The effect of the Protection of Personal Information Act of 2013 on the short-term insurance industry

CE Fryer

orcid.org/0000-0002-7595-4920

Mini-dissertation submitted in partial fulfilment of the requirements for the degree *Master of Laws in Estate Law* at the North-West University

Supervisor: Prof HJ Kloppers

Co-Supervisor: Prof W Erlank

Graduation ceremony: May 2021

Student number: 25029746

ACKNOWLEDGEMENTS

The following persons warrant specific recognition in the completion of this study:

- My Lord and Saviour, for the knowledge bestowed upon me and the ability to follow my passions.
- My parents, Charles and Elna Fryer, for their love and support throughout this process.
- My brother, Reghardt, for always being there.
- My supervisors, for your help and guidance during this year.
- My friend and colleague, Roua Pienaar, for your continuous encouragement and counsel.

ABSTRACT

The value of information has seen a substantial increase in recent years. This is due to the rapid advancements in technology and the expanded digital manner in which society interacts. It is viewed as the cornerstone of successful business and has become a staple of modern society. Personal information in particular has received increased attention. Consequently, it is no wonder that legislative intervention would be sought sooner or later.

After many years of uncertainty, the majority of the *Protection of Personal Information Act* has received executive approval. This Act seeks to regulate the manner in which personal information is processed by providing specific conditions that need to be adhered to and aims to uphold the right to privacy throughout this process. Due to its determinations its reach will be wide and many industries will have to align their practices therewith, but with the effective date of 1 June 2020 having already passed, time is running out to achieve compliance within the one-year grace period.

The South African short-term insurance industry, in particular, is a purveyor of vast amounts of personal information. This is used to both provide a service to and assess the risk of a client. As such this industry will most assuredly be affected by the *Protection of Personal Information Act.* The only question, though, is to what extent this will happen. In considering this question it is necessary to take into account the legislation currently governing this industry as well as the secondary effects of this act as it pertains to the reporting of financial crimes and insurers' relationships with third-party information processors. The regulation of personal information protection at an international level will also play a crucial role.

KEY WORDS

Personal information; data; short-term insurance; insurance; privacy; PoPi

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

CPA	Consumer Protection Act
ECT	Electronic Communications and Transactions Act
EJBSS	European Journal of Business and Social Sciences
EJIL	European Journal of International Law
FAIS	Financial Advisory and Intermediary Services Act
FICA	Financial Intelligence Centre Act
GDPR	General Data Protection Regulation
IBERJ	International Business and Economics Research Journal
ICS	Information & Computer Security
IJMR	International Journal of Market Research
ILR	Iowa Law Review
ISGA	Information Security Group Africa: Privacy Special Interest Group
ISSA	Information Security for South Africa
JBL	Juta's Business Law
JCP	Journal of Consumer Policy
JDFSL	Journal of Digital Forensics, Security and Law
JICLT	Journal of International Commercial Law and Technology
JILT	Journal of Information, Law & Technology
JSCI	Journal of Systemics, Cybernetics and Informatics
JICES	Journal of Information, Communication and Ethics in Society

PAIA	Promotion of Access to Information Act
PAJA	Promotion of Administrative Justice Act
PELJ	Potchefstroom Electronic Law Journal
PoPi Act	Protection of Personal Information Act
SAIEE	South African Institute of Electrical Engineers
SAJIM	South African Journal of Information Management
SALJ	South African Law Journal
SAMLJ	South African Mercantile Law Journal
SHLR	Seton Hall Law Review
SSL	Scandinavian Studies in Law
THRHR	Tydskrif vir Heedendaagse Romeins-Hollandse Reg

Chapter 1: Introduction

1.1 Problem Statement

Information, and personal information in particular, has become an increasingly important asset in today's society.[1] This is because of the (mostly) digital way in which people have been interacting with one another.[2] It is one of the cornerstones of successful business[3] and has become a staple of modern societal dealings and interaction,[4] even to such an extent that the period civilisation currently finds itself in has been bestowed the sobriquet of "the information age".[5] The concept of "information" has not remained stagnant throughout history. Over the years, it has developed to assume various forms, from spoken and written word to physical and electronic text.[6] It may also vary from news regarding world issues to facts and science-based material.[7] Not surprisingly, with the scope of information so vast, the quality and quantity of collected information has been rising steadily for years.[8]

Technology and its continuous advancement over time has also brought about numerous problems and consequences. Since the 1960s, concern has increased steadily regarding the effect technology has on information and the way these two concepts interact as a result of the rapid expansion of electronic commerce.[9] With new technology regularly being created and integrated into society, the manner in which information is being collected and handled is faced with continuous change and adaptation.[10] The processing of personal information, in particular, has seen a change in recent years due to the advancement of technology, with the collection

---

1 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3.
2 Swales 2016 *SAMLJ* 49. See also Heyink 2015 *De Rebus* 31.
3 Taylor and Cronjé *101 Questions and Answers about the Protection of Personal Information Act* 3.
4 Swales 2016 *SAMLJ* 49.
5 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3. See also Heyink 2015 *De Rebus* 31.
6 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 15.
7 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 15.
8 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3.
9 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf. See also Van der Bank 2012 *EJBSS* 79; Van Ooijen and Vrabec 2019 *JCP* 92.
10 Kandeh, Botha and Futcher 2018 *SAJIM* 1.

and processing of this category of information being expanded to include details such as people's financial information, health and healthcare information and even their employment history.[11] It is no wonder then that, despite the advantages technology has brought about, it is seen as one of the biggest threats to individuals and their privacy.[12] These concepts are firmly entwined and have a unique and ever-present impact on one another.[13]

1.1.1 Right to Privacy

When it comes to the processing of personal information there is a generally held belief that it threatens not only a person's privacy but also their identity through the disposal of distinguishing information relating to that person.[14] The idea is that if a person is not able to exert control over their information, their privacy will suffer

---

11 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3.

12 Van der Bank 2012 *EJBSS* 78. As far back as 1890 people have been studying the relationship between technology and privacy and commenting on the impact that they have on one another. Warren and Brandeis even went so far as to state that the creation of photography and the expansion of newspapers and journalism justified a need to protect the right to privacy of individuals. A century later the debate regarding technology and privacy has not yet abated, with the introduction of new technology every day complicating matters. See also Kandeh, Botha and Futcher 2018 *SAJIM* 1 in reference to Warren D and Brandeis D "The right to privacy" 1890 *Harvard Law Review* 4(5) 193–220.

13 Kandeh, Botha and Futcher 2018 *SAJIM* 1. When it comes to information processing and the possible risk this poses to individuals it is important to understand who accesses this information. They are commonly known as data controllers and can be found in both the private and public sectors of society. Public data controllers process data on a vast range of topics such as learners at educational institutions, incarcerated persons held by the police or at correctional facilities or census report data. Private data controllers, on the other hand, collect information relating to specific topics of interest to them such as banks and financial institutions gathering information relating to an individual's financial status or insurance companies who refine data relating to the risk posed by their clients, be it either short term risks (referring to a client's property) or long-term risks (referring to a client's life). It is also important to understand the concept of "data" and "information" before seeking to explore the threat posed. These two concepts are often used interchangeably although their meaning indicates there might exist a difference between them. This is because data is seen as "raw" material that is as yet unprocessed, while information pertains to material that has already been structured and refined to such an extent that it has meaning for the recipient. Those who oppose this view believe that, in practice, it becomes difficult to differentiate between these concepts which leads to unnecessary nit-picking. See also Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 11, 12, 13, 18.

14 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 14. Ackermann J even went so far as to determine in *Bernstein ao v Bester NO AO* (1996 (2) SA 751 (CC) that, "The nature of privacy implicated by the right to privacy related only to the most personal aspects of a person's existence, and not every aspect within his/ her personal knowledge and experience". See also van der Bank 2012 *EJBSS* 80.

greatly or might even be lost.[15] This right is firmly entrenched in the democratic values that form the foundation of society, with every person having an interest in the protection of not only their own but other peoples' privacy.[16] It is a relatively modern concept and has become one of the most important rights in contemporary culture, having been recognised across the world.[17] Concurrently, the notion of privacy is not seen as a natural right, mainly because of the fact that the idea of protecting a person's privacy through legislation is more recent than one would think.[18] It is not absolute in its nature[19] which implies that when disputes arise between the right to privacy and any other fundamental rights the courts will have to balance the rights that are in conflict with one another.[20]

In South Africa, the right to privacy was recognised for the first time as part of case law during the 1950s, in the case of *O'Keeffe v Argus Printing and Publishing Co Ltd*.[21] Since then South Africa has come a long way in its definition and protection of this right. Most notably is its inclusion in the Constitution, specifically through section 14 which determines that every person has the right to privacy, which includes the right to not have themselves or their homes searched, their property searched, their possessions taken or the privacy of their communications intruded upon.[22]

---

15 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 16. See also van der Bank 2012 *EJBSS* 77; Da Veiga and Swartz 2017 *SAIEE* 56.

16 Van der Bank 2012 *EJBSS* 78.

17 Van der Bank 2012 *EJBSS* 78. Interestingly, the greater part of foreign legislation protecting an individuals' privacy was only formulated as recently as the 1960s. This right is also unique in nature due to the fact that it is fairly relative and its understanding differs from person to person. See also De Bruyn 2014 *IBERJ* 1315; Van Ooijen and Vrabec 2019 *JCP* 92; Heyink 2013 *Law Society of South Africa* 30 for more information regarding the inspiration behind information protection in the international community.

18 Van der Bank 2012 *EJBSS* 79; Swartz and da Veiga 2016 *ISSA* 9.

19 Van der Bank 2012 *EJBSS* 79.

20 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 15.

21 *O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C)*. In this case the right to privacy was protected mainly through the common law remedy of the *actio iniuriarum.* See also Roos 2012 *SALJ* 377; Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 2.

22 Section 14 of the *Constitution of the Republic of South Africa*, 1996. It is clear that the Constitution recognises the right to privacy as fundamental through Section 14 of the Bill of Rights. See also Roos 2012 *SALJ* 394; Kandeh, Botha and Futcher 2018 *SAJIM* 2.

The right to privacy that is enshrined in the Constitution is not restricted to the "areas of privacy" as found in section 14.[23] By making use of the word "including", section 14 illustrates that the right to privacy is not limited to the specific areas mentioned in the Constitution but may rather encompass a broader range of rights.[24] It is only a general right to privacy that is emphasized in this section, with specific mention being given to searches and seizure of property and communication privacy.[25] Although it does not explicitly mention personal information, the notion persists that a person has the right to the privacy of their communication which in turn establishes the protection of personal information and data.[26] This right may also be lawfully infringed upon where the infringement is reasonable and justified[27] and has to be balanced with other contesting rights such as one's freedom of speech or the access to information.[28]

1.1.2 Information protection legislation

In light of the codification of the right to privacy it is no wonder that the protection of personal information has been labelled as a basic necessity[29] and one warranting legislative consideration.[30] In recent years, the protection of personal information

---

23 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 4. Justice Sachs even went so far as to explain, in the case of *National Coalition for Gay and Lesbian Equality & another v Minster of Justice & others* (1999 (1) SA 6 (CC) at paragraph 32 that the concept of privacy includes the right to a "sphere of private intimacy and autonomy" and not having the outside community interfere. It has also been noted, in *Bernstein & others v Bester & others NNo* (1996 (2) SA 751 (CC) at paragraph 32, that privacy is based on what is "necessary to have one's own autonomous identity". See also Heyink 2015 *De Rebus* 31; van der Bank 2012 *EJBSS* 78.

24 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 4. See also Heyink 2013 *Law Society of South Africa* 5; Swales 2016 *SAMLJ* 50; Millard 2013 *THRHR* 614.

25 Roos 2012 *SALJ* 394, 395. This implies that Section 14 can be extended to the collection or disclosure of other information. See also van der Bank 2012 *EJBSS* 79; Da Veiga and Swartz 2017 *SAIEE* 57.

26 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 15.

27 Swales 2016 *SAMLJ* 50. It is important to remember that the right to privacy is not an absolute right. Both the public interest and societal interest have to be accounted for. See also van der Bank 2012 *EJBSS* 79.

28 Swales 2016 *SAMLJ* 51.

29 Swales 2016 *SAMLJ* 49. The main reason for this classification can be found in modern human interactions. The globalisation of economies and the speed at which technology expands has held information as its key to success. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 4.

30 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 5.

has received global recognition, initially by the European Union through its *Charter of Fundamental Rights of the European Union*, but also by countries such as Australia and Canada.[31] All of these legislative guidelines have had a profound impact on the development of information legislation across the globe,[32] and unsurprisingly, the idea of global data protection has become the buzz word in everyday speech.[33] In spite of the international attention afforded to the protection of personal information, it is necessary to remember that this is not just an international problem but one that should also receive the appropriate local attention.[34]

The *Protection of Personal information Act* (hereafter PoPi Act) was promulgated on the 19th of November 2013 after a long and arduous process.[35] This act has as its main reason for creation the protection of each citizen's constitutionally mandated right to privacy by prohibiting the inadvertent disclosure of personal information.[36] The goal of this legislation is not to inhibit the "free flow" of information but rather to ensure that this is done in such a manner that is in balance with other constitutional rights and values.[37] It is aimed at protecting the personal information

---

31 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 1. In Australia, the protection of information is mainly enforced through the *Privacy Act* 119 of 1988 relating to the use etc of personal information while. Canada has gone a similar route and codified these principles in the *Personal Information Protection and Electronic Documents Act* of 2001. In Europe, two of the main governing documents have been the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention) and the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines governing the protection of privacy and transborder data flows of personal data. See also Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf; Goddard 2017 *IJMR* 703 for a further examination of international regulation of this matter.

32 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf.

33 Swales 2016 *SAMLJ* 49.

34 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf. Considering that the European Union has been at the helm of personal information protection, it is no wonder that South African legislation has depended heavily on European legal examples and guidelines when it comes to data protection. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 5.

35 Swales 2016 *SAMLJ* 49; Swartz and da Veiga 2016 *ISSA* 9; Da Veiga *et al* 2019 *ICS* 400.

36 Swales 2016 *SAMLJ* 49. See also Taylor and Cronjé *101 Questions and Answers about the Protection of Personal Information Act* 2.

37 Taylor and Cronjé *101 Questions and Answers about the Protection of Personal Information Act* 2.

of individuals as processed by both private and public entities[38] and gives significance to the ecumenical fundamental rights emphasized in section 14(d) of the Bill of Rights.[39] At the same time it strives to align the right to privacy with the other rights such as the right to access to information.[40] One of the main concerns of the PoPi Act refers to the processing of personal information where it is entered into a record (being any type of recorded information in any form of medium), has been created in an automated or non-automated way (or forming part of a filing system), where the responsible party is domiciled in South Africa, or, if not domiciled in South Africa, uses an automated or non-automated means in South Africa.[41]

This act has been rolled out in stages, with various sections having already been brought into effect in 2014, such as those sections dealing with the establishment of the Information Regulator.[42] Section 2 to 38, 55 to 109, Section 111 and 114 (1 to 3) commenced on 1 July 2020.[43] These are key parts of the PoPi Act and they relate, specifically, to the lawful processing of personal information, amongst other things.[44] With the commencement of these sections, public and private bodies will have just one year in order to establish compliance with the Act.[45]

The question remains, however, why it would be necessary to promulgate specific privacy related legislation when one has the Constitution, and in some cases,

---

38 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013.

39 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 16; Millard 2013 *THRHR* 615.

40 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013.

41 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 6.

42 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013; Swales 2016 *SAMLJ* 82.

43 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013; Moyo 2020 *De Rebus* 6.

44 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013. See also Kandeh, Botha and Futcher 2018 *SAJIM* 3.

45 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013. The procession of personal information must adhere to the provision set out in the PoPi Act within one year after the commencement of Section 114. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 11.

common law, to effect the right to privacy?[46] In answering this question the reasoning behind the PoPi Act must be considered. It was initially drafted due to overwhelming recommendation from the South African Law Reform Commission in their discussion paper 109 of project 124.[47] They realised that it was necessary for the right to privacy (as enshrined in the Constitution and common law) to be properly recognised.[48] Currently there are numerous locally existing legislative instruments that affect the protection of personal information such as the *Promotion of Access to Information Act* (hereafter PAIA)[49] and the *Promotion of Administrative Justice Act* (hereafter PAJA).[50] This means that the PoPI Act cannot be viewed in isolation[51] but must rather be considered in conjunction with these legislative instruments as all of them either directly or indirectly affect the protection of individuals' information.[52] Respecting individuals' privacy remains the order of the

---

46 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 4.

47 Luck 2014 *De Rebus* 45. See also Heyink 2013 *Law Society of South Africa* 5.

48 Luck 2014 *De Rebus* 45. After careful research and consideration they reached the following conclusions, which had a direct influence on the creation of the PoPi Act: in the first instance they determined that privacy and information protection should be regulated through general information protection legislation; secondly it was clear that general principles of information protection would have to be developed and incorporated into this legislation; in order to regulate this legislation it would be necessary for a regulatory agency to be established to oversee adherence to this legislation; a flexible approach should be followed through which industries can develop their own codes of conduct in line with legislation and which would, in turn, be overseen by the regulatory agency; and lastly, the legislation that is developed as a result of the Law Reform Commission's recommendations must provide an adequate level of information protection in line with international instruments of a similar nature, such as the EU Directive. See also Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf; van der Bank 2012 *EJBSS* 85; Cronje 2009 *JDFSL* 44.

49 *Promotion of Access to Information Act* 2 of 2000. See also Heyink 2013 *Law Society of South Africa* 44 for a discussion regarding the transfer of obligations from the Human Rights Commission to the Information Regulator and the latter's role in the enforcement of this Act.

50 *Promotion of Administrative Justice* Act 3 of 2000.

