue that informed consent is obtained through the opt-out model, in terms of which the user must actively decline or refuse permission for certain processing or use of their PI if they do not want it used in this way. In comparison, the user gives informed consent for certain processing or use of their information within the opt-in model; this is regarded as requiring less effort on the part of the user, and is considered better than the opt-out model in terms of advantage to the user (Noain-Sánchez, 2016). This is made possible using active data collection, whereby an individual knowingly and willingly provides PI on a website (Swire and Berman, 2007). Informed consent also applies when PI is collected online and where organisations plan to use the PI for direct marketing purposes.

For the purpose of this research, informed consent was investigated in the context of obtaining consent for marketing preferences at the time of obtaining online insurance quotes. A case study was conducted in both SA and the UK in which consent for direct marketing, the secure processing of PI, the use of privacy policies on websites and third party sharing of PI in the two countries were compared from a regulatory and compliance perspective in order to make recommendations for improved compliance.

2 Research Objectives

The objective of the research is to compare aspects of data protection compliance between SA and the UK to establish if a country that has had data protection in place for a longer period of time had a higher level of compliance with data protection requirements compared to a country that is preparing for compliance. The results can be used to make recommendations for non-compliance aspects to aid organisations by learning from good practice towards the implementation and regulation of privacy.

The data protection requirements in POPIA and the DPA are similar (Botha et al., 2017; Da Veiga, 2017) and both pieces of legislation incorporate the privacy principles of the Guidelines on the Protection of Personal Information and Trans-border Flow of Personal Data (OECD, 2013) as well as the Fair Information Practice Principles (FIPPS, 2018). As such data privacy implementation in these two countries can be compared. Similar data protection requirements from POPIA and the DPA that could be tested when PI is deposited via a website were selected for the comparison. Consideration was also given

to requirements that can be evaluated from a consumer perspective as to whether the consumer will experience that his/her privacy rights, as outlined in the respective regulations, were upheld. As such the following aspects were included for the evaluation: the openness principle whereby consumers must be notified of the purposes and other conditions of processing (typically through an online privacy policy), the secure processing of PI (using Hyper Text Transport Protocol Secure (HTTPS)), the consent for direct marketing (through opt-in for receiving or opting-out to decline) and consent for third party sharing of PI (thereby not receiving unwanted communication from third parties).

It is recognised that privacy perceptions differ between consumers (Morton and Sasse, 2014; Kumaraguru and Cranor, 2015). Moreover, cultural aspects also play a role in privacy perception (Greenleaf, 2013; Bygrave, 2010) and even national culture (Hoffstede, 2010). While the aforementioned also play a role in privacy implementation in a country the requirements of the DPA and POPIA were used from a regulatory perspective as the theoretical basis to evaluate the implementation of the privacy requirements in this study. The scope of this research is therefore limited to organisations, being the responsible party, who must implement certain privacy requirements in line with the DPA and POPIA requirements and consumers on the other hand who should through their interaction with the organisation experience that their privacy rights are maintained in line with the regulatory requirements.

3 Overview of POPIA and the DPA

POPIA and the DPA are both based on the OECD privacy principles (Organisation for Economic Co-Operation and Development, 2013), namely accountability, processing or use limitation, collection limitation, purpose specification, information quality, openness, security safeguards, and data subject participation or access. Both pieces of legislation further include the concept of sensitive PI and cross-border data transfer limitations. POPIA covers breach notification, whereas the DPA does not include it, but the Privacy and Electronic Communications Regulations of 2003 require that organisations notify the ICO in the event of a data breach of personal data (DLA Piper, 2018). Table 1 illustrates the conditions of POPIA that maps to the principles of the DPA (Botha et al., 2017; Da Veiga, 2017). The General Data Protection Regulation (GDPR) mapping is also considered as organisations in the UK will in future also have to comply with its requirements. Table 1 includes a mapping to the OECD privacy principles and FIPPS, indicating that similar privacy principles are covered by both acts allowing for the comparison. The last column indicates which of the principles were selected for inclusion in scope of this study.