51 *The Regulation of Interception of Communications and Provision of Communication-Related information Act* 70 of 2002, the *Electronic Communications and Transactions Act* 25 of 2002 and the *National Credit Act* 34 of 2005 all affect the processing of personal information and should always be taken into account when the protection of this information is being considered. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 9.

52 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 9. The PoPi act must ultimately be brought in line with existing legislation so that it contributes to society rather than hinder it. See also Heale 2018 https://www.sapiens.com/blog/additional-popi-challenges-for-insurers-in-south-africa/.

day but the difficulty arises when this needs to be aligned with legislation and society as a whole.[53]

1.1.3 Short-term insurance and personal information

Currently, the main drive behind the PoPi Act is to ensure that an individual's personal information is used only for legitimate reasons and that the use thereof does not infringe on an individual's right to privacy.[54] It is interesting to note that although the PoPi Act spans across all industries and affects both the public and private sectors[55] it is the private sector, in actuality, that poses the biggest threat to the protection of individuals' information privacy.[56] This is largely due to the digitisation of personal records.[57]

The PoPi Act is especially important to the financial services sector as financial services providers often find themselves in possession of personal information that they collect and operate with on behalf of their clients.[58] The short-term insurance industry, in particular, is one of the main parties responsible for the handling of vast quantities of personal data and processing it into a vast array of information such as risk profiles.[59] This is due, in short, to the rise of the credit and insurance market in recent years and has led to a rapid increase in the variety of personal information held and dealt with.[60] The PoPi Act might also have a direct impact on this industry

---

53 Da Veiga and Swartz 2017 *SAIEE* 59.

54 Rodrigues 2012 www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286. A secondary reasoning for the creation of the PoPi Act relates to the international regulation of personal information – the enactment of this legislation will see the alignment of local information protection with the international community and their developments. See also van der Bank 2012 *EJBSS* 85.

55 Kandeh, Botha and Futcher 2018 *SAJIM* 1.

56 Van der Bank 2012 *EJBSS* 80.

57 Da Veiga and Swartz 2017 *SAIEE* 56, 57. In spite of the mass digitisation that has taken place in recent years, people still have a reasonable expectation that their information will be processed in a sufficiently secure manner by companies. Any resultant mistreatment of information may then lead to people losing trust in the various companies holding their information.

58 Rabenowitz *et al The South African Financial Planning Handbook* 57.

59 Da Veiga and Swartz 2017 *SAIEE* 60. As a result, the most common question is not if information can be obtained but rather should it be collected and to what extent will it be used. See also Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf.

60 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf. By providing policy benefits to clients, the short -term insurance industry finds itself in the midst

due to its requirement that personal information be managed in a secure and proper manner.[61]

1.2 Research question

Considering the previously discussed problem statement, the following research question was pondered: To what extent does the *Protection of Personal Information Act* affect the short-term insurance industry?

In order to answer the posed research question, the inspiration behind and contents of the PoPi Act will have to be explained and examined. This will be viewed in light of and in conjunction with the current position held in the insurance industry as it relates to the processing of a client's personal information.

The main objective of this study will consequently be to determine what the PoPi Act requires in terms of personal information processing, how the short-term insurance industry interacts with personal information and if these two positions intersect at any point. Subject to this objective it will also be necessary to determine whether the reporting obligations imposed on short-term insurers in terms of financial crimes and the processing of information by third-party processors will be impacted by the PoPi Act.

1.3 Preview of study

The present study investigates how the PoPi Act affects the short-term insurance industry. This topic was chosen because of the ignorance surrounding the content of the PoPi Act and the manner in which it might affect important information processors such as short-term insurers.

---

of this developing matter. See also Rodrigues 2012 www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286.

61 Rabenowitz *et al The South African Financial Planning Handbook* 57, 58. In order to ensure compliance with the act employers will also be responsible for ensuring that their employees receive the necessary training to guarantee their actions are in line with the act. The PoPi Act will also force short-term insurance companies to balance their relationship with services providers and third parties with their need to provide customer centric service. See also Miller and Milligan 2019 *KPMG*: *The South African Insurance Industry Survey* 39.

This dissertation has been divided into six chapters. Chapter 2 will discuss the inception of personal information protection legislation as well as examine the PoPi Act and its conditions relating to the lawful processing of personal information. Thereafter, in chapter 3 the current insurance law position relating to information processing will be analysed and interpreted, with chapter 4 going into more detail regarding the reporting obligations imposed on short-term insurers in terms of financial crimes and the processing of information by third-party processors. Chapter 5, in turn, then analyses the international position regarding the protection of personal information, with chapter 6 rounding out this study by concluding the applicable findings.

Chapter 2: The PoPi Act

2.1 Legislative Origins

Information protection forms one part of the ultimate protection of a person's privacy. In order to protect this right, the Constitution and common law may be employed, but to ensure effective protection of people's privacy and personal information, legislative oversight is necessary.[62] The South African Law Reform Commission was of the opinion, in their discussion paper on Data Privacy, that individuals should also be able to control their personal information and what happens to it.[63] They believed that this would only be attained through legislative intervention and made recommendations in this regard in their discussion paper.[64] They also determined that it should be possible for responsible parties to approach an Information Commissioner for exemption, should it be required. The PoPi Act was the direct result of their recommendations[65] and will be analysed throughout this chapter.

2.2 The Protection of Personal Information Act

The PoPi Act was promulgated on the 19th of November 2013,[66] with the majority of the provisions brought into effect only on 1 July 2020.[67] It recognizes that every

---

62 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf.

63 Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf. See also van der Bank 2012 *EJBSS* 77; Swales 2016 *SAMLJ* 59; Van Ooijen and Vrabec 2019 *JCP* 92.

64 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 5. Because the definition of personal information is so broad, they deemed it necessary to differentiate between that which is in need of legislative regulation and that which is not. They proposed that the information in need of regulatory oversight should include, but not be limited to information held by both the private and public sector on natural and juristic persons and should be extended to include automatic and manual records, sound and image information, professional and sensitive information to critical information (only where necessary). Information pertaining to purely personal and household activities could be excluded in this instance. See also Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf; Swales 2016 *SAMLJ* 59.

65 Luck 2014 *De Rebus* 45.

66 Swales 2016 *SAMLJ* 49; Swartz and da Veiga 2016 *ISSA* 9.

67 The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013.

person has the right to privacy in accordance with Section 14 of the Constitution[68] and that this right includes the protection of their personal information[69] against illegal processing,[70] theft and security breaches.[71] It also reiterates that information should be allowed to exist, be processed without unnecessary impediment and that this should be done in line with international standards.[72] It is notable that some information has been excluded from regulatory oversight though, especially as it relates to information used for solely personal or household purposes, information that has been de-identified or, in the case of public bodies, that relates to national security or the prohibition of unlawful activities.[73]

There are also certain recurring terms in the Act that require clarity. Most importantly is the notion of "consent" which has to be obtained before any information is collected. This forms a central part of information processing and indicates that a deliberate agreement exists on the part of the data subject that their personal information may be processed.[74] The data subject is the individual or entity whose personal information is being processed and must be competent to

---

68 Heyink *De Rebus* 31. Section 2 of the PoPi Act emphasizes this by stating that the purpose of the act relates to the implementation of the right to privacy as enshrined in the Constitution as follows - by aligning this right with other rights and protecting the movement of information, by coordinating the way in which personal information is refined, by ensuring that individuals have appropriate countermeasures should the processing of their information be at risk and by guaranteeing adherence to the act through specific procedures.

69 It is important to note that there exists a distinction between confidential information and personal information. Taylor and Cronjé state on page 25 of their book, *101 Questions and Answers about the Protection of Personal Information Act* that confidential information refers to a more extensive classification of personal information. This implies that not all confidential information can be classified as personal information but all personal information will be deemed confidential.

70 Preamble of the *Protection of Personal Information Act* 4 of 2013.

71 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/.

72 Preamble of the *Protection of Personal Information Act* 4 of 2013.

73 Heyink 2013 *Law Society of South Africa* 11; Hamann and Papadopoulos 2014 *De Jure* 56.

74 Taylor and Cronjé *101 Questions and Answers about the Protection of Personal Information Act* 11. Taylor and Cronje continue by noting that in Section 1 of the PoPi Act it notes that consent must be "voluntary, specific and informed". Voluntary refers to consent that is given without being coaxed or unduly influenced, specific implies that the consent cannot be general in nature and must pertain to the purpose that the information is being collected for and informed shows that the data subject must be fully aware of what they are agreeing to and what the effect thereof will be. In order for a data subject's consent to be justifiable all three requirements must be satisfied.

provide the necessary consent for their personal information to be processed.[75] They are entitled to the legal processing of their information and have to be informed if this information is being collected or procured by unauthorised personnel. At the same time, they may also enquire if their information is being held by an entity, ask for the correction or elimination of their information, or challenge the processing of this information. Should a request in this regard not be complied with, a data subject can lodge a complaint with the Information Regulator or may initiate civil proceedings.[76]

The PoPi Act has also created its own term for the handling of personal information, namely "processing", which is purposefully wide to include every possible action that could be undertaken with a data subject's personal information.[77] This processing must be done for legitimate purposes[78] by a responsible party[79] and includes information relating to either a natural or juristic person and their personal attributes, be it their race, gender, sex, nationality, age, health, religion or language, their education, medical or financial history, communication information such as a telephone number, email address or physical address, biometric information, opinions or correspondence of an intimate nature.[80]

It should be noted that this act does not apply to the use of personal information for journalism or literary and artistic expression in the event that the aforementioned is done in the public interest and falls within the ambit of expressive freedom.[81]

---

75 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 54. Section 1 of the PoPi Act states that a competent person is someone legally qualified to provide permission with regards to actions or decisions involving children.

76 Section 5 of the *Protection of Personal Information Act* 4 of 2013. The role of the Information Regulator will be clarified in section 2.3 of this chapter.

77 Milo and Ampofo-Anti 2014 *Without Prejudice* 30.

78 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/.

79 Milo and Ampofo-Anti 2014 *Without Prejudice* 30. Section 1 of the PoPi Act states that a responsible party is deemed a public or private body who process personal information for a specific purpose. They are able to process personal information, but the processing only becomes lawful once the eight conditions set out in the act are adhered to. In order for the processing to be lawful there must also be an element of fairness. This implies that there must exist an element of procedural fairness in the way which the Information regulator fulfils its duties.

80 Section 1 of the *Protection of Personal Information Act* 4 of 2013; Moyo 2020 *De Rebus* 5; Milo and Ampofo-Anti 2014 *Without Prejudice* 30.

81 Coetzee 2014 *Without Prejudice* 69.; Hamann and Papadopoulos 2014 *De Jure* 56.

Should a dispute arise regarding the aforementioned processing of personal information a weighing up of interests will have to take place.

In order to ensure lawful processing of a data subject's personal information the PoPi Act proposes eight conditions which need to be adhered to by data processors.[82] These main conditions are supported by three less descript conditions and are unique in nature while simultaneously ensuring that information is processed securely, responsibly and with consent from the relevant individual, should it be required.[83]

2.2.1 Accountability

Accountability is the first condition that needs to be adhered to. It necessitates that the data processor is responsible for ensuring compliance when data is being processed[84] and that those involved with the processing of personal information must adhere to the conditions set out in the act at all times.[85] The notion of accountability of the responsible party is also a common thread throughout the PoPi Act. It relates to not only the initial processing of a data subjects' information but is extended to the further processing thereof (if applicable) or when the information is placed in a third party's charge. This ensures adequate preservation of the information.[86]

---

82 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 43. These conditions set out the most basic requirements for the lawful processing of personal information. See also Kandeh, Botha and Futcher 2018 *SAJIM* 3.

83 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/.

84 Heyink 2013 *Law Society of South Africa* 13. For more information regarding an insurer's duty to transparency and the manner in which this facilitates accountability see also Millard and Kuschke's article titled "Transparency, Trust and Security: An Evaluation of the Insurer's pre-contractual duties".

85 Milo and Ampofo-Anti 2014 *Without Prejudice* 31. Only this person will be held accountable, which would ease prosecution in the event of non-adherence. See also Moyo 2020 *De Rebus* 5; Swales 2016 *SAMLJ* 61.

86 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 45. In this way the responsible party will remain responsible for the information regardless of where the information is in the processing chain. See also Heyink 2013 *Law Society of South Africa* 13.

2.2.2 Processing Limitations

The second condition relates to processing limitations of personal information. It determines what it means to lawfully process information, from obtaining and recording consent where necessary to making provision for consent removal by the relevant data subject.[87] This condition specifically notes that personal information has to be processed in a manner that is lawful,[88] reasonable[89] and which protects the privacy of the data subject.[90] At the same time it may only be processed for a specific reason that adheres to the parameters of relevance and moderation,[91] which will severely limit the access to information by third parties. The processor will then either have to prove consent from the data subject, legitimate interest or public record of the information.[92] The notion of processing limitations emphasizes the need for consent, with Section 11 specifically stating that processing may only be done once the proper consent has been obtained, requiring indication of whether it is done in terms of a contractual relationship of which the data subject is a party or in terms of a public body's duty. It should also only be done if it protects the justified interest of the data subject or the processing complies with a legal requirement. [93] Section 12 then goes further to note that personal information needs to be obtained from the data subject personally except where it forms part of the public record,

---

87 Moyo 2020 *De Rebus* 5.

88 Although the PoPi act requires the processing of personal information to be lawful, thus according to the conditions set out in the act, this requirement of lawfulness can be extended further to include that the processing has to be in line with the basic ideals set out in the Constitution, the international standards as confirmed by South Africa, the Common Law as well as PAIA and PAJA, where applicable. See Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 31. Burns and Burger-Smidt continue on page 43 by stating that the conditions found in the PoPi act can be seen as the minimum standards to be upheld by those processing the information.

89 The notion of reasonableness determines that responsible parties must consider the reasonable expectations of data subjects as well as their interests when they interact with personal information. See also Heyink 2013 *Law Society of South Africa* 15; Moyo 2020 *De Rebus* 5.

90 Section 9 of the *Protection of Personal Information Act* 4 of 2013; Moyo 2020 *De Rebus* 5.

91 Milo and Ampofo-Anti 2014 *Without Prejudice* 31; Heyink 2013 *Law Society of South Africa* 15.

92 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/. See also Swales 2016 *SAMLJ* 61.

93 Section 11 of the *Protection of Personal Information Act* 4 of 2013. This section goes further to confirms that the burden of proof will fall on those processing the personal information and a data subject may oppose the use of their personal information at any point. Should this occur the responsible party must give reverence to this request.

permission has been received for the collection thereof from another party - which will not negatively affect the interest of the data subject - or if the acquisition relates to national security or ongoing legal proceedings.[94]

2.2.3 Purpose Specifications

Together with the above there has to be appropriate reasoning for the collection of the information.[95] Personal information has to be obtained for a predefined purpose which is known to the data subject[96] and may only be held until the processing purpose has been fulfilled.[97] The information in question may only be kept, outside of the parameters of this condition, should the retention be expected by law, relate to the functioning of the collector, be contractually required in terms of an agreement between the parties or where formal permission has been received from the data subject.[98] Thereafter it needs to be destroyed through de-identification and re-identification must not be possible.[99]

2.2.4 Further Processing Limitations

Further processing limitations also exist and make up the fourth condition. This condition determines how information can and cannot be processed.[100] Section 15 specifically states that should personal information that has been collected be processed further, this processing will need to be done in accordance with the

---

94 Heyink 2013 *Law Society of South Africa* 16; Section 12 of the *Protection of Personal Information Act* 4 of 2013; Moyo 2020 *De Rebus* 5.

95 Section 13 of the *Protection of Personal Information Act* 4 of 2013; Millard 2013 *THRHR* 616.

96 Milo and Ampofo-Anti 2014 *Without Prejudice* 31; Moyo 2020 *De Rebus* 5.

97 Heyink 2013 *Law Society of South Africa* 17. This condition entails three aspects that all have to be adhered to in order to fulfil this condition. See also Swales 2016 *SAMLJ* 62.

98 Section 14 of the *Protection of Personal Information Act* 4 of 2013. It is important to note that personal information records may be kept for longer periods if it is required for historical or statistical records and where the proper steps have been taken to safeguard the information.

99 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 62; Swales 2016 *SAMLJ* 62.

100 Burns and Burger-Smidt are of the opinion that this condition takes into account whether the further processing of the information in question holds reference to the original reasoning behind the processing of the information. See Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 63; Heyink 2013 *Law Society of South Africa* 19.

original collection purpose[101] and may only be extended in specific instances, such as where the data subject provides explicit consent or collection is in the public interest,[102] and where the following has been considered: the need for further processing in light of the initial processing, the type of information in question, the repercussions that further processing hold, the way the information was collected and if any liability exists between the parties.[103]

2.2.5 Information Quality

Information quality is another condition in need of adherence. This means that the information processed must be factually complete and that the quality of the information collected must be insured by confirming the accuracy and completeness thereof.[104]

2.2.6 Openness

Condition six relates to the transparency that must exist in personal information processing and requires that proper documentation must be kept as information is processed.[105] This maintenance of documentation must adhere to Section 14 and 51 of PAIA[106] and a data subject has to be aware of the collection and processing of their information.[107] This includes confirming when and from whom information is

---

101 Section 15 (1) of the *Protection of Personal Information Act* 4 of 2013; Milo and Ampofo-Anti 2014 *Without Prejudice* 31.

102 Moyo 2020 *De Rebus* 5; Heyink 2013 *Law Society of South Africa* 19.

103 Section 15 of the *Protection of Personal Information Act* 4 of 2013; Moyo 2020 *De Rebus* 5.

104 Milo and Ampofo-Anti 2014 *Without Prejudice* 31. It is the duty of the responsible party to take reasonable and practical steps to ensure that the information in questions holds true as far as possible. See also Moyo 2020 *De Rebus* 5 and Heyink 2013 *Law Society of South Africa* 19.

105 This condition also ensures that transparency and fairness are considered through the process of interacting with a person's personal information. See also Heyink 2013 *Law Society of South Africa* 20; Millard 2013 *THRHR* 616.

106 Section 17 of the *Protection of Personal Information Act* 4 of 2013. Section 14 of the *Promotion of Access to Information Act* 2 of 2000 indicates that the information officer of a public body is responsible for the creation of a manual that indicated its purpose and make-up, contact information and any further details that allow one to gain access to records placed in the care of the body. This manual must be updated on a frequent base. Section 51 of the same act notes that the head of a private body is responsible for the creation of a manual specifying the contact details of the body, how one would go about gaining access to information held by them and what information they have under their charge.

107 Milo and Ampofo-Anti 2014 *Without Prejudice* 31. A data subject has to consequently be informed of certain information when their personal data is collected.

acquired[108] the physical address of the collector, the reasoning behind the information collection, whether the collection of information is voluntary or required by law, the consequences of non-compliance and whether the information will be handed over to a third party.[109]

2.2.7 Security Safeguards

The penultimate condition notes that sufficient security safeguards must exist to protect personal information whilst it is being processed[110] and necessitates taking the requisite steps to prohibit loss of or improper access to that information. It is usually done through a proper risk assessment which indicates internal and external exposure points.[111] These security safeguards need to be consistent and information processed on behalf of a mandated party must only be done with the proper authorisation and bearing the appropriate confidentiality in mind, except where the disclosure of that information is required by law.[112] Should a breach in information security happen the Information Regulator and the relevant data subject have to be notified as soon as reasonably possible[113] unless notification of this breach should hinder a criminal investigation.[114]

---

108 Moyo 2020 *De Rebus* 6.

109 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/; Swales 2016 *SAMLJ* 63; Moyo 2020 *De Rebus* 6.

110 Heyink 2013 *Law Society of South Africa* 21.

111 Moyo 2020 *De Rebus* 6; Millard 2013 *THRHR* 617; Milo and Ampofo-Anti 2014 *Without Prejudice* 31.

112 Section 20 of the *Protection of Personal Information Act* 4 of 2013. Section 21 continues by declaring that, in the event that information is processed by an operator, a written contract must exist between the responsible party and the operator that necessitates adequate security measures for the processing of the information by the operator. Should a breach of information happen this operator must immediately inform the responsible party. See also Swales 2016 *SAMLJ* 63.

113 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 72; Moyo 2020 *De Rebus* 6.

114 Section 22 (3) of the *Protection of Personal Information Act* 4 of 2013. Section 22 (5) goes further to note that notification must be in writing or through means of an alert and should contain sufficient information to allow the data subject to take the necessary steps to protect themselves.

2.2.8 Data Subject Participation

The last condition notes the need for data subject participation. It illustrates the rights of data subjects and determines that they have a right to access their information in order to determine if and what information is being held by a responsible party and to request any correction of the information should it be necessary.[115] The destruction of their information may also be requested and must be afforded the proper attention by the responsible party.[116] Any requests made in terms of Section 23 will be subject to Section 18 and 53 of PAIA.[117]

2.2.9 Processing additional information and direct marketing

The PoPi Act also provides specification regarding the processing of special information, the processing of information related to children and when the processing of personal information will not be in contravention of the Act. In the case of special information, a responsible party may not process information that relates to a data subjects' religion, race, political opinions, health, sex life or philosophical beliefs,[118] except where express consent has been received or where it is in the public interest.[119] When it comes to children, the processing of their personal information is prohibited except where consent has been obtained from a

---

115 Milo and Ampofo-Anti 2014 *Without Prejudice* 31; Heyink 2013 *Law Society of South Africa* 22; Moyo 2020 *De Rebus* 6.

116 Section 24 of the *Protection of Personal Information Act* 4 of 2013. See also Swales 2016 *SAMLJ* 66.

117 Section 18 of PAIA specifies that requests for access need to be done via the prescribed forms and must be sent to the Information Officer of a public body. This form needs to contain sufficient information in order to determined which records are required and in which manner they are required. Section 53 of PAIA specifies the same in relation to a private body.

118 Heyink 2013 *Law Society of South Africa* 23; Section 26 of the *Protection of Personal Information Act* 4 of 2013.

119 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/. Section 27 to 33 of the PoPi Act discusses these items individually and indicates in which instances the processing of special information may be allowed, such as where permission is given by the data subject or if the access of this information is done in accordance with the law, be it national or international in nature. Should the accessing of special information not fall within the ambit as specified in section 27 to 33 of the act, it will not be permitted and those who access this information will make themselves guilty of non-compliance. See also Heyink 2013 *Law Society of South Africa* 23; Da Veiga *et al* 2019 *ICS* 407.

"competent person" or where there is a legal obligation.[120] This may, however, be reconsidered by the Information Regulator should they receive sufficient and compelling notice.[121] In certain instances the processing of personal information would not be in contravention of the act, for example where the Information Regulator provides a responsible party with permission to process certain information because the public interest is greater than any interference the processing may create or if the processing is done to the benefit of the data subject.[122] If the information is also processed for a "relevant function" by a public entity or in terms of legislation it will be permitted.[123]

Direct marketing is another contentious issue when personal information is considered. It refers to the practice of engaging in direct contact with a potential client to inform or convince them of the marketer's product or service[124] and is usually done through electronic means such as phone calls or an SMS. Noteworthy is that the processing of personal information for this reason is strictly prohibited in terms of Section 69 except where a data subject has given consent for their information to be processed, they are a customer of the data processor or if the responsible party markets products of a similar nature to the data subject.[125] The data subject must, however, be allowed the opportunity to halt any correspondence,

---

120 The Preamble of the General Data Protection Regulation (2016/679) gives a reason for this. It states that children are in need of specific protection when it comes to the processing of their personal information because they do not understand what the processing of their personal information entails and what consequences improper processing might have. Section 35 of the PoPi Act also stipulates in which specific instances this information may be processed, which mainly relates to when consent has been obtained from a competent person, where the processing of this information is done in accordance with a legal obligation or if it is done for research purposes (that fall within the public interest). Should this information have been made public previously it may also be accessed. See also Nicole 2019 http://www.privacypolicies.com/blog/popi-act/.

121 Section 35 of the *Protection of Personal Information Act* 4 of 2013.

122 Section 37 of the *Protection of Personal Information Act* 4 of 2013.

123 Section 38 of the *Protection of Personal Information Act* 4 of 2013.

124 Da Veiga and Swartz 2017 *SAIEE* 58; Hamann and Papadopoulos 2014 *De Jure* 44.

125 Millard 2013 *THRHR* 618. Millard goes further to note that Section 69 (3) expands on this point and states that even if the data subject is a customer, they must have been given the opportunity to object to the use of their information in this regard and the information must have been obtain through the conclusion of a sale of goods or services. See also Swales 2016 *SAMLJ* 72; Swartz and da Veiga 2016 *ISSA* 12.

colloquially referred to as having an "opt-in/ opt-out" option[126] and must be informed by the responsible party regarding where their personal information was obtained from.[127] But Section 69 is not as great as it seems. In the first instance it only regulates unsolicited electronic communication which implies that unsolicited communication through traditional means, such as the post, does not fall within its scope.[128] At the same time it is only applicable on the practice of direct marketing itself which implies that should the unsolicited communication fall outside the definition of direct marketing it would not be in contravention of the Act.[129]

2.3 Information Regulator and Non-Compliance

It is notable that the countries who have seen success in protecting personal information through legislation have the same thing in common – they appointed an information regulator.[130] In terms of the PoPi Act, Section 39[131] is responsible for the establishment of the office of the Information Regulator. This is an independent body[132] who is beholden to no one and is similar in its independence to the Chapter 9 institutions as established by the Constitution.[133] Its jurisdiction is limited to the borders of the Republic[134] and it gives reverence to the law, and the Constitution in particular, whilst being answerable only to the National Assembly.[135]

This regulator is tasked with overseeing and administering compliance with the PoPi Act[136] and receives its powers and duties from Section 40, which includes but is not limited to educating people on the importance of protecting personal information (in any way, shape or form), ensuring compliance with legislation through

---

126 Da Veiga and Swartz 2017 *SAIEE* 58. See also Heyink 2013 *Law Society of South Africa* 29; Swales 2016 *SAMLJ* 72.
127 Da Veiga and Swartz 2017 *SAIEE* 59.
128 Swales 2016 *SAMLJ* 72.
129 Swales 2016 *SAMLJ* 72; Hamann and Papadopoulos 2014 *De Jure* 46.
130 Heyink 2013 *Law Society of South Africa* 26.
131 *Protection of Personal Information Act* 4 of 2013.
132 Department of Justice date unknown http://www.justice.gov.za/inforeg/index.html.
133 Heyink 2013 *Law Society of South Africa* 26.
134 Section 39 of the *Protection of Personal Information Act* 4 of 2013.
135 Department of Justice date unknown http://www.justice.gov.za/inforeg/index.html; Swales 2016 *SAMLJ* 76.
136 Department of Justice date unknown http://www.justice.gov.za/inforeg/about.html.; Swales 2016 *SAMLJ* 75; Hamann and Papadopoulos 2014 *De Jure* 56.

continuous assessment and examination of public and private entities. It must also provide Parliament with continuous feedback regarding its activities.[137] Because the PoPi Act protects information that has been processed by both public and private entities, the Information Regulator acts in terms of both the PoPi Act and PAIA, as PAIA makes provision for the access to information of both public and private entities that is in the care of the state.[138] This body is also responsible for consulting with stakeholders, intervening should intervention be required and giving proper attention to complaints[139] regarding the processing of personal information. It has to ensure that the most recent legislative position on personal information is upheld, monitor the codes of conduct[140] of responsible parties and ensure transnational protection of privacy legislation.

Thus, it is clear that the office of the Information Regulator is an important establishment. Due to the fact that personal information protection is still being established in South Africa and the legislative and judicial positions are being considered and developed[141] they will be playing an active role in the interpretation and execution of the Act. This will require both a flexibility on their part and their continuous involvement in the development of certainty and legal precedent.[142] Only then will the PoPi Act be successful in its purpose.

Non-compliance with the PoPi Act will have its own consequences.[143] Both private and public entities have been given one year to become compliant with the

---

137 *Protection of Personal Information Act* 4 of 2013.

138 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 44.

139 Section 40 of the *Protection of Personal Information Act* 4 of 2013. Should any complaints arise regarding the processing of personal information they must be brought to the attention of the Information Regulator. See Department of Justice date unknown http://www.justice.gov.za/inforeg/about.html.

140 Section 40 of the *Protection of Personal Information Act* 4 of 2013. Together with this they provide different sectors with codes of conduct as well as guidelines regarding the development of codes of conduct. This is important as the development of a proper code of conduct will assist with the adherence to the conditions set out in Chapter 3 of the act regarding the lawful processing of personal information. See Department of Justice date unknown http://www.justice.gov.za/inforeg/about.html. Section 60 provides clarity by indicating that the code of conduct must stipulate how the conditions will be adhered to within a specific sector, such as the short-term insurance industry.

141 Heyink 2013 *Law Society of South Africa* 26.

142 Heyink 2013 *Law Society of South Africa* 26.

143 Nicole 2019 http://www.privacypolicies.com/blog/popi-act/; Moyo 2020 *De Rebus* 6.

conditions in the Act.[144] If compliance has not been achieved after this year and a data subject believes a responsible party has not adhered to the conditions for lawful processing set out in the Act, they may proceed as follows: submit a complaint in terms of the responsible party's code of conduct - which will prescribe the procedure to resolve the complaint,[145] lodge a complaint with the Information Regulator in terms of the prescribed format[146] or initiate judicial proceedings against the guilty party for damages that have been incurred.[147] Should a breach of certain sections of the Act such as Section 54 or 82 occur it might incur additional penalties which can vary from a fine (subject to the discretion of the Regulator and of no more than R10 million) or imprisonment of between 12 months and 10 years.[148]

2.4 Litigious Scrutiny

As the PoPi Act has only recently come into force there has been, as yet, little to no litigation around its application[149] or relating to the enacted provisions.[150] There have, however, been some decisions relating to the notion of privacy in general,[151]

---

144 Moyo 2020 *De Rebus* 6.

145 Section 63 of the *Protection of Personal Information Act* 4 of 2013.

146 Section 74 of the *Protection of Personal Information Act* 4 of 2013. This complaint must be in writing and upon receipt thereof the Information Regulator may either conduct an investigation, act as a conciliator between the data subject and responsible party or refer the complaint to the Enforcement Committee for further action. See further Section 75 and 76 of the *Protection of Personal Information Act* 4 of 2013. If the data subject or responsible party are not satisfied with the eventual outcome, they may then appeal the decision in terms of Section 97 within the prescribed time limit.

147 Moyo 2020 *De Rebus* 6.

148 Milo and Ampofo-Anti 2014 *Without Prejudice* 31.

149 Privacy International 2019 https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa.

150 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* X.

151 Two cases bear specific mention in this instance. In the case of *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others* the Constitutionality of Section 2(1) of the *Indecent or Obscene Photographic Matter Act* 37 of 1967 was in question. This concerned the possession of indecent or obscene photographic and how the possessor will be guilty of an offense. The Constitutional Court determined that section 2(1) was incompatible with the right to privacy and imposed and indefensible restriction on this right. Another case to be noted is that of *Mistry v Interim National Medical and Dental Council and Others*. It reviewed section 28(1) of the *Medicines and Related Substances Control Act* 101 of 1965 in light of the right to privacy. This section determined that in order to enter any premises etc, medicine or a scheduled substance had to be present or there had to exist a reasonable suspicion that it was present. It also allowed access to any document that might be present. The court held at par 23 that this section would enable an intrusion into the inner parts of an individual's life and home and would ultimately intrude on their privacy.

but only time will tell how this act will stand up to litigious scrutiny.[152] Unsurprisingly, in light of the influence the European Union's General Data Protection Regulation[153] had on the development of the PoPi Act and their advanced protection of personal information in general, the majority of case law relating to the protection of personal information can be found in international law.[154] As a result, South African courts will, for the foreseeable future, have to look to international case law for their interpretation of the PoPi Act and personal information protection in general.

In summary, through a clear study of the PoPi Act, the lengths to which an information processor must go to ensure the processing remains lawful becomes apparent. There are eight specific conditions ranging from processing limitations to security safeguards that need to be satisfied throughout the process and various additional requirements that need to be met when certain restricted information will be processed, as is the case with the specific consent required when a child's information is processed. At the end of the day, the reality is that data and information have become a central aspect of successful business.[155] Companies need to consider the security risks that the personal information under their control is exposed to[156] and each industry, from insurance to health services, will have to determine how the PoPi Act will affect them and amend their practices accordingly. In this study only one sector will be reviewed in the following chapter, namely the short-term insurance industry, to determine what its current regulatory determinations are and how the PoPi Act will either change or reinforce this position.

152 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* X.
153 General Data Protection Regulation (EU) 2016/679.
154 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* X.
155 Milo and Ampofo-Anti 2014 *Without Prejudice* 32.
156 Milo and Ampofo-Anti 2014 *Without Prejudice* 32.

Chapter 3: Client information protection in the short-term insurance sector

In the South African short-term insurance industry vast amounts of personal information are processed on a daily basis.[157] This information is understandably necessary to accurately calculate the insurable risk of a client. Any time that sensitive information of this nature is accessed the risk exists that it might be misused, accessed illegally or lost.[158] With the implementation of the PoPi Act the question arises whether this legislation would radically change the way the short-term insurance industry functions or if it would merely reiterate the current legislative position.

The South African insurance industry is very comprehensive, offering a wide range of insurance contracts. Because of this wide range of services offered it is deemed one of the most established sectors in Africa as the nature of the business necessitates a high state of trust by local customers[159] and because the South African insurance sector is supported by a highly cultivated financial sector which endorses healthy competition in the industry.[160] It is subject in all its dealings to the Constitution[161] as the supreme law in South Africa, and any non-compliance will invalidate the relevant law or contract.[162] The rights as found in the Bill of Rights are especially important when it comes to insurance law.[163]

---

157 Da Veiga and Swartz 2017 *SAIEE* 60. See also Mukwakungu and Mbohwa "Short-term insurance company's perspective of Information management and its influence on Continuous Improvement to improve customer satisfaction" 1710 – 1719.

158 Da Veiga and Swartz 2017 *SAIEE* 57.

159 This is due in large part to the fact that the short-term insurance sector holds and processes a high and detailed quality of information due to the services they provide their clients with. See also Mukwakungu and Mbohwa "Short-term insurance company's perspective of Information management and its influence on Continuous Improvement to improve customer satisfaction" 1710 – 1719. Clients also have a reasonable expectation that their privacy will be upheld by companies who interact with their personal information, such as short-term insurers. See also Swartz and da Veiga 2016 *ISSA* 9.

160 Mukwakungu and Mbohwa "Short-term insurance company's perspective of Information management and its influence on Continuous Improvement to improve customer satisfaction" 1710 – 1719.

161 *Constitution of the Republic of South Africa*, 1996.

162 Rabenowitz *et al The South African Financial Planning Handbook* 152.

163 Reinecke, van Niekerk and Nienaber *South African Insurance Law* 22.

In terms of the PoPi Act, information processing will only be deemed lawful in the event that it adheres to the eight conditions stipulated in the act and previously examined in Chapter 2.[164] These conditions might seem ground-breaking at first glance but it is important to also consider the measures imposed by existing legislation. Currently the short-term insurance industry is governed by various laws regulating an insurer's actions towards and interactions with their clients.[165] Together they form the starting point in assessing an insurer's actions and will be scrutinised during the course of this chapter.