Privacy Condition/Principle	FIPPs	OECD	POPIA SA	DPA UK	GDPR	Included in Scope
Accountability	Y	Y	Y	N	Y	N
Processing/use limitation	Y	Y	Y	Y	Y	N
Collection limitation	Y	Y	Y	Y	Y	N
Purpose specification	Y	Y	Y	Y	Y	N
Further processing limitation	N	N	Y	Y	Y	N
Information quality	Y	Y	Y	Y	Y	N
Openness	Y	Y	Y	Y	Y	Y
Security safeguards and third parties	Y	Y	Y	Y	Y	Y
Data subject participation / access	Y	Y	Y	Y	Y	N
DPO/ IO required	N	N	Y	Y	Y	N
Breach notification	N	N	Y	N	Y	N
Cross-border data transfer limitations	N	N	Y	Y	Y	N
Direct marketing	N	N	Y	Y	Y	Y
Online privacy	N	N	N	N	Y	Y
Sensitive PI	N	N	Y	Y	Y	Y

Table 1. Mapping of standards/act requirements to privacy compliance evaluation

The next section provides an overview of the two regulations.

3.1 Overview of POPIA

The PI of SA citizens is protected by the South African Constitution in terms of the common law and the right to privacy as a fundamental human right (South Africa, 1996). POPIA (South Africa, 2013) regulates the processing of PI by public and private organisations domiciled in SA. It defines PI as "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person" (South Africa 2013, p. 14), being the data subject. This includes information such as a person's name, race, language, sex, pregnancy, marital status, and national, ethnic or social origin; information relating to a person's educational level or medical or financial status; the biometric information of a person; the personal opinions or preferences of a person; and even correspondence.

POPIA refers to the organisation that defines the purpose and means of processing of the PI as the "responsible party". There are eight conditions for the processing of PI namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, data subject participation. Processing of special PI, rights regarding direct marketing and transborder information flows are addressed as separate chapters in the law. Two conditions are relevant for this research project namely, condition 6 relating to openness, condition 7 relating to security safeguards and the chapter regarding direct marketing requirements. Provisions are also included for the establishment of an Information Regulator. Only the sections relating to the Information Regulator have been enforced to date. The Information Regulator chairperson and members were appointed in December 2016 and have subsequently established the Information Regulator website (Information Regulator South Africa, 2018).

3.2 Overview of the DPA

In the UK, personal data that is stored on computers or in an organised paper filing system is regulated by the Data Protection Act of 1998 (Great Britain, 1998). The DPA regulates the processing and movement of personal data for all purposes other than domestic use. Section 1.1 of the DPA defines personal data as "data which relate to a living individual who can be identified (a) from those data or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller." According to the ICO guidelines entitled "Determining what is personal data", examples of personal data include a person's name, place of work, medical history, and telephone number (ICO, 2012).

The DPA defines how personal data are (or are to be) processed by the data controller. The data controller needs to follow eight principles to ensure that personal data are processed lawfully. Those eight principles are listed in Schedule 1 of the DPA and relate to fair and lawful processing, specific and lawful purposes, adequate and relevant to the purpose of processing, ensuring accuracy, not keeping PI for longer than necessary, processing in accordance with data subject rights, appropriate technical and organisational measures and transborder flow requirements. The rights of data subjects include the right to prevent processing for purposes of direct marketing. This right together with principles 2 and 7 are deemed relevant to this research study. Principle 2 relates to personal data that will not be further processed if the aim of the usage is incompatible with the original purpose of collecting the data, and principle 7 establishes appropriate technical measures to be taken against unauthorised processing of the personal data.

4 Overview of Specific Regulatory Requirements

With the aim to compare how organisations in SA and the UK meet the respective privacy requirements, a number of key requirements of POPIA and the DPA were selected, namely direct marketing, openness using online privacy policies, secure processing and third party sharing. Detailed overviews of these requirements are presented in the next section.

4.1 Overview of Direct Marketing Consent Requirements

POPIA defines direct marketing as communication whereby goods or services are offered to a data subject in person, by mail or via electronic communication (South Africa, 2013). Section 69 of POPIA deals with direct marketing using unsolicited electronic communications. A responsible party may contact a data subject only if consent has been obtained, or if the data subject is an existing consumer and communication relates to similar products or services. New consumers may be contacted only once, with consent (opt-in) being required for continued communication. Consent in POPIA refers to "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information" (South Africa, 2013, p. 12). In terms of POPIA, consent for direct marketing is given through consumers electing to opt in. Until POPIA is enacted, the Consumer Protection Act (CPA) of 2010 (South Africa, 2008) gives consumers the right to restrict unwanted direct marketing by opting out.