3.1 Short-Term Insurance Act[166] *and Insurance Act*[167]

The *Short-Term Insurance Act* relates mainly to the establishment of the Registrar of Short-Term Insurance and the regulation of short-term insurance companies in general, from its establishment which includes its registration, conditions of operation, business model and naming rights, to client policies including the processing of policies entered into by minors, assessments regarding the potential for misrepresentation and the limitations of policy benefits.[168] It can thus be surmised that this legislation has as its purpose the regulation of an insurer's general administration, with little to no mention of how short-term insurers have to interact with clients and their information. This legislation also does not provide a definition for what it deems "information" or "privacy".[169]

The *Insurance Act*, on the other hand, is a relatively new act that sets out a legal framework for the prudential regulation and supervision of insurers in light of the Twin Peaks model.[170] Whilst it aims to expand the protection of policyholders it mostly repeals the prudential requirements set out in previous legislation such as

---

164 Kandeh, Botha and Futcher 2018 *SAJIM* 3.

165 Insurance legislation is unique in its nature as it is aimed at primarily protecting the insured or data subject. See also Millard and Kuschke 2014 *PELJ* 2419.

166 *Short-Term Insurance Act* 58 of 1998.

167 *Insurance Act* 18 of 2017.

168 *Short-term Insurance Act* 58 of 1998.

169 Section 1 of the *Short-Term Insurance Act* 58 of 1998.

170 *Insurance Act* 18 of 2017.

the *Short-term Insurance Act*[171] and makes provision for the introduction of new products under the mantle of micro-insurance.[172] Although beneficial, this Act might be geared more towards the insurance companies and their products than to specific interactions with clients.

All things considered, these two Acts do not really prescribe the manner in which insurers must interact with clients and their information. Viewed in isolation they would clearly justify the information protection reforms that the PoPi Act would lead to. Fortunately, they are not alone in regulating the short-term insurance industry.

3.2 Financial Advisory and Intermediary Services Act[173]

Another pillar of the short-term insurance industry is the *Financial Advisory and Intermediary Services Act* (hereafter FAIS Act). This act governs the financial advice that advisors and intermediaries provide for clients[174] whilst simultaneously regulating the services rendered[175] through strict rules and regulations.[176] As a result it plays an important role in prescribing the market conduct of financial services providers.[177] This is done through its determination of, amongst others, "fit and proper" requirements that representatives of financial services providers have to adhere to in order to perform their services[178] and which are seen as the minimum standards to be upheld when interacting with clients.[179] Another requirement relates to the licencing of financial services providers. This is obtained once the Registrar is satisfied that the financial services provider in question is competent, has proper

---

171 Masthead 2018 https://www.masthead.co.za/newsletter/commencement-of-the-insurance-act/.

172 Unknown 2018 https://businesstech.co.za/news/business/255519/the-new-insurance-act-takes-effect-today-in-south-africa-heres-what-you-need-to-know/.

173 *Financial Advisory and Intermediary Service Act* 37 of 2002.

174 Preamble of the *Financial Advisory and Intermediary Services Act* 37 of 2002.

175 Millard 2013 *THRHR* 620.

176 Millard 2018 *THRHR* 377.

177 Reinecke, van Niekerk and Nienaber *South African Insurance Law* 511.

178 Section 6A (2) of the *Financial Advisory and Intermediary Services Act* 37 of 2002. Section 6A specifies that in order the be classified as "fit and proper" a representative has to be honest and display integrity, be deemed competent by having the necessary experience, qualification, and knowledge, have operational ability, financial soundness and partake in continuous professional development.

179 Millard and Botha 2016 *THRHR* 45; Millard 2018 *THRHR* 377.

operational ability and reflects the necessary characteristics of honesty, integrity and financial soundness.[180] Without these a short-term insurer will not be able to operate within this industry.[181]

It might be argued with some merit that if FAIS requires insurers and representatives to be fit and proper that these requirements will govern the actions of insurers with regard to client information as well. The problem, though, is that FAIS focusses more on the advice that clients are furnished with[182] than how an insurer has to protect a client's personal information. Another issue of note is that although it requires insurers to operate only once licenced, different licences may be issued to insurers subject to different conditions and restrictions.[183] A natural consequence of this would be a lack of uniform actions and treatment of clients by insurers. As a result, there are differing opinions on the success and effectiveness of this law.[184] In closing it would seem that, viewed on its own, the FAIS Act may possibly not protect the personal information of clients as effectively as the PoPi Act.

3.2.1 General Code of Conduct

Read together with the FAIS Act is the General Code of Conduct for financial services providers. It applies to all representatives and intermediaries, except where expressly excluded[185] and determines that financial services providers have to render their services and interact with clients and their personal information in a manner that is honest, fair, done with the proper skill, care, diligence and integrity and in

---

180 Section 8(1) of the *Financial Advisory and Intermediary Services Act* 37 of 2002. Section 9 of the FAIS Act makes specific provision for the withdrawal of a financial services provider's authorization should the license holder no longer adhere to the fit and proper requirements as set out in the act. Should a financial services provider have been debarred in this way due to non-compliance with the fit and proper requirements they will not be allowed to reapply for a license for a period as determined by the registrar. See also Section 9(6)(a) of the *Financial Advisory and Intermediary Service Act* 37 of 2002.

181 Reinecke, van Niekerk and Nienaber *South African Insurance Law* 511.

182 Millard and Botha 2012 *THRHR* 46.

183 Unknown 2003 https://www.itweb.co.za/content/Gb3BwMWom3OM2k6V.

184 Millard 2018 *THRHR* 377.

185 Section 1(3) in Board Notice 80 of 2003 in GG25299 of 8 August 2003 in terms of Section 15 of the *Financial Advisory and Intermediary Services Act* 37 of 2002; Millard and Maholo 2016 *THRHR* 595.

the interest of the client.[186] They may also not make the confidential information of their clients public unless either the client has provided the financial services provider with written consent beforehand, the disclosure of the information is required by law or is in the public interest.[187] Section 12(c) of the General Code of Conduct goes even further to determine that, in the event that a financial services provider does not comply with it, they will be in contravention of the FAIS Act.[188]

It is curious that the General Code of Conduct makes specific mention of the disclosure of confidential information whilst the FAIS Act does not. Section 3(3) seemingly echoes the essence of the PoPi Act in that a data subject must actively agree to the use and processing of their information[189] but the fact that this protection is not duplicated in the FAIS Act itself is notable as one would expect such an important client protection regulation to be prioritised in the act itself and not only in accompanying subsequent regulation. If one considers the legislation currently in development this might not be such a big problem as the General Code of Conduct could eventually be replaced by the approved *Conduct of Financial Institutions Act*.[190]

3.3 Conduct of Financial Institutions Bill

The *Conduct of Financial Institutions Bill*[191] has been lauded the next stage in regulations governing customer interaction in the financial sector[192] and owes its existence to the establishment of the Prudential Authority and Financial Services Conduct Authority by the *Financial Sector Regulation Act*[193] (which governs prudential risk and market conduct respectively).[194] Once enacted, this act will guide

---

186 Millard and Maholo 2016 *THRHR* 599; Millard 2013 *THRHR* 606.

187 Section 3(3) in Board Notice 80 of 2003 in GG25299 of 8 August 2003 in terms of Section 15 of the *Financial Advisory and Intermediary Services Act* 37 of 2002.

188 Kruger 2016 http://www.moonstone.co.za/popi-and-the-general-code-of-conduct/.

189 Section 1 of the *Protection of Personal Information Act* 4 of 2013.

190 Millard 2018 *THRHR* 390.

191 *Conduct of Financial Institutions Bill* [B-2018].

192 Parliamentary Monitoring Group 2018 https://pmg.org.za/call-for-comment/784/.

193 *Financial Sector Regulation Act* 9 of 2017. See also Janse van Rensburg 2019 https://www.werksmans.com/legal-updates-and-opinions/conduct-of-financial-institutions-bill/.

194 Parliamentary Monitoring Group 2018 https://pmg.org.za/call-for-comment/784/.

the conduct of financial institutions currently regulated by multiple laws[195] and will replace the conduct regulations for financial services providers set out in current legislation, such as the FAIS Act and *Insurance Act*, with a new "market conduct legislative framework".[196] Most notable is the incorporation of confidential information protection in its regulations. In Section 34 of the Bill it presently states that financial institutions, specifically, may not disclose or process either confidential or personal information of a customer except when this is done in line with the PoPi Act.[197] This echoes regulations of a similar nature found in the General Code of Conduct[198] and ensures that consumer information will be properly protected as the processing thereof will be measured against the conditions set out in the PoPi Act.[199]

This could imply a dependency of the *Conduct of Financial Institutions Act* on the PoPi Act as it does not really contain its own information regulation principles and merely refers back to the PoPi Act but as this legislation is still in its developmental phase and has not yet been signed into law this remains to be seen.

3.4 Additional guidelines and legislation

The short-term insurance industry is governed by various laws that regulate its establishment and interactions with clients. The most notable has already been discussed but there are a number of other guidelines and laws that also play an important role in the regulation of this industry.

3.4.1 Treating Customs Fairly

In 2014 the National Treasury published a conduct policy framework which was aimed at reforming and ultimately improving the conduct of financial services providers.[200] This is informally known as the TCF and is a principles-based

---

195 Janse van Rensburg 2019 https://www.werksmans.com/legal-updates-and-opinions/conduct-of-financial-institutions-bill/.

196 Janse van Rensburg 2019 https://www.werksmans.com/legal-updates-and-opinions/conduct-of-financial-institutions-bill/.

197 Section 34 of the *Conduct of Financial Institutions Bill* [B-2018].

198 Section 3(3) in Board Notice 80 of 2003 in GG25299 of 8 August 2003 in terms of Section 15 of the *Financial Advisory and Intermediary Services Act* 37 of 2002.

199 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 43.

200 Millard and Maholo 2016 *THRHR* 595.

approach[201] aimed at ensuring fair treatment, needs considerations of clients, transparency, suitability and upholding of standards as well as post-sale assistance. As a result, it echoes much of what has been established by the FAIS Act and General Code of Conduct in terms of interacting with clients and their personal information and although the TCF does clarify these existing principles it will not alter the manner in which financial services providers perform their function and address client interactions.[202]

3.4.2 National Credit Act[203]

In chapter 4 of the *National Credit Act* consumer credit policies, as they relate to consumer's rights and their personal information, are specifically dealt with. It finds resonance with financial services providers considering that it explicitly notes that consumers are entitled to the confidential treatment of their information.[204] Anyone who processes information in terms of this act must first acknowledge the confidential nature of that information and may only use this information for its initial collection purpose or in accordance with legislation.[205]

Although the *National Credit Act* provides for impressive regulation of credit information – which is highly personal and confidential in nature - it does not account for any direct offences in the case of unsolicited electronic communications, merely the misuse of this information.[206] This is something that is specifically protected by the PoPi Act and will be discussed further on, but there are authors who believe that one could argue that sending unsolicited communications might constitute a misuse of personal information that would be deemed an offence in terms of this Act.[207] This reasoning appears somewhat dubious and any offences committed in this regard might be better governed by the PoPi Act.

---

201 Millard and Maholo 2016 *THRHR* 596.
202 Millard and Maholo 2016 *THRHR* 612.
203 *National Credit Act* 34 of 2005.
204 Section 68 of the *National Credit Act* 34 of 2005. See also Swales 2016 *SAMLJ* 65.
205 Section 68 (1)(a) of the *National Credit Act* 34 of 2005; Cronje 2009 *JDFSL* 44.
206 Swales 2016 *SAMLJ* 66.
207 Swales 2016 *SAMLJ* 66.

3.4.3 Electronic Communications and Transactions Act[208]

The *Electronic Communications and Transactions Act* (hereafter ECT Act) is another act that finds relevance in this instance. It determines that the protection of personal information, as detailed in chapter 8 of this Act, refers to information that has been obtained through electronic transactions. Any subscription to the principles set out in this chapter are voluntary but, if subscribed to, the relevant party will have to subscribe to all the principles set out in the act.[209] In other words, compliance with the Act will be either wholly or not at all. It also echoes the requirements of consent and collection purpose prescribed by the PoPi Act and expands on this issue by necessitating that this consent be explicit and in written format.[210] Together with this the ECT Act requires that data controllers keep a record of which information has been shared with third parties as well as the reasoning behind the disclosure.[211]

Contrary to the *National Credit Act* this act does make provision for the regulation of unsolicited commercial communication[212] and this will be noted in the following section.

3.5 Direct marketing

Direct marketing plays an important role in the short-term insurance industry. In order to facilitate a competitive environment insurers make use thereof to approach clients and market their products.[213] Currently the *Financial Advisory and Intermediary Services Act*[214] and *Consumer Protection Act*[215] (hereafter FAIS and

---

208 25 of 2002.

209 Section 50 of the *Electronic Communications and Transactions Act* 25 of 2002; Cronje 2009 *JDFSL* 44.

210 Section 51 of the *Electronic Communications and Transactions Act* 25 of 2002.

211 Section 51 of the *Electronic Communications and Transactions Act* 25 of 2002. Any information that is no longer used or has served its purpose must be destroyed. The personal information that has been collected may then also be used for statistical purposes but only if the information cannot be linked back to a data subject by a third party.

212 Swales 2016 *SAMLJ* 68.

213 Da Veiga and Swartz 2017 *SAIEE* 60.

214 37 of 2002.

215 68 of 2008. The main reasoning behind this legislation relates to the protection of consumer against unfair business practices and to place suppliers and consumers on the same level. See also Swales 2016 *SAMLJ* 66.

CPA) regulate this practice, with additional contributions made by the *Electronic Communications and Transactions Act* (hereafter ECT).[216] According to the Section 11 of the CPA a person's right to privacy includes the right to refuse, request a discontinue or block communications relating to direct marketing.[217] This implies that existing customers have the right to only "opt-out" of marketing communications in this regard but it does not address the issue of private information being sold between companies.[218] In the same breath the FAIS Act only addresses the services rendered in this regard as well as the content and manner in which direct marketing is done[219] whilst the ECT renders unsolicited consumer communications a criminal offence only in some circumstances.[220] Subsequently, these laws merely imply that this practice is somewhat unwelcome.[221]

This position has been amended by the PoPi Act, which eliminates the practice of cold-calling consumers in no uncertain terms.[222] Through Section 69 direct marketing through electronic means has been specifically prohibited unless the data subject in question has consented thereto.[223] It requires a pertinent "opt-in"/"opt-out" action on the part of the data subject which could restrict the marketing and communications' freedom of an insurer to a detrimental degree.[224] Lastly it will also change the persistence in direct marketing attempts towards a specific data subject by restricting this to only one attempt to acquire consent.[225] Should consent not be

---

216 *Electronic Communications and Transactions Act* 25 of 2002; Hamann and Papadopoulos 2014 *De Jure* 49; Da Veiga *et al* 2019 *ICS* 404.

217 Section 11(1) of the *Consumer Protection Act* 68 of 2008; Swales 2016 *SAMLJ* 66; Millard 2013 *THRHR* 619; Da Veiga and Swartz 2017 *SAIEE* 59; Hamann and Papadopoulos 2014 *De Jure* 51.

218 Millard 2013 *THRHR* 619.

219 Section 14 and 15 in Board Notice 80 of 2003 in GG25299 of 8 August 2003 in terms of Section 15 of the *Financial Advisory and Intermediary Services Act* 37 of 2002; Millard 2013 *THRHR* 620.

220 Section 45 of the *Electronic Communications and Transactions Act* 25 of 2002; Swales 2016 *SAMLJ* 68; Hamann and Papadopoulos 2014 *De Jure* 49.

221 Millard 2013 *THRHR* 621.

222 Da Veiga and Swartz 2017 *SAIEE* 60; Millard 2013 *THRHR* 618; Swartz and da Veiga 2016 *ISSA* 12.

223 Section 69 of the *Protection of Personal Information Act* 4 of 2013; Da Veiga *et al* 2019 *ICS* 404.

224 Da Veiga and Swartz 2017 *SAIEE* 59. This would also negatively impact the marketing costs of insurers.

225 Swales 2016 *SAMLJ* 73; Hamann and Papadopoulos 2014 *De Jure* 57; Da Veiga *et al* 2019 *ICS* 404.

obtained through this one attempt a responsible party may not repeatedly contact the data subject asking for this.[226] In the end it is clear that although direct marketing laws exist and regulate this practice by insurers, the current laws offer a patchwork of protection that is not as comprehensive as is necessary.[227] The PoPi Act has tried to remedy this and although it has improved information protection it has offered only broad restrictions and protection.[228] There might therefore be room for improvement.

3.6 Possible changes to the insurance industry

Despite the vast range of legislation currently governing the insurance industry and already regulating the manner in which data subjects and their information are being treated, it is clear that the implementation of the PoPi Act, in and of itself, will still have an impact on this industry. On the one hand it will require the implementation of or upgrade to information safeguarding processes as it relates to personal information under an insurance company's control.[229] This is required through condition seven of the PoPi Act and many companies are investigating various avenues to prevent the unauthorised access to information under their control. In this way short-term insurance companies will guarantee the security of their databases and safeguard against improper information access.[230] This act might also reform the way that personal information is being managed and could see a shift in information processing from paper-based processing to digitization.[231] Another advantage of the PoPi Act conditions is that there will be more clarity regarding what information insurance companies hold, who has access to said

---

226 Swales 2016 *SAMLJ* 73.

227 Swales 2016 *SAMLJ* 83; Millard 2013 *THRHR* 618.

228 Swales 2016 *SAMLJ* 84; Hamann and Papadopoulos 2014 *De Jure* 57.

229 Swartz and da Veiga 2016 *ISSA* 11. The PoPi Act requires that responsible parties have to identify any risks that might exist in the processing of a data subject's information before taking steps towards the correction thereof. This would imply the necessity of a companywide audit or review that short-term insurers have to undertake to identify any problem and correct any problem areas in their processing systems. See also Milo and Ampofo-Anti 2014 *Without Prejudice* 32.

230 Swartz and da Veiga 2016 *ISSA* 11.

231 Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.

information and what is being done with that information.[232] More explicit transparency will be the main consequence and insurance companies will have to regulate the information under their control from start to finish, even extending to where it is under the control of other parties. Written agreements will have to be updated to ensure compliance by all parties.[233] Short-term insurers will have to let data subjects know what information they hold and make sure they have the proper consent to hold said information. This will guarantee sufficient transparency in insurance companies' dealings with personal information whilst also ensuring ethical treatment of data subjects.[234]

On the other hand, this legislation could require infrastructural changes on the part of the insurers to facilitate their compliance which might necessitate information technology investments or the use of third-party processors to guarantee proper regulation and handling of individuals' personal information.[235] This would also have serious cost implications for insurers who do not currently have access to these measures and who would have to explore these options anew.[236] Proper procedures and contingency plans will need to be implemented should unlawful access to personal information be obtained.[237] Furthermore, the terms and conditions of existing agreements with policyholders will need to be reviewed to ensure compliance and data subjects will need to provide insurers with consent should it be necessary. Lastly an Information Protection Officer will have to be appointed and

---

232 Swartz and da Veiga 2016 *ISSA* 11. In this way individuals' rights will be sufficiently protected. Any requests relating to their information need to be attended to and should this not happen they have various remedies available. It will require of insurance companies to review who has access to their information and to what extent this access exists. See also Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.

233 Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.

234 Da Veiga and Swartz 2017 *SAIEE* 59.

235 Swartz and da Veiga 2016 *ISSA* 11.

236 Da Veiga and Swartz 2017 *SAIEE* 59. In order to process personal information insurers will have to implement certain measures to ensure compliance, such as making sure that the data subjects are aware of why their personal information is being collected, upgrading security measures to protect the information of policy holders against unauthorised access, keeping information for a limited duration and ensuring that the information on hand is factually correct. See also Da Veiga 2011 *ISGA* 42.

237 Da Veiga 2011 *ISGA* 42.

registered with the Regulator to oversee an insurer or company's adherence to the act.[238]

3.7 Concluding remarks

Before the enactment of the PoPi Act, information protection legislation did exist but it was more a muddle of legislation that created a hodgepodge of protection.[239] As has been illustrated in this chapter, different laws protect different aspects of both the personal information of a client and the actions of an insurer towards said client. Although the PoPi Act seems not to be as innovative as first believed[240] it does still introduce new minimum standards to be upheld when the personal information of a data subject is accessed and processed by a short-term insurer.[241] Most importantly it offers new guidelines targeted at unsolicited communication.[242] There have been suggestions in the past that with the enactment of the PoPi Act, legislation such as the *Financial Advisory and Intermediary Services Act* and *Consumer Protection Act* should be amended to reference the PoPi Act,[243] as in the case with the *Conduct of Financial Institutions Bill*, but any action in this regard should be handled with care.

Considering that the current legislative position in the short-term insurance industry has now been reviewed, it would be beneficial to further examine the impact of the PoPi Act on insurance practices such as the reporting obligations that might exist for short-term insurers as well as their use of third-party processors. The following chapter will address these issues and provide more clarity in this regard.

238 Da Veiga 2011 *ISGA* 42.
239 Swales 2016 *SAMLJ* 83.
240 Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.
241 Millard 2013 *THRHR* 621. See also Kandeh, Botha and Futcher 2018 *SAJIM* 3.
242 Swales 2016 *SAMLJ* 84.
243 Millard 2013 *THRHR* 621.

Chapter 4: Secondary consequences of the PoPi Act

Current South African legislation necessitates that personal information may only be accessed with the data subject's permission.[244] As discussed in Chapter 2, there are specific conditions that have to be adhered to when personal information is being processed.[245] Whilst the PoPi Act gives effect to the right to privacy,[246] the question arises how the protection afforded by the PoPi Act will affect the reporting obligations[247] placed on short-term insurance companies as well as the third party processors they make use of the execution of their services.[248] In these instances, there is an obligation to protect the personal information of data subjects that has to be balanced with the execution of the insurer's duties.[249] This chapter will explore these secondary consequences of the PoPi Act.

4.1 Reporting obligation imposed on insurers

There are conflicting duties imposed on financial services providers.[250] On the one hand they have a duty of confidentiality[251] towards their clients, which is supported

---

244 The *Promotion of Access to Information Act* also needs to be considered in this instance. In terms of PAIA information held by another person can be accessed in the event that said information is needed to exercise or protect a person's rights. In this way access to records held by institutions, both public and private, can be garnered. This piece of legislation does, however, also provide for legitimate refusal of requests in this regard such as the protection of confidential information of, amongst others, third-parties. See also Leon and Ripley-Evans 2019 https://financialregulationjournal.co.za/2019/04/10/financial-services-litigation-in-south-africa/.

245 Collett et al 2020 http://www.bizcommunity.com/Article/196/751/207083.html See also Kandeh, Botha and Futcher 2018 *SAJIM* 3.

246 Masete 2012 *JICLT* 257. This is done through its protection of personal information and its observance of only justifiable limitations. See also Kandeh, Botha and Futcher 2018 *SAJIM* 2.

247 Masete 2012 *JICLT* 250.

248 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.

249 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 281. Chapter 4 of the PoPi Act, in particular, deals with instances where the processing of personal information will not be in contravention of the Act. It determines in Section 37 that the Information Regulator may provide a responsible party with permission to process certain information should the public interest in the processing of the information be greater than any deemed interference it may create and be to the benefit of the data subject. Section 38 then goes further to note that if information is processed for a "relevant function" by a public entity or in terms of legislation it will also be permitted.

250 Masete 2012 *JICLT* 258.

251 The duty of confidentiality was recognised in the case of *Abrahams v Burns* (1914 CPD 452). See also Millard 2013 *THRHR* 612.

by the right to privacy and which places a duty on financial services providers to protect the privacy and confidential information of their clients.[252] Should personal information then be disclosed by an insurer, said party will be in breach of their contractual duty and will act *contra bonos mores.*[253] On the other hand, an obligation can be created through legislation to disclose personal information.[254]

When it comes to interacting in the digital sphere financial services providers, such as short-term insurance companies, have to consider the risks posed by cybercrimes[255] and have to take note of the various obligations imposed on them through legislation such as the Cybercrimes Bill[256] which was recently passed and the *Financial Intelligence Centre Act* (hereafter FICA).[257] These obligations mainly relate to the reporting of crimes such as fraud and money laundering and, more often than not, involve the information they interact with and keep on hand, which inevitably includes the personal information of clients.[258] In that case the client's right to have their personal information protected is secondary to the public interest that exists and the need to protect the public against criminal activities.[259] Both

---

252 Masete 2012 *JICLT* 248.

253 Millard 2013 *THRHR* 612.

254 Masete 2012 *JICLT* 250. Masete goes further to note that it is important to note that Section 36(1) of the Bill of Rights places a statutory limitation on the right to privacy, which includes the right to financial privacy. All legislation obligating the disclosure of personal information consequently derives its power from Section 36's legitimate limitation of fundamental rights.

255 Collett et al 2020 http://www.bizcommunity.com/Article/196/751/207083.html; Grobler, Jansen van Vuuren and Zaaiman 2013 *JSCI* 33.

256 Miller and Milligan *2019 KPMG: The South African Insurance Industry Survey* 40. For more information regarding South Africa's combatting of cybercrime see Grobler, Jansen van Vuuren and Zaaiman's article "Preparing South Africa of Cyber Crime and Cyber Defence".

257 *Financial Intelligence Centre Act* 38 of 2001. Insurers have an obligation to entertain claims that might arise. It should be noted, though, that their civil obligation to settled claims in accordance with insurance policies are separate from their obligation to report fraud or suspicious transactions. Insurers have a duty imposed on them in terms of the *Prevention and Combatting of Corrupt Activities Act* 12 of 2004, specifically Section 34, to report offenses such as theft, fraud and extortion. Subsection 1 notes specifically that suspicions of fraud regarding amounts in excess of R100 000 need to be disclosed to the police. This duty is placed on a person of authority such as a manager, secretary or chief executive officer, with the question being asked whether a reasonable person would have suspected fraud to have been committed. See also Hardie and Wagner 2017 *Without Prejudice* 17.

258 Collett et al 2020 http://www.bizcommunity.com/Article/196/751/207083.html. Should this duty relate to the personal information of a data subject it may be authorised by the Information Regulator as the public interest will outweigh the possible infringement. See also Millard 2013 *THRHR* 617.

259 Millard 2013 *THRHR* 612.

pieces of legislation, as indicated above, will be addressed below for clarification purposes.

4.1.1 Cybercrime and the Cybercrimes Bill

With the advent of the internet and its expanded use during the 1990s a new form of criminal activity saw creation, namely cybercrime.[260] This term usually refers to crimes committed through technological means such as computers and can include activities like hacking and fraud.[261] Initially, before the inception of specific legislation, offenses in this regard were regulated by the common law,[262] but with the progression of time, laws such as the *Electronic Communications and Transactions Act*[263] (hereafter ECT Act) were formulated to target specific issues that arose.[264]

The main reasoning behind the creation of the ECT Act was to protect electronic communications and data messages, with cybercrime receiving specific attention in Chapter 13 thereof.[265] In short, Chapter 13 criminalizes the unlawful interception of data,[266] unauthorized interference with data,[267] and establishes new crimes such as hacking and cracking.[268] Together with other legislation such as the *Prevention of Organized Crime Act*[269] and the *Financial Intelligence Centre Act*[270] this Act strives to prosecute cybercriminals.[271] It also led to the creation of "cyber-inspectors" who had

---

260 Snail 2008 *JBL* 63. The concept of "cybercrime" refers to crimes that deal with intangible property. See also Cassim 2010 *JICLT* 118.

261 Snail 2008 *JBL* 63.

262 The problem with the common law was that it offered limited protection when it came to online crimes of theft and treason, amongst others. See Snail 2009 *JILT* 3.

263 *Electronic Communications and Transactions Act* 25 of 2002.

264 Cassim 2010 *JICLT* 118. See also Snail 2009 *JILT* 2; Snail 2008 *JBL* 63; Van der Merwe *et al Information Communication and Technology Law* 74.

265 Cassim 2010 *JICLT* 119. See also Grobler, Jansen van Vuuren and Zaaiman 2013 *JSCI* 35; Masete 2012 *JICLT* 256. It is important to note that cybercrimes cannot be limited to only that which has been stipulated in the ECT Act. See also van der Bank 2012 *EJBSS* 82.

266 Section 86(1) of the *Electronic Communications and Transactions Act* 25 of 2002.

267 Section 86(2) of the *Electronic Communications and Transactions Act* 25 of 2002.

268 Snail 2008 *JBL* 66. See also Snail 2009 *JILT* 6; Van der Merwe *et al Information Communication and Technology Law* 75.

269 *Prevention of Organized Crime Act* 121 of 1998. See also van der Bank 2012 *EJBSS* 82.

270 *Financial Intelligence Centre Act* 38 of 2001.

271 Snail 2009 *JILT* 7 9.

the authority to seize information relevant to cybercrime investigations.[272] The problem with this was the fact that the right to privacy, protected under Section 14 of the Constitution,[273] and the right to property, as held under Section 25 of the Constitution, could be infringed upon should these actions be carried out.[274] The jurisdictional prosecution of these crimes was another issue in need of clarification, due to the nature of cybercrime. Under Section 90 of the ECT Act it was determined that South African courts would have jurisdiction to try crimes committed in this regard in instances ranging from the actual crime being committed in South Africa to said crime even just being planned in South Africa.[275]

In the end the provisions in the ECT Act were commendable in their efforts to regulate cyber activities[276] but there was definitely room for improvement. The imposition of harsher consequences for cybercrimes[277] and the actual appointment of cyber-inspectors, as created under this Act were definitely at the top of that list.[278]

A few years after the introduction of the ECT Act the notion of cybercrime was further investigated and protection for offenses committed in this regard was expanded upon through the Cybercrimes Bill.[279]

This Bill was passed by the National Council of Provinces on the 1st of July 2020 but is yet to be signed into law by the president. It regulates various actions relating to

---

272 Cassim 2010 *JICLT* 119. See also Snail 2009 *JILT* 9.

273 *Constitution of the Republic of South Africa*, 1996.

274 Cassim 2010 *JICLT* 119.

275 Snail 2008 *JBL* 67. See also Papadopoulos and Snail *Cyberlaw @ SA III* 344.

276 Snail 2008 *JBL* 69. See also Snail 2009 *JILT* 11. It was believed that with the creation and promulgation of personal information protection legislation (as in the form of the PoPi Act) the ECT Act would be affected without a doubt. As a starting point the provisions in the ECT Act that correlate with this protection would be replaced. Currently the ECT Act deals with personal information in Section 50 and 51 and determines how personal information may be processed. Adhering to these principles are voluntary, though. See Cassim 2010 *JICLT* 123; Van der Merwe *et al Information Communication and Technology Law* 368; Papadopoulos and Snail *Cyberlaw @ SA III* 299.

277 Cassim 2009 *PELJ* 68. It has been stated that the penalties imposed under the ECT Act is not sufficient to alone curb offences committed in this regard. See also Cassim 2010 *JICLT* 119; Van der Merwe *et al Information Communication and Technology Law* 78.

278 Van der Merwe *et al Information Communication and Technology Law* 80.

279 *Cybercrimes Bill* [B6-2017].

cybercrimes, from unlawful access to information to cyber fraud and - forgery.[280] This Bill requires that financial institutions report cybercrimes to the relevant authorities and assist them however possible, as required.[281] This involvement may vary from providing active assistance during the course of authorities' investigations and their handling of cybercrimes to the storing and safeguarding of relevant information. According to the Bill, in the event that it comes to the attention of a financial institution that its computer system is used to commit an offence in terms of Chapter 2 Part 1, it should inform the South African Police Service within 72 hours and safeguard any relevant information that would assist with investigating the aforementioned offence.[282] The offences in question will be stipulated by notice in the *Gazette* which will also have to note the way in which these offences have to be reported.[283] By not adhering to these reporting obligations a financial institution may make itself guilty of an offence. If found guilty per this legislation, offenders could be faced with imprisonment for up to fifteen years or a fine per the court's discretion, depending on the severity of the offence.[284] It is important to also note that this Chapter does not apply to any financial sector regulators or any functions performed by the South African Reserve Bank in terms of Section 10 of the *South African Reserve Bank Act* 1989.[285] Should the above not be adhered to, the applicable financial entity could find itself subject to a fine of up to R50 000.[286]

---

280 Bhagattjee, Govuza and Sebanz 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html.

281 Miller and Milligan *2019 KPMG: The South African Insurance Industry Survey* 40.

282 Section 54 (1) of the *Cybercrimes Bill* [B6-2017]. The *Cybercrimes Bill* does not only regulate the penalties that may be imposed on offenders but also imposes obligations on financial services providers such as short-term insurers in relation to reporting cybercrimes and assisting with cybercrime investigations by safeguarding evidence in this regard. See also Bhagattjee, Govuza and Sebanz 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html.

283 Section 54(2) of the *Cybercrimes Bill* [B6-2017].

284 Bhagattjee, Govuza and Sebanz 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html. See also Section 54(3) of the *Cybercrimes Bill* [B6-2017].

285 *Cybercrimes Bill* [B6-2017].

286 Bhagattjee, Govuza and Sebanz 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html.

4.1.2 Financial Intelligence Centre Act[287]

The *Financial Intelligence Centre Act* (hereafter FICA) must also be considered in this instance. FICA is known in the vernacular as the anti-money laundering and anti-terrorist financing legislation.[288] It has as its main goal the monitoring and resolution of money-laundering in South Africa and imposes certain obligations on financial services providers which include the identification of customers, the record keeping of transactions, the reporting obligations that exist and the training of employees in accordance with the provisions set out in FICA.[289] Financial services providers, specifically, have certain reporting obligations imposed on them by the act. It requires that suspicious and unusual transactions or activities be reported to the Financial Intelligence Centre and has, through recent amendments, worked to expand the definition of "accountable institutions" as found in the first schedule to include short-term insurance companies.[290] This places an obligation on these companies to ensure sufficient protocols and procedures to comply with the duties imposed by FICA.

In terms of Section 28, applicable institutions have to report relevant cash transactions within a two-day period to the Financial Intelligence Centre.[291] Said transactions can then be made up of one transaction of R24 999.99 or more than one transaction totalling R24 999.99. Important to understand is that Section 29 relating to the reporting of dubious transactions is applicable to all parties that either have a business, manage a business or are employed by one, whilst Section 28A, relating to property that is suspected of having terrorist ties and the reporting thereof, is only applicable to the institution that has been identified in the act.[292]

---

287 *Financial Intelligence Centre Act* 38 of 2001.

288 Hardie and Wagner 2017 *Without Prejudice* 18.

289 *Financial Intelligence Centre Act* 38 of 2001. Part 3 of Chapter 3 of the act refers specifically to reporting obligations that exist in the event of cash transactions in excess of R24 999.99 as stipulated in Section 28, property that holds ties to terrorist activities in terms of Section 28A and transactions of a dubious nature per Section 29. Should information relating to any of the aforementioned become known to Financial Services Providers such as short-term insurers they have to share this information with the relevant parties. See also Masete 2012 *JICLT* 257.

290 Hardie and Wagner 2017 *Without Prejudice* 18; Millard 2013 *THRHR* 618.

291 *Financial Intelligence Centre Act* 38 of 2001.

292 *Financial Intelligence Centre Act* 38 of 2001.

Section 29 is of utmost importance and places an urgent reporting obligation on financial services providers to make the necessary authorities aware within 15 days after they have become aware of suspicious activities. Should they fail to heed this duty the penalty imposed may vary between a fine of up to ten million rand or imprisonment for a period of up to 15 years.[293]

It is clear that this reporting obligation stands in direct contrast to the privacy expectations of data subjects from financial services providers regarding their information, be it of a personal or financial nature.[294] Finding a balance between these duties will require immeasurable effort and dedication from financial services providers.[295]

4.2 Regulation of third-party processors

A normal occurrence in the short-term industry is the outsourcing of information processing and storage to third party processors. These processors act on behalf of the insurer and assist with various duties but due to the nature of the PoPi Act, their involvement begs scrutiny and may cause problems. This is due in large part to the fact that by making use of third-party service providers to process the personal information of data subjects, responsible parties such as short-term insurers are creating possible weak points that may expose clients to information-related risks.[296] As such, it is important to understand what is required in terms of the PoPi Act to ensure that data subjects' personal information is protected.