Similar to the definition given in POPIA, Section 11 of the DPA describes direct marketing as communications of any advertising or marketing material that are sent to a particular individual (Great Britain, 1998, s 11). In its document entitled "Direct Marketing," the ICO (2016) presents a number of direct marketing examples, such as a bank contacting a consumer regarding the administration of their bank account and at the same time also introducing its mortgage products. The same section regulates an individual's right to prevent their PI from being processed for the purposes of direct marketing. The Privacy and Electronic Communications (EC Directive) Regulations (Great Britain) 2003 provide more detailed privacy rules for an individual in relation to electronic communications (e.g. email), as these were designed to complement the DPA in respect of people's privacy rights (Great Britain, 2003). From the data controller's point of view, individuals can be contacted (e.g. via email, telephone or text message) only if they have consented to this (e.g. by means of opt-in or opt-out boxes) (ICO, 2016).

This requirement can be tested by evaluating if websites include an opt-in or opt-out option that consumers can select to indicate their preference in receiving direct marketing. The compliance of the organisation with the consumer preferences can be monitored through the direct marketing communication received on the personal email or cell phone numbers provided by a consumer.

4.2 Overview of Openness Using an Online Privacy Policy

Where PI is captured actively on websites, the website should include a link to a privacy policy or notice that is clear and easy to access (Swire and Berman 2007). This privacy policy should explain to the data subject what their PI will be used for and with whom it will be shared, and thus ensure that the data subject is aware of the purpose of information collection and other aspects to meet the requirements of the openness condition/principle.

POPIA requires the responsible party to notify the data subject about a number of aspects by means of a privacy policy or notice disclosing all the means by which the organisation collects, uses and discloses PI (South Africa, 2013, s 18). Principle 1 of DPA Schedule 1 states that "Personal data shall be processed fairly and lawfully". One of the ways to uphold this principle is to provide, in a privacy policy, additional information on how personal information is collected and processed, who the data controller is and the purpose for which the information will be processed (ICO, n.d.).

This requirement can be checked by establishing if websites have a privacy policy or includes privacy notices in their terms and conditions.

4.3 Overview of Secure Processing Requirements for Websites

Condition 7 of POPIA requires that a responsible party must secure the integrity and confidentiality of PI that it processes by applying technical and organisational measures to protect it (South Africa 2013, s 19(1)). As mentioned earlier, principle 7 of Schedule 1 of the DPA states that proper security controls should be used to protect PI from being misused. More specifically, the ICO document entitled "Protecting personal data online services" provides guidelines on various security mechanisms that can be used to protect PI online, including configuration of Secure Socket Layer, good password usage, and

software security updates (ICO, 2014). This will aid in preventing the loss, destruction, unauthorised access and processing of PI. In addition, it is also the responsibility of the responsible party to inform the data subject if a data breach occurs. For the purpose of this research, the use of HTTPS as one of the various security mechanisms was considered owing to the ease of identifying it for the case study.

This requirement can be verified by checking if an organisation's website uses HTTPS when a consumer deposits his/her PI on the websites, especially where sensitive PI is collected.

4.4 Overview of Third Party Requirements

Consent for direct marketing does not constitute consent to share or sell PI to third parties for direct marketing. Section 18 of POPIA requires a responsible party to take reasonable practical steps to notify the data subject of the recipient or categories of recipients of their PI. Furthermore, PI may be supplied to third parties only if this serves the legitimate interests of the responsible party or third party (South Africa 2013, s 11(f)). It is important to note that the purpose of collecting the PI must be explicitly stated, and must be lawful (South Africa 2013, s 13(1)). Any sharing of PI with a third party should be communicated to the data subject and must be in line with the original purpose of collection. Where PI is shared with a third party for legitimate reasons there must be a written contract in place between the responsible party and the third party outlining the security requirements to ensure that the integrity and confidentiality of the PI is secured (South Africa 2013, s 20 and s 21). It is the responsibility of the responsible party to ensure that a contract is in place stipulating the security measures and to ensure that the security measures are maintained (South Africa 2013, s 21).

The openness condition of POPIA stipulates that, "If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—…(h) any further information such as the – (i) recipient or category of recipients of the information" (South Africa 2013, s 18. (h)(i)). A responsible party may not transfer PI to a third party in a foreign country unless certain provisions are in place, such as a binding code of conduct or contract, or unless the data subject consents to this (South Africa 2013, s 69).