Third-parties and data warehouses often process and store information on behalf of insurance companies.[297] Their responsibilities may also include mass communication

---

293 Hardie and Wagner 2017 *Without Prejudice* 18.

294 Masete 2012 *JICLT* 248. Masete also notes that currently there exists no legislation governing the privacy of clients' financial information. These financial services providers are required to adhere to the notions of confidentiality when it comes to their customers' personal and financial information but this duty of confidentiality often conflicts with a disclosure duty that can be imposed in terms of existing legislation such as the *National Credit Act*.

295 Masete 2012 *JICLT* 258.

296 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.

297 Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.

with data subjects and premium collection on behalf of the financial services provider.[298] When it comes to their appointment and the role they play in the processing of a data subject's personal information, the latter does not normally play a role.[299] As a result, this information transfer has to be carefully considered. It can only be done in the event that the third-party will be subject to the PoPi Act, thus limiting the transfer of information across borders.[300] To account for this the PoPi Act explicitly states that any information processed by an operator on behalf of a responsible party may do so only per the knowledge and authorisation of the responsible party.[301] This requires the existence of a contractual relationship[302] of a written nature[303] between the responsible party and the third party, also known as the operator.[304] This contract will govern the operator's actions[305] and will set out the nature of the relationship between the parties.[306]

4.2.1 Third-party operational mandate

In order to be valid, the mandate as previously referenced must firstly include the eight conditions regulating the lawful processing of personal information and previously examined in Chapter 2.[307] This implies that the data subject has provided the necessary consent to the sharing of their information[308] and that any information provided to third-parties and intermediaries can only be used for the originally intended purpose.[309] It may not be sold or change hands more than necessary and

---

298 Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.
299 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 285.
300 Section 72 of the *Protection of Personal Information Act* 4 of 2013.
301 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 285.
302 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.
303 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.
304 Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.
305 Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.
306 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.
307 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 287.
308 Section 72 of the *Protection of Personal Information Act* 4 of 2013.
309 Rodrigues 2012 www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286.

each processing iteration must be accountable to the client in question.[310] This also requires specific indication that the sharing of information is necessary to uphold the contract between the data subject and responsible party, that the transfer is necessary for the fulfilment of a contract between the third-party and responsible party and that it is in the interest of the data subject or to the benefit of the data subject.[311]

Considering the complex relationship between third-parties and responsible parties, it is also advisable for the mandate that exists between the two to specify that the responsible party will provide authorisation for information processing by written instruction only.[312] As a result, the processor will only be able to act on behalf of the responsible party and only per its explicit authorisation,[313] limiting its interactions with data subjects' personal information and reigning in its previously-held free access. This mandate will also have to confirm that the information in question will be treated with the utmost confidentiality and will only be disclosed should it be required by law or for proper performance of functions by the operator.[314] In the event that a third-party does not adhere to the PoPi regulations, the responsible party will ultimately be held responsible.[315]

---

310 Rodrigues 2012 www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286. It is important to note that the responsible party and the third-party have the same compliance requirements. Should a complaint arise due to the processing of client's personal information they will have to prove that the proper consent had been obtained from the data subject.

311 In the event that it is not reasonably possible to obtain consent from the data subject it is necessary to indicate that had it been possible, they would have provided it. See Section 72 of the *Protection of Personal Information Act* 4 of 2013.

312 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.

313 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 287. It is prudent to set out exactly what is expected from the third-party processor as well as how this will be attained. See also Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.

314 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 287. Section 20 of the PoPi Act also states that any information dealt with in this regard must be viewed as confidential and may only be shared with the responsible party except where its disclosure is required by law or as part of the operator's performance of its functions.

315 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.

This mandate will also have to clarify that the security requirements per Section 19 will be adhered to, as well as indicate the extent to which this will be done.[316] The safeguarding of personal information is of utmost importance and needs to be ensured throughout by all the relevant parties. This implies that the proper level of security needs to be adhered to[317] and will place a duty on the responsible party to ensure that the operator is at all times compliant with the PoPi Act and adheres to their agreement.[318] This will also require that the operator needs to ensure that the information under their care is contained in a lawful manner and that the processing limitations that exist around this information are adhered to every step of the way.[319] This will require additional administration and regulation on the part of the insurance company to confirm compliance with the PoPi Act, transparency and accessibility so that clients may inspect their information and proper safeguarding of the information in question.[320] To date, there has not yet been any directives issued regarding the extent to which responsible parties should have insight into the security measures of the relevant third parties or their compliance with the Act.[321] All in all, this mandate requires the maintenance of sufficient technical and organisational measures to safely process a data subject's personal information.[322]

Lastly the agreement between a third-party processor and the responsible party needs to indicate the process to be followed in the event that unauthorised access has been granted to data subjects' personal information.[323] In the event that a data breach occurs, the third-party is legally required to notify the responsible party, who must in turn notify the Information Regulator and data subject.[324] The mandate itself

316 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 287.
317 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.
318 Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.
319 Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.
320 Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.
321 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.
322 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.
323 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 287.
324 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.

will govern the exact notification process and indicate what the notification period will be.[325]

At the end of the day the nature and volume of personal information being processed by the third party will have to be considered to establish the responsible party's involvement and govern the third-party's actions.[326] As previously mentioned, this may place additional administrative requirements on the relevant financial services providers but will ultimately be necessary in the protection of data subjects and their information and the adherence to their responsibilities by insurers.[327]

4.3 Summary

Through this chapter the secondary consequences of the PoPi Act have been investigated. It is clear that short-term insurers will have to carefully consider the determinations of this Act in order to, firstly, balance the protective rights bestowed upon data subjects with the reporting obligations imposed on them by external legislation and secondly, consider the role that third-party processors play in their client-workings and the extent to which the latter access client information.

Considering the thorough investigation done so far in this study on the local protection of personal information and the consequences of the PoPi Act, it is now necessary to examine the international community and the attention they have afforded personal information protection over the years. The next chapter will consider how and why this protection developed as well as briefly discuss the initial impact of this protection on short-term insurers.

---

325 Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.

326 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.

327 Miller and Milligan 2019 *KPMG: The South African Insurance Industry Survey* 40.

Chapter 5: International regulation of data protection

5.1 Consideration of international law

Information is one of the few things in life that is beholden to no borders.[328] It moves with great ease between countries and has become a commodity in its own right. As a result, it is necessary to not only know and understand how information, and personal information in particular, is being protected in South Africa but to also understand how the international community views and has developed personal information protection. This will be investigated during the course of this chapter.

The South African Constitution,[329] through its regulations and determinations, strives to develop legislation in conjunction with international law.[330] In this way inspiration may be drawn from the international community on how certain issues can be addressed.[331] In the past, members of the judiciary have often looked to international legislative positions to substantiate their views or provide clarity where necessary[332] although there have also been instances where this legal discipline has led to unfamiliar terrain.[333] Section 39 of the Constitution, in particular, determines that international law must be considered by a court or tribunal when the Bill of Rights is being interpreted.[334] In turn this created an obligation to include international law in the interpretation of rights such as the right to privacy.[335] The PoPi Act, in particular, also explicitly notes that international law has to be taken

328 Heyink 2013 *Law Society of South Africa* 30.

329 *Constitution of the Republic of South Africa*, 1996.

330 Dugard 1997 *EJIL* 92.

331 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 259.

332 When it comes to the consideration of international law the courts are not limited to those instrument that are binding on South Africa. On more than one occasion the Constitutional Court has determined that both "binding" and "non-binding" international law may be applied such as in the case of *S v Makwanyane* 1995 (3) SA 391 (CC) para 36 and 37.

333 Dugard 1997 *EJIL* 92.

334 Section 39 of the *Constitution of the Republic of South Africa*, 1996. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 259. This section is read in conjunction with section 231 to 233 of the Constitution. See also *Glenister v President of the Republic and Others* 2011 (7) BCLR 651 (CC) and 2011 (3) SA 347 (CC).

335 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 259.

into account when personal information is processed,[336] which supports the view that it plays a valuable role in the South African legal sphere and holds much reverence.[337] By examining the manner in which the international community protects and regulates personal information (on various levels such as insurance) one might be able to better understand and mitigate the impact of the PoPi Act on short-term insurers in South Africa.

5.2 Development of information protection

With the increased use of information and technology during the 1970s and their interdependence on one another, privacy concerns grew and created a need for legislative protection in this regard.[338] By the 1980s the realisation had dawned that information would require protection at more than just a national level.[339] Due to the emerging international market which necessitated the transfer of information across borders, regulation was required at multiple levels and in turn called for uniform international standards to be created.[340] Eventually, with the dawn of the 1990s, the push to protect personal information saw increased encouragement through the enactment of various pieces of international legislation seeking to limit the movement of personal information across borders.[341] Since then the importance of protecting information has received much attention.[342] Many countries have adopted principles into their legal systems to promote the realisation of information protection and its ideals although the degree to which these principles have been

---

336 Preamble of the *Protection of Personal Information Act* 4 of 2013. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 259.

337 Dugard 1997 *EJIL* 92. It is also important to note that, by enacting the PoPi Act, South Africa has aligned itself the international position on and regulation of personal information processing. See also van der Bank 2012 *EJBSS* 85.

338 De Bruyn 2014 *IBERJ* 1315. Many also believed that the advancement in technology limited consumers' control over their information. See also Van Ooijen and Vrabec 2019 *JCP* 92.

339 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 151.

340 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 151; Van Ooijen and Vrabec 2019 *JCP* 92.

341 Heyink 2013 *Law Society of South Africa* 30. The importance of information cannot be overstated. It plays a vital role in modern digital society, even to such an extent that it has been deemed a product in and of itself. See Da Veiga *et al* 2019 *ICS* 400.

342 Heyink 2013 *Law Society of South Africa* 30; Milo and Ampofo-Anti 2014 *Without Prejudice* 30.

adopted differs from country to country.[343] Moreover, the manner in which these principles need to be adhered to also differs between countries.[344] This creates a unique playing field.

There are various international documents that have had a profound impact on the development of information protection[345] as well as the PoPi Act.[346] The most influential will be discussed in this chapter.

5.3 Data protection in the European Union

In the European Union the initial reasoning behind data protection did not stem from a need to halt or limit interactions with personal information but rather to guide interactions with personal information and ensure its protection in light of the technological advances of the late 20th century.[347] Their aim was to create a universal standard in data processing and protection whilst not inhibiting the interaction of businesses and states with one another.[348]

5.3.1 General Data Protection Directive of 1995

The European Parliament and the Council of the European Union initially adopted the General Data Protection Directive of 1995 (95/46/EC)[349] (hereafter Directive 1995). This document is one of the most significant international documents on data protection to have ever been published[350] and was passed in consideration of the *European Convention on Human Rights*[351] and the Organisation for Economic Co-operation and Development's guidelines on the protection of privacy and the

---

343 Bygrave 2010 *SSL* 180; Swartz and da Veiga 2016 *ISSA* 9; Cronje 2009 *JDFSL* 43.

344 Bygrave 2010 *SSL* 180.

345 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 151.

346 Luck 2014 *De Rebus* 44.

347 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 262.

348 Luck 2014 *De Rebus* 44.

349 Bygrave 2010 *SSL* 182. This directive was on the protection of individuals with regard to the processing of personal data and the free movement of such data. See also Swales 2016 *SAMLJ* 78.

350 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 190; Swartz and da Veiga 2016 *ISSA* 10; Cronje 2009 *JDFSL* 43.

351 This is formally known as the Convention for the Protection of Human Rights and Fundamental Freedoms (1953). See also van der Bank 2012 *EJBSS* 78.

transfer of information across borders.[352] While Article 8 of the *European Convention on Human Rights* revolutionised the right to have one's private life, home and correspondence respected,[353] the Organisation for Economic Co-operation and Development's guidelines regulated the transfer of information across borders.[354] It subscribed to certain basic principles which actively steered data processing[355] and, while these principles were not binding in and of themselves, they were accepted by the member states of the European Union and incorporated into their subsequent data protection regulations as the minimum standards to be upheld.[356]

The purpose of Directive 1995 was to reconcile the free flow of personal data between the member states of the European Community but to also ensure a "high level of protection" for the fundamental rights and freedoms of individuals, in particular the right to privacy.[357] It aimed to regulate the processing of personal information by both the public and private entities through either manual or automated means[358] and was binding on all member states although it did not hold reference to the activities of the state in terms of criminal matters, public security or defence.[359] In addition, it determined that information processed by a third-party

---

352 Safari 2017 *SHLR* 812. See also Cate 1995 *ILR* 431; Da Veiga and Swartz 2017 *SAIEE* 58; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

353 Safari 2017 *SHLR* 812.

354 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 123. These guidelines are not stagnant in nature and are continuously reviewed, with the last update occurring in 2013.

355 These principles are as follows: collection limitation principle; data quality principle; purpose specification principle; use limitation principle; security safeguard principle; openness principle; individual participation principle; accountability principle. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 263; Principle 7 to 14 of the Organisation for Economic Co-operation and Development guidelines of 1980.

356 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 123. See also Cate 1995 *ILR* 431.

357 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 196. This directive sought to harmonise the protection of basic human rights without inhibiting the "free-flow" of information. In this way member states could interact with one another without undue restrictions in place. See also Safari 2017 *SHLR* 812. At the same time, it was created as a means of helping and guiding the European Union's member states in enacting their own information protection legislation to ensure the protection of individuals' basic rights. See also Swales 2016 *SAMLJ* 78.

358 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 264.

359 Bygrave 2010 *SSL* 182. Subjecting the latter to data protection principles modelled in the directive was up to each state.

in another country should not interfere with the rights granted to European citizens.[360]

Directive 1995 is quite encompassing in its protection of data.[361] It determined that "processing" of data occurs when data is collected, recorded, stored, used or amended through automated or manual means in a single or multilevel operation and viewed "personal data" as any information with regards to an identified or identifiable person.[362] Consequently, the processing of data was encouraged in a manner that subscribed to the notion of fairness and lawfulness whilst emphasizing that data could not be collected for vague, nonsensical reasons.[363] At the same time, consent was vital to any interactions with personal data.[364] Data subjects had to be aware at all times if their information was being collected and by whom.[365] Data controllers had to inform the relevant supervisory authorities before any information was processed[366] and any complaints relating to the information that had been processed, the manner in which it was done or any relevant details would be addressed by this authority.[367] This directive also subscribed to the requirements that only necessary data should be kept for no longer than necessary.[368] Article 6, in particular, noted that the data controllers would ultimately be held responsible should these principles not be complied with.[369] Interestingly, Directive 1995 did not make provision for a singular regulation of liability but rather left the details for the

---

360 Safari 2017 *SHLR* 812. The right to privacy was held as central to the realisation of this directive.

361 Swales 2016 *SAMLJ* 78.

362 Cate 1995 *ILR* 433.

363 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 264.

364 Directive 1995 emphasized the idea that data may only be processed after having received consent from the data subject. This consent had to be accurate and limited to the intended scope of collection. Information processing pertaining to a data subject's health, religion, opinions or race required written consent from the data subject. See also Cate 1995 *ILR* 433.

365 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 264.

366 Cate 1995 *ILR* 435. Cate goes further to note that this is done by indicating who will access the information, where they are situated, what the processing purpose is, whether third-party operators will have access to the information, if it will be transferred across borders and how it will be protected.

367 Cate 1995 *ILR* 436.

368 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 264.

369 Article 6 of the General Data Protection Directive of 1995 (95/46/EC). See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 264.

determination and enforcement thereof up to the member states.[370] It also had a profound impact on other countries due to its regulation of transborder movement of information.[371] In this way it guaranteed that recipient countries had to have sufficient data protection measures in place before receiving and processing data.[372]

It is clear that Directive 1995 played a vital role in developing data protection measures. Due to the expansion of electronic networks and the increasingly global nature of information[373] this became necessary to ensure progression in society and technology. The reality is that information is not limited by borders and boundaries and is pervasive in its nature.[374] Directive 1995 therefore played an invaluable role in laying the groundwork for data protection.

5.3.2 General Data Protection Regulation

As previously mentioned, Directive 1995 paved the way for personal information protection but in 2012 the European Union saw it necessary to reform some of its principles due to the advancement in technology and its subsequent impact on the manner in which information was accessed and processed.[375] Directive 1995 also did not make provision for the uniform implementation of its principles by all member states, which was seen as a problem in need of fixing.[376]

In May of 2018 the European Union passed what would become known as the General Data Protection Regulation 2016/679 (hereafter GDPR), which repealed Directive 1995[377] and was applicable on all member states.[378] It recognised the right to privacy as an essential human right and sought to protect the personal information of all European Union members, regardless of where they were based

---

370 Safari 2017 *SHLR* 824.
371 Bygrave 2010 *SSL* 183.
372 Bygrave 2010 *SSL* 183.
373 Cate 1995 *ILR* 441; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.
374 Cate 1995 *ILR* 441.
375 Safari 2017 *SHLR* 811; Swartz and da Veiga 2016 *ISSA* 10.
376 Safari 2017 *SHLR* 811.
377 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.
378 Goddard 2017 *IJMR* 703; Da Veiga and Swartz 2017 *SAIEE* 57; Van Ooijen and Vrabec 2019 *JCP* 92; Goddard 2017 *IJMR* 704.

or where the processing occurred,[379] whilst simultaneously determining new regulations pertaining to the protection of personal data.[380] Important issues such as the advancement in technology, globalisation of individuals' interactions and the effective protection of personal information also saw mention in the GDPR.[381]

Although similar to Directive 1995 there are some key differences that should be noted. Firstly, its definition of "personal data" was broadened to account for the constant change in what was deemed "personal information" due to technological advancements.[382] Together with this the idea of "consent" was expanded[383] by requiring explicit acquiescence on the part of the data subject and which afforded them more power to regulate by whom their personal data would be used.[384] The GDPR has also granted data subjects the ability to access their personal data,[385] to request that their data be erased[386] and has expanded its protection of "special information" to include genetic and biometric data.[387] Finally, it necessitated that the relationship between data controllers and – processors had to be contractually regulated to ensure accountability[388] and set forth a requirement that impact assessments had to be done in instances where information would be processed through any means that could expose a data subject or their personal information.[389] Most notably the GDPR is based on six underlying principles which govern its

---

379 Goddard 2017 *IJMR* 703. Goddard further notes that the GDPR expands the territorial limits of personal information protections, which will require active oversight both in- and outside of the European Union. See also Van Ooijen and Vrabec 2019 *JCP* 92.