Section 70(1) of the DPA defines a third party as any person other than "a) the data subject, b) the data controller or c) any data processor or other person authorised to process data for the data controller or processor". In terms of data sharing, Schedule 3 Section 4 of the DPA states that disclosure of sensitive personal data to third parties can be processed only if the consent of the individual is given. As a result, many data collectors use a privacy notice to explain to individuals how their personal data will be processed (e.g. the sharing of their data with third parties if required) during the data collection phase (Audiencedatasharing, n.d.) and the individuals can then decide whether to give permission to the data collector to allow third parties to use their personal data.

This requirement can be evaluated by establishing if websites notify consumers or obtain consent for sharing the consumer's PI with third parties. In addition compliance can be verified through the communications which the consumer receives on his/her email or cell phone number as deposited on the website, which should not include third parties that are not related to the purpose of sharing the PI.

5 Research Methodology

A multi-case study methodology with multiple units of analysis was utilised to conduct this research study (Yin, 2003). The multi-case study methodology follows a replication logic through the selection of two countries, SA and UK. More than one unit of analysis are included in each country, namely ten short-term vehicle insurance companies in each country. The privacy compliance requirement tests, as defined at the beginning of the research study in section 4, are replicated across the organisations in each country. Ethical clearance for this research project was obtained through the relevant research ethics bodies at the University of South Africa (Unisa) and the University of Plymouth. Ethical clearance required data anonymisation and confidentiality of the companies included in the sample, and therefore no company names or distinguishing characteristics are disclosed in the research result discussion.

5.1 Case Study Overview

The insurance industry was selected for the research study due to several reasons. Firstly, the insurance industry processes large volumes of personal information (Norton Rose Fulbright, 2013) and are regarded as one of the industries that are affected by a large number of data breaches (PwC, 2015). Also, the insurance industry provides consumers with the service of obtaining online insurance quotes. During this process consumers deposit their PI online which enabled the researchers to conduct the case study to test the selected privacy requirements. The convenience sampling method was used to select the insurance companies (Etikan et al., 2016).

To facilitate the data depositing and data collection four new cellular phone SIM cards were linked to four newly created email addresses for each country, thus eight user profiles in total. In each country, two of the cellular numbers were used to opt in and the other two cellular numbers were used to opt out for direct marketing in order to monitor compliance with direct marketing preference (see Table 2).

Cell/email contacts	Option	Company sites
Cell1-email1	Opt in	Opted in for companies 1–10
Cell2-email2	Opt out	Opted out for companies 1–10
Cell3-email3	Opt in	Opted in for companies 1–10
Cell4-email4	Opt out	Opted out for companies 1–10

Table 2. Data depositing plan for the 10 companies in each country

The researchers requested online quotes for each cell number and corresponding email. Thus, in SA the four SA profiles were used to request quotes at each of the ten insurance companies with a total of forty online quotes. Similarly, forty online quotes were obtained in the UK. As such PI was deposited on the websites of the ten insurance companies included in the sample for each country. The PI requested on the websites, the use of HTTPS on the website and the availability of a privacy policy and/or disclaimer were noted during the depositing process. All cell phone calls, short messages (SMS) and emails received resulting from the request for an insurance quotation were recorded for a period of three months.

In addition to POPIA, the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA) (South Africa, 2003) also plays a role in the collection of PI in SA. RICA requires telecommunication companies to verify the identity of a consumer through their personal identification documentation and to retain copies thereof. For one of the SA profiles the cell phone provider requested the personal identification documentation, but the second cell phone provider did not adhere to these requirements for verification. The UK cell phone provider did not require any PI when the SIM cards were purchased.

6 Results

All cellular telephone calls received, SMS and emails received were recorded in a MS-Excel spreadsheet, noting the identity of the caller/contact, which company contacted the data subject, the nature of the contact, e.g. was it insurance related and if the data subject had opted in or opted out to receive any direct marketing communication from the insurance company. The evidence was quantified and analysed firstly per country and thereafter both countries results were compared and evaluated for differences and/or similarities.

6.1 Overview of PI Collected

There was variation in the PI requested of the data subjects by the insurance companies in the SA sample, whereas the PI requested by the UK insurance companies was more consistent, as set out in Table 3.