380 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265. The GDPR also highlighted the need for individual control over personal data, which was one of the drives behind its creation. See also Van Ooijen and Vrabec 2019 *JCP* 92.

381 Safari 2017 *SHLR* 821.

382 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265.

383 This cannot be granted through coercion, must relate to the processing of the information at hand and has to be informed. See also Goddard 2017 *IJMR* 704. By providing active consent to the use of personal information a data subject also indicates that they understand the consequences of their approval. See also Van Ooijen and Vrabec 2019 *JCP* 100; Swartz and da Veiga 2016 *ISSA* 10.

384 Article 7 of the General Data Protection Regulation 2016/679. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265; Goddard 2017 *IJMR* 703.

385 Article 15 of the General Data Protection Regulation 2016/679.

386 Article 17 of the General Data Protection Regulation 2016/679.

387 Safari 2017 *SHLR* 826; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

388 Article 28 of the General Data Protection Regulation 2016/679. See also Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265.

389 Article 35 of the General Data Protection Regulation 2016/679.

protection of personal information, namely fairness and lawfulness, purpose limitation, data restriction, accuracy, storage limitation, and integrity and confidentiality.[390] These are supported by the notion of transparency[391] and accountability, which ensures accessibility to the relevant information and consequences for non-compliance.[392]

There are, however, still some issues that require consideration. The existing information protection guidelines, as promoted by Directive 1995, have led to differing interpretations by member states.[393] This is due to the fact that while directives are extensive, goal-centric legislation which provide recommendations to member states pertaining to a specific topic, they are dependent on the promulgation of similar legislation by the member state itself.[394] In contrast to this, a regulation is legislation of a restricting nature which is directly enforceable on member states without the need for them to promulgate legislation of a similar nature.[395] Due to the nature of Directive 1995 member states had thus been allowed to regulate themselves which led to conflicting interpretations and executions of Directive 1995's principles and which created a warped view of data protection and privacy. The GDPR does not allow for this anymore and will require conformation in the manner that personal information is dealt with.[396] There does, however, remain some leeway for member states' own expression in certain matters, such as the requirements for data protection officer appointments,[397] but for the most part they will be required to enforce the principles as set out in the GDPR. As previously mentioned, Directive 1995 also did not make provision for a singular regulation of liability but rather left the details for the determination and enforcement thereof up

---

390 Goddard 2017 *IJMR* 703. Most notably the GDPR requires that data subjects have to be informed, before any information processing takes place, of the reasoning behind the processing as well as who will be processing the information and for how long the information will be kept. See also Van Ooijen and Vrabec 2019 *JCP* 96.

391 There must exist a reasonable degree of "openness" in the communication between the people processing the information and the data subject. See also Goddard 2017 *IJMR* 704.

392 Goddard 2017 *IJMR* 703.

393 Goddard 2017 *IJMR* 704.

394 Safari 2017 *SHLR* 820.

395 Safari 2017 *SHLR* 821.

396 Goddard 2017 *IJMR* 704; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

397 Goddard 2017 *IJMR* 704.

to the member states. With the repeal of Directive 1995 the GDPR changed this by providing for administrative fines that could be implemented against member states in the event of non-compliance.[398] Lastly, although the GDPR requires that data controllers explain the purpose of the data processing, who will be processing the information and for how long the information will be kept (amongst others) to data subjects, it does not specify how explicit this explanation has to be, nor does it indicate how this explanatory duty has to be fulfilled.[399]

It is clear that the GDPR is evolutionary in the manner which it re-establishes the balance between organisations and individuals when it comes to the processing of personal information. It has improved the standards of operation and brought them in line with basic ethical and good practice principles,[400] but will require time and effort to ensure that its enforcement is as effective as its theoretical grounding.

5.4 Data protection in the United Kingdom

Traditionally speaking the right to privacy is not recognised in English Common Law.[401] In the past it was protected through indirect remedies established to protect an individual against the misuse of information or the unauthorised disclosure of said information[402] but in 1998 the United Kingdom passed the *Data Protection Act*[403] to regulate the processing of personal information.[404] This vital piece of legislation sought to change the indirect protection afforded by English common law by providing a more direct and forceful protection of privacy and personal information.[405] Interestingly, although the United Kingdom is in the process of

---

398 Safari 2017 *SHLR* 824.

399 Van Ooijen and Vrabec 2019 *JCP* 96, 97; Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237; Goddard 2017 *IJMR* 704.

400 Goddard 2017 *IJMR* 705.

401 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 245. See also van der Bank 2012 *EJBSS* 84.

402 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 245.

403 *Data Protection Act* (1998); Da Veiga *et al* 2019 *ICS* 400.

404 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 270; Swales 2016 *SAMLJ* 78.

405 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 245.

leaving the European Union, this legislation will apply in conjunction with the GDPR to regulate the processing of data and personal information.[406]

Currently this act is the main source of data protection in the United Kingdom and was adopted due to both national and international pressure on the government at the time.[407] Not surprisingly it is an ideal example of a specific country's compliance with Directive 1995, which spearheaded the protection of personal data.[408] Much of what is said in the GDPR and Directive 1995 is echoed in this act, especially as it pertains to the importance of data processing being done lawfully, fairly and with the data subject's consent, the notion that data may not be acquired for undefined purposes and the fact that the data subject must be allowed unrestricted access to their information.[409] This act does not, however, mention the protection of privacy outright and includes this protection only so far as it pertains to the processing of information.[410]

When the content of this act is investigated the similarities with and differences to the PoPi Act become apparent. Most notable is that while the PoPi Act provides for the regulation of direct marketing the *Data Protection Act* does not, which has necessitated the implementation of additional legislation in the form of the *Privacy and Electronic Communications Regulation*.[411] This protects data subjects against unsolicited direct marketing[412] and while the *Data Protection Act* provides for the creation of an Information Commissioner to oversee compliance with legislation, the South African equivalent is the Information Regulator.[413] At the same time the *Data*

---

406 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 270.

407 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 251, 252.

408 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 271.

409 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 271.

410 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 252, 387. Constitutional protection of the right to privacy is provided by the *Human Rights Act* of 1998.

411 The Privacy and Electronic Communications (EC Directive) Regulation 2003. It determines that no recording of calls or communication with clients (of a marketing nature) may be done without prior approval from the client. This is mirrored in Chapter 8 of the PoPi Act. See also De Bruyn 2014 *IBERJ* 1316, 1320. The Privacy and Electronic Communications Regulation sets out detailed privacy rules with regard to electronic communication. As a result, individuals may be contacted but only if they have provided the necessary consent beforehand. See Da Veiga *et al* 2019 *ICS* 404.

412 De Bruyn 2014 *IBERJ* 1320.

413 De Bruyn 2014 *IBERJ* 1318. See also van der Bank 2012 *EJBSS* 84; Swales 2016 *SAMLJ* 78.

Protection Act does not include the same data breach notification requirements as the PoPi Act, although the *Privacy and Electronic Communications Regulation* does require the Information Regulator to be notified should a data breach in this regard occur.[414]

On the other hand, the PoPi Act echoes the *Data Protection Act's* requirement for explicit consent[415] to have been obtained from a data subject before their information is processed and expands upon this by stipulating that data controllers[416] have to keep careful record of the details surrounding the consent that has been provided. The PoPi Act also contains similar terminology to the *Data Protection Act*, as illustrated by the shared use of the terms such as "data subject", and both pieces of legislation have incorporated principles from the Guidelines on the Protection of Personal Information and Trans-border Flow of Personal Data, or the OECD principles.[417] Should the conditions of the *Data Protection Act* be contravened, compliance may be forced through the issuing fines (of up to £500 000) by prosecuting the applicable party or by serving them with enforcement notices,[418] similar to the PoPi Act.

From a data protection point of view, the protection afforded to the right to privacy by this Act is not revolutionary. In the United Kingdom data protection is essentially

---

414 Da Veiga *et al* 2019 *ICS* 402.

415 Should information be obtained from a third-party this will not constitute consent and direct marketing in this regard will be prohibited. See also De Bruyn 2014 *IBERJ* 1320. Schedule 3 Section 4 of the *Data Protection Act* also states that the disclosure of personal information to a third-party may only be done once the data subject has provided their consent to this. As a result, many data controllers use a privacy notice when personal information is collected. This explains to data subjects how their information will be processed, which allows them to either provide or withhold the required consent. See also Da Veiga *et al* 2019 *ICS* 407.

416 De Bruyn 2014 *IBERJ* 1320. De Bruyn also writes on page 1318 that the *Data Protection Act* has dubbed the processor of the information a "data controller" and requires that data controllers have to be registered with an oversight body, namely the Information Commissioners Office, if they perform specific data processing activities. South Africa's PoPi Act does not currently have a provision equalling this.

417 Da Veiga *et al* 2019 *ICS* 401. The *Data Protections Act* also regulates the processing of personal information for various reasons, excluding domestic use.

418 De Bruyn 2014 *IBERJ* 1320.

provided through legislation and although this Act implements the provisions of Directive 1995, in some respects it seems to be more restrictive.[419]

5.5 Information privacy in the European insurance sector

It has been illustrated throughout this chapter that international data privacy legislation such as the GDPR has changed the manner in which personal information is both viewed and interacted with. On the one hand it has recognised that the right to privacy is an essential human right[420] whilst simultaneously increasing the standards of operation[421] and setting out the new regulations to protect the personal data of individuals.[422] The question remains though, in the context of short-term insurance, how these standards and regulations would translate to practice.

The insurance industry, even at an international level, is often tasked with administering large quantities of sensitive and confidential information.[423] They make use of third-party processors which necessitates that said third-party's actions be governed by the GDPR as well.[424] The problem that has now arisen is that some European insurers have multiple third-party processors with whom they work, which entails an operational mandate (that has been negotiated and accepted) with each third-party.[425] Together with this the GDPR also requires an update in contract terminology and conditions as well as increased record keeping on the manner in which data is processed.[426] This has required both additional time and energy on the part of the insurer.

The processing and settling of claims have also been influenced by the GDPR. When claim documentation is received, both Directive 1995 and the GDPR requires an

---

419 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 387.

420 Goddard 2017 *IJMR* 703.

421 Goddard 2017 *IJMR* 705. For an interesting view on digital privacy in the United Kingdom's insurance sector, see Blakesley and Yallop's article "What do you know about me? Digital privacy and online data sharing in the UK insurance Sector".

422 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265.

423 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045.

424 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 265.

425 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045.

426 Ganotra 2018 *Court Uncourt* 3.

insurer to inform the insured of who is accessing the information, the manner and extent to which this is done as well as acquire their consent and identify any sensitive information that may have been received, which can often delay the claims process.[427] Another issue that has seen the light relates to the fact that multiple parties are involved in the claims process, from brokers to loss adjusters and co-insurers.[428] They all require access to the information in question in order to facilitate the claim and settle any damage, yet the GDPR would see their access restricted in favour of the data subject's protection.[429] A data subject is also entitled to access their information in relation to claims, but whether this right includes access to opinions and analysis by the claim's manager is something that has to be settled on a case by case basis.[430]

Another problem that has been experienced by insurers relates to the notion of accountability as the GDPR obligates insurers to prove the manner in which they ensure accountability for their actions but does not provide guidance on how this is to be achieved.[431] At the same time it also requires the deletion of information which has satisfied its processing justification, but some insurers have found certain types of personal information to be in "legacy systems" and consequently cannot be deleted.[432]

Additionally, maintaining a balance between authorisation and a data subject's protection, accessibility to information held by insurers for legal purposes and

---

427 Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

428 Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

429 Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

430 Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

431 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045. There is also little precedent to be followed in this regard and has left insurers flailing on how to satisfy this requirement. See also Van Ooijen and Vrabec 2019 *JCP* 96.

432 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045. Some legislation has also provided insurers with the right to maintain access to certain information relating to claims. This still needs to be brought in line with the GDPR.

ensuring that any consent received is informed consent has also been cause for concern.[433]

It is clear that application of the GDPR principles still holds many challenges for insurers.[434] Its protection is commendable and its reasoning noble but its real-world enforcement has highlighted some areas of concern, especially in the short-term insurance industry, which will need to be addressed to ensure effective application.

5.6 Conclusion

The South African legislature has deemed it wise to regulate the processing of personal information in accordance with the standards set out by the international community.[435] Whilst this decision does satisfy the Constitutional requirements determined in Section 39 it also acknowledges the advances in this field by other countries.[436] When one considers the conditions set out in the PoPi Act, in relation to the international documents set out in this chapter, it is clear that the latter has had a profound impact on this legislation, both in the content and wording thereof.[437] Due to the relatively "young" status of the PoPi Act and the lack of case law surrounding its interpretation (at the moment), it will be especially important to consider international legislation and case law, in particular, in the interpretation of this act and the execution of its protections.[438]

As the conditions and principles in these national and international regulations mirror one another, it is easy to see that the PoPi Act will play a vital role on the

---

433 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045. The question has now been raised how insurers ensure that the consent they receive is informed, which has necessitated a reconsideration of how data subjects need to be approached. At the same time information required by data subjects to fight claims in court requires manual work on the part of the insurer and has presented challenges.

434 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045; Van Ooijen and Vrabec 2019 *JCP* 96.

435 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 271.

436 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 271.

437 Its conditions and standards are of a similar nature to that currently governing the European Union. See also Luck 2014 *De Rebus* 46.

438 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 272. These sources will be invaluable to the South African judiciary when it comes to the establishment of precedents in this field.

international stage in protecting personal information.[439] This chapter has clearly illustrated the development in and extent to which international legislation such as the GDPR aims to protect personal information. Unfortunately, as illustrated, the practical application thereof on an insurance level has revealed problems which will have to be addressed.[440] Due the similarities between specifically the PoPi Act and the GDPR it is highly likely that the difficulties encountered in the latter's application will also be experienced by South African short-term insurers when they incorporate the PoPi Act into their business practices. Although the development of personal information protection has already come far there will always be room for improvement, as has also been shown in this chapter. Going forward the best possible outcome would consequently be to learn from the international community and improve on their advances as far as possible.

When determining the influence of the PoPi Act on the local short-term insurance industry it is prudent to consider the impact of similar international laws within the same environment. This needs to be done in conjunction with previously discussed points to reach a topical conclusion and will be illustrated in the conclusion following this discussion, as laid out in the next chapter.

439 Luck 2014 *De Rebus* 46.

440 Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045.

Chapter 6: Conclusion

6.1 Introduction

Considering the increasingly digital manner in which people have been interacting with one another in recent years it is no wonder that information has become a valuable asset.[441] Advancements in technology are constantly changing how society interacts with information[442] and personal information in particular has not been left behind. As every person is entitled to the right to the privacy of themself and their identity, personal information processing has received increased attention, mostly due to the advancement in technology.[443] With such an unintended consequence it is no wonder that legislative intervention would be required sooner or later. [444]

The PoPi Act was introduced to regulate the processing of an individual's personal information by setting out requirements for legitimate processing and to ensure that the right to privacy was upheld.[445] It seeks to regulate the processing of personal information by all industries and may have a unique impact on the short-term insurance industry in particular. This is due in large part to the fact that the short-term insurance industry finds itself in the position of handling vast quantities of personal data and processing it into a vast array of information such as risk profiles.[446] Although this information is required to ensure it renders its services effectively the amount and type of information under its control has created questions around its interaction with and adherence to the PoPi Act. This led to the research question that was posed in Chapter 1, mainly how the PoPi Act would affect the short-term insurance industry, especially in light of its interactions with the personal information of clients.

---

441 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3; Swales 2016 *SAMLJ* 49.

442 Kandeh, Botha and Futcher 2018 *SAJIM* 1.

443 Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 3.

444 Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 5.

445 See para 1.1.3 above.

446 See para 3 above.

To answer this question, it became necessary to examine the PoPi Act in its entirety and to consider both what the current legislative position on information processing and privacy was for the short-term insurance industry together with how this would be affected by the PoPi Act.

6.2 Summary of findings

6.2.1 The PoPi Act

Individual privacy is protected through various ways. This includes the protection of a person's personal information. Initially the South African Law Reform Commission believed that individuals should be able to exercise greater control over their information and that this control would coincide with the protection of their privacy.[447] This would ultimately be attained through legislative intervention[448] in the form of the PoPi Act.