PI requested	Number of websites		PI requested	Number of websites	
	SA	UK		SA	UK
Name	9	10	Physical address	1	10
Surname	8	10	Marital status	3	10
ID	7	0	Vehicle registration number	1	10
Gender	0	9	Secure parking	3	9
Birth date	0	10	Driving with disability/medical condition	1	2
Cell phone	9	10	Driving record (judgment)	1	10
Email address	7	10	Vehicle details	5	10

Table 3. PI requested

In SA, a person's identity number can be utilised to deduce their birth date, age and gender (Western Cape Government, 2016), and this number was validated as part of the online request for authenticity. Where the email address was not requested by the SA websites, the cell number was requested and vice versa. One of the SA websites requested information about disability status. This is classified as "special personal" information by POPIA, as it falls under health information (South Africa 2013, s 26), which may not be processed unless consent is obtained, or certain other provisions apply. Of concern is that this website was also one of the websites that did not include an option for direct marketing preferences.

In comparison, the UK insurance companies requested a wider, but consistent range of PI. The UK does not have a national identity programme, and therefore none of the UK insurance companies asked for an identity number. The insurance premium paid by drivers is based on their physical address, which is why all companies requested this information. Two insurance companies requested information on whether the insurer had a medical condition that requires the Driver and Vehicle Licensing Agency (DVLA) to be notified.

6.2 Opt-in/opt-out Preferences for Direct Marketing

During the data depositing phase, the availability of an opt-in or opt-out option for direct marketing was recorded to establish and verify whether responsible parties honoured the data subject's choice during subsequent contacts. In the South African sample, only two organisations gave the data subject the choice of either opting in or opting out when it came to receiving direct marketing communication (see Table 4). In the case of two of the SA companies, the data subject could not proceed with the online insurance quotation request unless the opt-in option was selected (mandatory opt-in). In the SA context, six companies did not provide either an opt-in or an opt-out option. By contrast, eight of the UK companies provided an opt-in or opt-out option from which the data subject was free to choose. The remaining two UK companies set the opt-in by default, with the data subject being able to ask to change their status to opt-out via email or by completing an online opt-out form.

Options	SA (10 websites)	UK (10 websites)
Opt in/opt out preference available	2	8
Mandatory opt-in	2	2
Use of opt-out form	0	2
No option	6	0

Table 4. Opt-in/opt-out options: SA versus UK

6.3 Use of Privacy Policy

The availability (or absence) of a privacy policy or terms and conditions was noted during the data depositing process. Where 9 UK organisations had a privacy policy on their websites and 1 UK organisation had a privacy notice in terms and conditions on its website. In comparison, 5 SA organisations

had a privacy policy on their websites and also 5 organisations had a privacy notice in terms and conditions on their websites.

6.4 Security Processing on Websites Using HTTPS

All the organisations included in the UK sample used HTTPS on their websites to process PI for the purpose of the online quotation requests. However, the website of one SA organisation did not.

6.5 Sharing Of PI with Third Parties

None of the SA or UK websites had a third party sharing option or notification at the point of collection. Only one SA organisation had a notice indicating that information would not be shared; however, no option was available to the participant to opt out of third party sharing.

Table 5 sets out the number of contacts received for the opt-out and opt-in profiles in SA and the UK. Of concern is the number of contacts received from companies that were not part of the sample. In all, 42 contacts were received that were not part of the sample for two of the profiles in SA (20 in the opt-in and 22 in the opt-out group). This indicates that third parties that were not part of the sample contacted the data subjects for direct marketing. The contacts varied from competitions to win airtime, to offers of funeral cover, to product promotions. In comparison, the UK profiles only received contacts from the sampling insurance companies, regardless of whether they were opt-in or opt-out.

OPT-IN CONTACTS		**SA TOTAL**	**UK TOTAL**
Part of sample	SMS - quote follow-up	2	0
	Calls - quote follow-up	19	1
	Email - quote follow-up	15	8
	Email - promotional	3	12
	Total opt-in part of sample	***39***	***21***
Not part of sample	SMS	18	0
	Calls	0	0
	Email	0	0
	Email – promotional	2	0
	Total opt-in not part of sample	***20***	***0***
Total Opt-In Contacts		**59**	**21**
OPT-OUT CONTACTS		**SA TOTAL**	**UK TOTAL**
Part of sample	SMS - quote follow-up	4	0
	Calls - quote follow-up	16	0
	Email - quote follow-up	7	8
	Email - promotional	6	7
	Total opt-out part of sample	***33***	***15***
Not part of sample	SMS	21	0
	Calls	0	0
	Email	0	0
	Email - promotional	1	0
	Total opt-out not part of sample	***22***	***0***
Total Opt-Out Contacts		**55**	**15**

Table 5. Summary of contacts received

Regarding the opt-in and opt-out preferences, 59 and 55 contacts were received by the opt-in profile and opt-out profile respectively in SA, while 21 and 15 contacts were received by the UK opt-in profile and opt-out profile accordingly. The promotional emails received included retail advertisements as well as those relating to insurance. It is not clear whether these were received as a possible result of email profiling or whether they were related to sharing of the email addresses by the companies in the sample. The 13 promotional emails (six from SA profiles and seven from UK profiles) received as part of the opt-out profile were a concern, as the data subject elected not to receive direct marketing as part of this profile.

7 Discussions

Table 6 provides a summary of the aspects tested in the multi-case study with the results for SA and the UK, and the related observation and recommendations. In the SA context the opt-out preference and third party sharing are of concern – it would appear that companies do not yet comply with the POPIA requirements. In the UK, the case study data shows that the data collectors do not share PI with third party companies; nonetheless, individual preference for the opt-out option is not fully honoured, as those who chose the opt-out option were contacted seven times via email.

Requirement	SA	UK	Observation	Recommendation
Opt-in/opt-out available on website	2	8	The SA websites did not comply with this option, although the CPA requires an opt-out option for direct marketing. Most of the UK websites provided an opt-in/opt-out option.	Opt-in/out preferences for direct marketing should be provided on websites at the point of data collection.
Privacy policy on website or in terms and conditions	10	10	All SA and UK websites had a privacy policy or included privacy in their terms and conditions.	N/A
Secure website using HTTPS	9	10	One of the SA companies did not have a secure website, whereas all the UK companies did.	SA organisations should ensure secure processing of PI using for example HTTPS.
Third party sharing (Number of third party contacts received)	42	0	A number of contacts were received from companies that were not part of the SA sample. It is possible that the insurance companies or the telecommunication companies shared the data subject's PI without the data subject's knoweldge or consent. In comparison, the UK profiles did not receive anything that was not from the sampling insurance companies.	SA organisations should ensure that PI is processed lawfully and implement measures to ensure that it is not shared with unauthorised third parties e.g. policy updates, training and awareness to staff, further processing approval process.
Honouring of opt-out (Uncolicited promotional emails received)	6	7	A few promotional emails were received in the opt-out group of the SA and UK profiles. This might be related to the profiling of the email accounts.	Organisations should maintain opt-in and opt-out preferences of consumers and exclude consumers from direct marketig if they opted out.

Table 6. Synopsis of results: SA versus UK

The results of this research study indicate that in a country where there is enacted data privacy legislation with an active regulator, the companies in the sample were more compliant with data privacy conditions than those in a country with pending data privacy legislation. In the UK, the ICO has become more prominent in terms of issuing enforcement actions (which can include monetary penalties and prosecutions) in relation to breaches of the DPA. Indeed, 2017 saw an increase of over 100% in the

number of enforcements, and an almost 50% increase in the value of associated fines; the total value of fines has increased significantly over time, as shown in Table 7.

Year	Number of fines	Total value
2010	2	£160,000
2011	7	£541,100
2012	17	£2,143,000
2013	14	£1,520,000
2014	9	£668,500
2015	18	£2,031,250
2016	21	£2,155,500
2017 (Aug)	44	£3,107,500

Table 7. ICO fines 2010–2017 (Metzger, 2017)

In future, the introduction of new legislation will deliver even greater power to persuade and to prosecute non-compliance. To date, the ICO has issued fines of up to £500,000 for DPA contraventions, although in practice it has not issued any above £400,000. However, the permitted threshold will increase significantly with the introduction of the GDPR in May 2018 (Leyden, 2017). Specifically, the GDPR will permit penalties of up to €20 million or 4% of annual global turnover (whichever is higher). Thus, the incentive to comply, and the price of not doing so, will be even greater.

The research results indicate the insurance organisations in the UK sample were more compliant than their SA counterparts. This can be attributed to the longer time frame that the DPA has been in place, the active Regulator and trend of fines imposed. This supports to the work of the DLA Piper that categorises the UK as a country with a heavy stance towards privacy whereas SA is categorised as low (DLA Piper 2018). The SA insurance industry can leverage the results in this study to improve their opt-in/opt-out provisions on company websites and to further improve its processes of data sharing with third parties to ensure that it complies with the provisions of POPIA by obtaining consent for direct marketing and for third party sharing. The UK can focus on implementing measure to comply with provisions for unsolicited marketing in order to honour opt-in and opt-out preferences and to implement measure to obtain consent prior to sending direct marketing material.

8 Limitations

The sample was limited to 10 insurance companies in SA and the UK, which could be expanded to a larger sample for future research. Although the insurance industry is categorised under the financial sector, it would be advantageous to expand the research sample to other financial sector companies. The availability of a website policy or disclaimer was noted; however the analysis of website policy content fell outside the scope of this research. In the SA context, contacts received via the cell phone numbers could be the result of previous ownership of a cell phone number, as in this country cell phone numbers are reassigned.

9 Conclusion

The study sought to understand and compare the handling and processing of PI practices across two countries that differed in terms of privacy adoption/maturity. Interestingly, at the heart of both sets of legislation one finds a similar set of privacy requirements, themselves drawn from internationally accepted privacy principles. However, in terms of practice, while maturity will constitute a factor in adoption, enforcement of regulation appears to be key, with UK-based practice (with a few minor exceptions) adhering to legislative requirements. With SA still at an early stage of implementation, with no degree of enforcement, it is left up to companies to determine suitable policies with regard to PI while preparing for compliance, with some choosing to monetise rather than to protect the data as evident in the number

of contacts received from companies not included in the sample. This trend is not unique to SA, and can be identified as having occurred in many countries (including the UK) prior to full adoption and enforcement of appropriate legislation. Organisations in SA can leverage the results to identify gaps in compliance with POPIA while learning from UK organisations to define their compliance plans.

Acknowledgements

This research is supported by the Women in Research (WiR) Grant from the University of South Africa.

References

Audiencedatasharing (n.d.). "Data Protection What the Regulations Say", URL: https://www.audiencedatasharing.org/asset/26 (visited on: 09/11/2017).

Botha, J., Grobler, M. M., Hahn, J. and Eloff, M. (2017). "A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws," in *International Conference on Cyber Warfare and Security Conference Proceedings*, p. 57.

Bygrave, L. (2010). "Privacy and data protection in an international perspective," *Scand. Stud. Law*.

Da Veiga, A. (2017). "The influence of data protection regulation on the information security culture on an organisation – a case study comparing legislation and offices across jurisdictions", In Furnell, S. and Clarke N. (eds.), Proceedings of the *Eleventh International Symposium on Human Aspects of Information Security & Assurance* (HAISA 2017), Australia, Adelaide, pp. 65-79, ISBN: 978-1-84102-428-8.

DLA Piper (2018). *Data Protection Laws of the World, Full Handbook.* (April 2018), p. 1–513. URL: https://www.dlapiperdataprotection.com/index.html (visited on: 17/04/208).

Etikan, I., Musa, S.A. and Alkassim, R.S. (2016). "Comparison of Convenience Sampling and Purposive Sampling". *American Journal of Theoretical and Applied Statistics* 5(1), p. 1–4. URL: 10.11648/j.ajtas.20160501.11 (visited on: 10/15/2017).

European Commission DG Connect (2013). "A European strategy on the data value chain". URL: https://ec.europa.eu/digital-single-market/news/elements-data-value-chain-strategy (visited on: 10/15/2017).

Fair Information Practice Principles (FIPP). (2018), IT Law Wikia, http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (Accessed 29 March 2018).

Great Britain (2003). The Privacy and Electronic Communications (EC Directive) Regulations (PECR). London: The Stationary Office.

Great Britain (1998). Data Protection Act (DPA). London: The Stationery Office.

Greenleaf, G. (2013). "Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories", *UNSW Law Research Paper No. 2013*, 40(September), 29. URL: 10.2139/ssrn.2280877 (visited on: 10/15/2017).

Hofstede, G., Hofstede, G. J. and Minkov, M. (2010). *Cultures and Organizations:Software of the mind*, Third edition. US: The McGraw-Hill Companies.

ICO (2017a). "Home Logic UK Ltd: Monetary Penalties." URL: https://ico.org.uk/action-weve-taken/enforcement/home-logic-uk-ltd/ (visited on: 10/22/2017).

ICO (2017b). "Moneysupermarket.com Ltd: Monetary Penalties." URL: https://ico.org.uk/action-weve-taken/enforcement/moneysupermarketcom-ltd/ (visited on: 09/22/ 2017).

ICO (2016). "Direct Marketing." URL: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf (visited on: 11/07/2017).

Information Regulator (South Africa) (2017). "Department of Justice and Constitutional Development." URL: http://www.justice.gov.za/inforeg/index.html (visited on: 08/15/2017).

ICO (2014). "Protecting personal data in online services: learning from the mistakes of others", URL: https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf (visited on: 11/05/2017).

ICO (2012). "Determining what is Personal Data", URL: https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf (visited on: 11/05/2017).

ICO (n.d.). "Privacy notices, transparency and control", URL: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/ (visited on: 11/07/2017).

Korzilius, H. (2012). "Quantitative Analysis in Case Study." *Encyclopaedia of Case Study Research*, p. 761-764. Thousand Oaks, Sage Publications.

Kumaraguru, P. and Cranor, L.F. (2015). Privacy Indexes: A Survey of Westin's Studies. 2005. *Available as ISRI Technical Report CMU-ISRI-05-138*.

Leyden, J. (2017). "Last year's ICO fines would be 79 times higher under GDPR", *The Register*, URL: https://www.theregister.co.uk/2017/04/28/ico_fines_post_gdpr_analysis/ (visited on: 11/17/2017).

Metzger, M. (2017). "Sharp rise in ICO fines and enforcement notices as GDPR races closer", SC Media UK, URL: https://www.scmagazineuk.com/sharp-rise-in-ico-fines-and-enforcement-notices-as-gdpr-races-closer/article/665466/ (visited on: 11/17/2017).

Morton, A. and Sasse, M.A. (2014). Desperately seeking assurances: Segmenting users by their information-seeking preferences. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on* (pp. 102-111). IEEE.

Noain-Sánchez, A. (2016). "'Privacy by default' and active 'informed consent' by layers." *Journal of Information, Communication and Ethics in Society* 14(2), p. 124–138. URL: 10.1108/JICES-10-2014-0040 (visited on: 09/22/2017).

Norton Rose Fulbright, (2013). PoPI and Insurance, [Online]. Available: http://www.nortonrosefulbright.com/knowledge/publications/74156/popi-and-insurance, 2013.

Organisation for Economic Co-Operation and Development (OECD) (2013). "The OECD Privacy Framework." URL: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (visited on: 29/03/ 2018).

PricewaterhouseCoopers (PwC), (2015). "Turnaround and transformation in cybersecurity", [Online]. Available: https://www.pwc.com/gx/en/ consultingservices/information-security-survey/assets/pwcgsiss-2016-financial-services.pdf, 2015.

Sarkhel, A. and Alawadhi, N. (2017). "How your personal data sells cheaper than chewing gum." ETtech. URL: http://tech.economictimes.indiatimes.com/news/internet/how-your-personal-data-sells-cheaper-than-chewing-gum/57380518 (visited on: 09/22/2017).

South Africa (2013). Protection of Personal Information Act (POPIA) No. 4 of 2013. *Government Gazette*. Cape Town.

South Africa (2008). The Consumer Protection Act (CPA) No. 68 of 2008. *Government Gazette*. Cape Town.

South Africa (2003). Regulation of Interception of Communication and Provision of Communication-related Information Act No. 70 of 2002. *Government Gazette*. Cape Town, 451(24286).

South Africa (1996). Constitution of the Republic of South Africa Act No. 108 of 1996. *Government Gazette* (No. 17678).

Spiekerman, S., Böhme, R., Acquisti, A. and Hui, K.L., (2015). "The challenges of personal data markets and privacy." *Electronic Markets* 25(2), p. 161–167. URL: 10.1007/s12525-015-0191-0 (visited on: 09/22/2017).

Swire, P. P. and Berman, S. (2007). *Information Privacy, Official Reference for the Certified Information Privacy Professional.* Edited by P. Kosmala. Portsmouth, USA: IAPP.

The Economist (2017). "The world's most valuable resource is no longer oil, but data." The Economist Group Limited. URL: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (visited on: 09/22/2017).

Western Cape Government (2016). "Decoding your South African ID Number." URL: https://www.westerncape.gov.za/general-publication/decoding-your-south-african-id-number-0 (visited on: 09/19/2017).

Yin, R. (2003). *"Case study research and applications: Design and methods."* 3rd edition. California, USA. Sage Publications