This act determines that a data subject has to provide consent before their information may be processed,[449] thereby bestowing data subjects with greater control over who has access to their information and what it is used for. This ensures a deliberate agreement on the part of the data subject.[450] Any processing of personal information must also be done for legitimate purposes by a responsible party[451] and must adhere to the eight conditions stipulated in the act.[452] Should these not be adhered to an individual may be guilty of an offence which might incur consequences ranging from a fine to imprisonment.[453] When it comes to direct marketing the PoPi Act explicitly prohibits the use of personal information for this reason except where a data subject has consented to this beforehand or is an existing customer of the responsible party.[454] Said data subject must also be able to

447 See para 2.1 above.
448 See para 2.1 above.
449 See para 2.2 above.
450 See para 2.2 above.
451 See para 2.2 above.
452 See para 2.4 above.
453 See para 2.3 above.
454 See para 2.2.9 above.

halt correspondence at any moment, should it be necessary.[455] Most notably the PoPi Act also makes provision for the establishment of the office of the Information Regulator. This independent body is tasked with ensuring compliance with the PoPi Act.[456]

6.2.2 Current insurance regulation

The South African short-term insurance industry processes vast amounts of personal information in order to determine and consider a client's risks.[457] The PoPi Act states that this processing is only lawful once it adheres to the eight conditions stipulated in the act, but by examining the legislation currently governing the short-term insurance industry it is clear that limited information protection predates the PoPi Act. The problem with current insurance legislation is that it has created a patchwork of protection[458] that may not protect the personal information of data subjects to the same standards as the PoPi Act.[459] There is legislation currently in development which might improve this position, such as the *Conduct of Financial Institutions Bill*, but this is still in the developmental phase.

6.2.3 Subsequent consequences of the PoPi Act

The PoPi Act has both direct and indirect consequences as it relates to the processing of a data subject's personal information. On one hand it determines that processing must happen with the data subject's express permission but on the other hand it may be processed if a legitimate interest exists that is both reasonable and justified.[460] This places a conflicting duty on short-term insurers. Typically, insurers have a duty to protect the privacy of their clients and any actions violating this duty will have severe consequences.[461] Sometimes, however, insurers also have a duty to disclose personal information. This is imposed through legislation such as the

---

455 See para 2.2.9 above.
456 See para 2.3 above.
457 See para 3 above.
458 See para 3.7 above.
459 See para 3.7 above.
460 See para 4.1 above.
461 See para 4.1 above.

Cybercrimes Bill and FICA which requires that insurers report cybercrimes and assist the authorities however necessary.[462] In order to satisfy this duty insurers have to keep records of transactions and identify customers in certain instances, which contrasts directly with the privacy expectations that clients have of their insurers as it relates to their information, be it of a personal or financial nature.[463]

Initially, the prosecution of cybercrimes was regulated through Chapter 13 of the *Electronic Communications and Transactions Act* but as time progressed it was found to be lacking in certain areas and the need for harsher punishment of cybercrimes[464] led to the drafting of the Cybercrimes Bill.

Another indirect consequence of the PoPi Act relates to the use of third-party operators in the processing of clients' personal information. In the insurance industry it is not unusual for information processing to be outsourced to third-parties acting on behalf of insurance companies.[465] In this regard the PoPi Act requires that a contractual relationship must exist between the parties which stipulates how the third-party may interact with clients' information.[466] In the event that a third-party does not adhere to the PoPi regulations the responsible party will ultimately held responsible.

6.2.4 International protection of privacy

Considering the Constitution's requirement that international law be considered in the interpretation of the Bill of Rights it is important to note how the international community views the protection of privacy and personal information. Directive 1995 paved the way for protecting people's privacy and information. It set out the basic principles for the manner in which data had to be processed[467] but was unfortunately not binding on the members of the European Union. It was, however, seen as the

462 See para 4.1.1 above.
463 See para 4.1 above.
464 See para 4.1.1 above.
465 See para 4.2 above.
466 See para 4.2.1 above.
467 See para 5.3.1 above.

minimum standards to be upheld[468] and later made way for the introduction of the GDPR. This legislation reformed the principles already set out in Directive 1995 and was binding on all member states.[469] It determined that the right to privacy was essential and expanded on the regulations already set out in Directive 1995. The United Kingdom went even further and promulgated their own legislation to regulate the processing of personal information. The *Data Protection Act* consequently echoes much of what is already said in Directive 1995 and the GDPR.[470]

The implementation of legislation such as the GDPR by European insurers has, however, not been problem free. Practical compliance with the determinations of the GDPR has been difficult as it necessitates insurers to perform certain functions, such as obtaining consent from data subjects, without providing guidelines on how this should be obtained or considering the measures that compliance would entail, as in the case with third-party mandates.[471] Certain information has also been found to be vital to the working of said insurers and cannot be deleted once it has been processed.[472]

Due to the correlation between the above-mentioned legislation and the PoPi Act it is clear that it had a direct impact on the creation and wording of the PoPi Act. As a result, it is highly likely that the difficulties encountered in the former's application will also be experienced by South African short-term insurers with regards to their compliance with the PoPi Act.

6.3 Final considerations

The initial reason behind the creation of the PoPi Act related to the regulation of the manner in which personal information was processed by parties such as short-term insurers. This was done to ensure the protection of the right to privacy as well as adherence to responsible information processing practices. When the short-term

468 See para 5.3.2 above.
469 See para 5.3.2 above.
470 See para 5.4 above.
471 See para 5.5 above.
472 See para 5.5 above.

insurance industry in South Africa is considered, compliance with the PoPi Act might seem daunting. This study has, however, found that this industry already has some experience with information protection which has laid the groundwork to comply with the conditions of the PoPi Act. At the same time plans have been implemented to advance the current legislative position in this industry through legislation such as the *Conduct of Financial Institutions Bill* but viewed in isolation it would not provide the same protection as afforded by the PoPi Act.

In conclusion, the South African short-term insurance industry will be affected by the PoPi Act and will have to adapt to ensure their survival in this new legislative environment, but the advantages to themselves and their clients in accepting the PoPi Act might ultimately justify the work it would take to ensure proper compliance with the Act.

BIBLIOGRAPHY

Literature

Blakesley and Yallop 2019 *JICES* 281.

Blakesley IR and Yallop AC "What do you know about me? Digital privacy and online data sharing in the UK insurance sector" 2019 *JICES* 281 – 303

Burns & Burger-Smidt *A commentary on the Protection of Personal Information Act* 4.

Burns Y & Burger-Smidt A *A commentary on the Protection of Personal Information Act* 1st ed (Lexis Nexis Cape Town 2018)

Bygrave 2010 *SSL* 180.

Bygrave LA " Privacy and Data Protection in an International Perspective " 2010 *SSL* 165 - 200

Cassim 2009 *PELJ* 68.

Cassim F "Formulating Specialised Legislation to Address the Growing Spectre of Cyber Crimes: A Comparative Study" 2009 *PELJ* 36 – 79

Cassim 2010 *JICLT* 118.

Cassim F "Addressing the Challenges posed by Cybercrime: A South African Perspective" 2010 *JICLT* 118 – 123

Cate 1995 *ILR* 431.

Cate FH " The EU Data Protection Directive, information privacy and the public interest " 1995 *ILR* 431 - 444

Coetzee 2014 *Without Prejudice* 69.

Coetzee F "The press and PoPi" 2014 *Without Prejudice* 69 - 71

Cronje 2009 *JDFSL* 43.

Cronje FS "A Synopsis of Proposed Data Protection Legislation in SA" 2009 *JDFSL* 43 - 50

Da Veiga 2011 *ISGA* 42.

Da Veiga A "Revealing privacy in South Africa: What you need to know" 2011 *ISGA* 1 - 90

Da Veiga and Swartz 2017 *SAIEE* 56.

Da Veiga A and Swartz P "Personal Information and regulatory requirements for direct marketing: a South African insurance industry experiment" 2017 *SAIEE* 56 - 70

Da Veiga *et al* 2019 *ICS* 400.

Da Veiga A *et al* "Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements" 2019 *ICS* 399 - 422

De Bruyn 2014 *IBERJ* 1315.

De Bruyn M " The Protection of Personal Information (PoPI) Act – Impact on South Africa " 2014 *IBERJ* 1315 - 1340

Dugard 1997 *EJIL* 92.

Dugard J " International Law and the South African Constitution " 1997 *EJIL* 77 - 92

Ganotra 2018 *Court Uncourt* 3.

Ganotra S "GDPR Complaint or Not?" 2018 *Court Uncourt* 2 - 4

Goddard 2017 *IJMR* 703.

Goddard M " The EU General Data Protection Regulation (GDPR): European regulation that has a global impact " 2017 *IJMR* 703 - 705

Grobler, Jansen van Vuuren and Zaaiman 2013 *JSCI* 35.

Grobler M, Jansen van Vuuren J and Zaaiman J "Preparing South Africa for Cyber Crime and Cyber Defence" 2013 *JSCI* 32 – 41

Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" 5039 – 5045.

Grundstrom *et al* "Making sense of the General Data Protection Regulation – Four Categories of Personal Data Access Challenges" in IEEE Computer Society *Proceedings of the 52nd Hawaii International Conference on System Sciences* (8 – 11 January 2019 Honolulu) 5039 – 5048

Hamann and Papadopoulos 2014 *De Jure* 44.

Hamann B and Papadopoulos S "Direct marketing and spam via electronic communications: An analysis of the regulatory framework in South Africa" 2014 *De Jure* 42 - 62

Hardie and Wagner 2017 *Without Prejudice* 18.

Hardie T and Wagner K "Fraud: to report or not to report?" 2017 *Without Prejudice* 17 - 18

Heyink 2013 *Law Society of South Africa* 26.

Heyink M "Protection of Personal Information Guideline" 2013 *Law Society of South Africa* 1-49

Heyink 2015 *De Rebus* 31.

Heyink M "Why are South African lawyers remaining in the dark with PoPi?" 2015 *De Rebus* 31 – 33

Kandeh, Botha and Futcher 2018 *SAJIM* 1.

Kandeh AT, Botha RA and Futcher LA "Enforcement of the Protection of Personal Information (PoPi) Act: Perspective of data management professionals" 2018 *SAJIM* 1 - 9

Luck 2014 *De Rebus* 45.

Luck R "PoPi – is South Africa keeping up with international trends" 2014 *De Rebus* 44 - 46

Masete 2012 *JICLT* 256.

Masete NT "The Challenges in Safeguarding Financial Privacy in South Africa" 2012 *JICLT* 248 - 259

Mezzetti "Data Protection in the Insurance Sector under EU Law" 232 – 237.

Mezzetti CE "Data Protection in the Insurance Sector under EU Law" in Marano P, Rokas I and Kochenburger P (eds) *The "Dematerialized" Insurance* (Springer International Publishing Switzerland 2016) 225 - 238

Millard 2013 *THRHR* 612.

Millard D "Hello, PoPi? On cold calling, financial intermediaries and advisors and the Protection of Personal Information Bill" 2013 *THRHR* 604 - 622

Millard 2018 *THRHR* 375.

Millard D " CoFL and T(CF): Further along the Road to Twin Peaks and a Fair Insurance Industry" 2018 *THRHR* 374 – 392

Millard and Botha 2012 *THRHR* 44.

Millard D and Botha MM " Something's Got to Give: The Future of Financial Advisors and Intermediaries as Employees" 2012 *THRHR* 43 - 69

Millard and Kuschke 2014 *PELJ* 2419.

Millard D and Kuschke B "Transparency, Trust and Security: An Evolution of the Insurer's Precontractual Duties" 2014 *PELJ* 2412 - 2449

Millard and Maholo 2016 *THRHR* 595.

Millard D and Maholo CJ "Treating Customers Fairly: A new name for existing principles?" 2016 *THRHR* 594 - 613

Miller and Milligan 2019 *KPMG*: *The South African Insurance Industry Survey* 39.

Miller M and Milligan D "Data Privacy: Key regulatory challenges emerging from POPIA and the GDPR" 2019 *KPMG*: *The South African Insurance Industry Survey* 39 - 42

Milo and Ampofo-Anti 2014 *Without Prejudice* 30.

Milo D and Ampofo-Anti O "A not so private world" 2014 *Without Prejudice* 30 - 32

Moyo 2020 *De Rebus* 5.

Moyo BJ "An overview of the Protection of Personal Information Act" 2020 *De Rebus* 5 – 6

Mukwakungu and Mbohwa "Short-term insurance company's perspective of Information management and its influence on Continuous Improvement to improve customer satisfaction" 1710 – 1719.

Mukwakungu SC and Mbohwa C "Short-term insurance company's perspective of Information management and its influence on Continuous Improvement to improve customer satisfaction" in Department of Quality and Operations Management *International Conference on Industrial Engineering and Operations Management* (11 – 13 April 2017 Rabat, Morocco) 1710 - 1721

Papadopoulos and Snail *Cyberlaw @ SA III* 345.

Papadopoulos S and Snail S *Cyberlaw @ SA III* 3rd Edition (Van Schaik Publishers 2012)

Rabenowitz *et al The South African Financial Planning Handbook* 57.

Rabenowitz P *et al* (eds) *The South African Financial Planning Handbook* 16th ed (Lexis Nexis Durban 2018)

Reinecke, van Niekerk and Nienaber *South African Insurance Law* 22.

Reinecke MFB, van Niekerk JP and Nienaber PM *South African Insurance Law* 2nd ed (Lexis Nexis Cape Town 2013)

Roos 2012 *SALJ* 377.

Roos A "Privacy in the Facebook Era: A South African Perspective" 2012 *SALJ* 375 - 402

Roos *The Law of Data (Privacy) Protection: a comparative and theoretical study* 13.

Roos A *The Law of Data (Privacy) Protection: a comparative and theoretical study* (LLD-thesis University of South Africa 2003)

Safari 2017 *SHLR* 811.

Safari BA "Intangible Privacy Rights: How Europe's GDPR will set a new global standard for personal data protection" 2017 *SHLR* 809 – 848

Snail 2008 *JBL* 63.

Snail S "Cyber crime in the context of the ECT Act" 2008 *JBL* 63 – 69

Snail 2009 *JILT* 2.

Snail S "Cyber Crime in South Africa – Hacking, Cracking and other unlawful online activities" 2009 *JILT* 1 – 13

Swales 2016 *SAMLJ* 49.

Swales L "Protection of Personal Information: South Africa's answer to the Global Phenomenon in the context of unsolicited electronic messages (Spam)" 2016 *SAMLJ* 49 - 84

Swartz and da Veiga 2016 *ISSA* 11.

Swartz P and da Veiga A "PoPi Act – opt-in and opt-out compliance from a data value chain perspective: A South African insurance industry experiment" 2016 *ISSA* 9 - 17

Taylor and Cronjé *101 Questions and Answers about the Protection of Personal Information Act* 2.

Taylor D and Cronjé F *101 Questions and Answers about the Protection of Personal Information Act* 1st ed (Juta 2014)

Van der Bank 2012 *EJBSS* 78.

Van der Bank CM "The Right to Privacy – South African and Comparative Perspectives" 2012 *EJBSS* 77 - 86

Van der Merwe *et al Information Communication and Technology Law* 24.

Van der Merwe D *et al Information Communication and Technology Law* 1st Edition (LexisNexis 2008)

Van der Merwe *et al Information Communication and Technology Law* 80.

Van der Merwe D *et al Information Communication and Technology Law* 2nd Edition (LexisNexis 2016)

Van Ooijen and Vrabec 2019 *JCP* 92.

Van OoijenI and Vrabec HU "Does the GDPR Enhance Consumer's Control over Personal Data? An Analysis from a Behavioural Perspective" 2019 *JCP* 91 – 107

Warren and Brandeis 1890 *Harvard Law Review* 193–220.

Warren D and Brandeis D "The right to privacy" 1890 *Harvard Law Review* 4(5) 193–220

Case law

Abrahams v Burns (1914 CPD 452)

Bernstein ao v Bester NO AO (1996 (2) SA 751 (CC)

Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others (CCT 20/95: CCT 21/95) (1996) ZACC 7

Glenister v President of the Republic and Others 2011 (7) BCLR 651 (CC) and 2011 (3) SA 347 (CC).

Mistry v Interim National Medical and Dental Council and Others (CCT 13/97) (1998) ZACC 10

National Coalition for Gay and Lesbian Equality & another v Minster of Justice & others (1999 (1) SA 6 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (C)

S v Makwanyane 1995 (3) SA 391 (CC)

Legislation

European Union

Human Rights Act (1998)

South Africa

Conduct of Financial Institutions Bill [B-2018]

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Cybercrimes Bill [B6-2017]

Electronic Communications and Transactions Act 25 of 2002

Financial Advisory and Intermediary Services Act 37 of 2002

Financial Intelligence Centre Act 38 of 2001

Financial Sector Regulation Act 9 of 2017

Indecent or Obscene Photographic Matter Act 37 of 1967

Insurance Act 18 of 2017

Medicines and Related Substances Control Act 101 of 1965

National Credit Act 34 of 2005

Personal Information Protection and Electronic Documents Act of 2001

Prevention and Combatting of Corrupt Activities Act 12 of 2004

Prevention of Organized Crime Act 121 of 1998

Privacy Act 119 of 1988

Promotion of Administrative Justice Act 3 of 2000.

Protection of Access to Information Act 2 of 2000.

Protection of Personal Information Act 4 of 2013.

Regulation of Interception of Communications and Provision of Communication-Related information Act 70 of 2002

Short-term Insurance Act 58 of 1998

South African Reserve Bank Act 1989

United Kingdom

Data Protection Act (1998)

International Instruments

Convention for the Protection of Human Rights and Fundamental Freedoms (1953)

General Data Protection Directive of 1995 (95/46/EC)

General Data Protection Regulation (2016/679)

Organisation for Economic Co-operation and Development guidelines (1980)

The Privacy and Electronic Communications (EC Directive) Regulation (2003)

Government Publications

Board Notice 80 of 2003 in GG25299 of 8 August 2003

Internet Sources

Bhagattjee, Govuza and Sebanz 2020 https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html.

Bhagattjee P, Govuza A and Sebanz L 2020 *CYBERCRIMES BILL – A POSITIVE STEP TOWARDS THE REGULATION OF CYBERCRIMES IN SOUTH AFRICA* https://www.cliffedekkerhofmeyr.com/en/news/publications/2020/technology/tmt-alert-7-july-The-Cybercrimes-Bill-is-one-step-away-from-becoming-law.html accessed 29 September 2020

Collett et al 2020 http://www.bizcommunity.com/Article/196/751/207083.html.

Collett C et al 2020 *Digital Transformation in the Financial Services Sector – FinTech News South Africa* http://www.bizcommunity.com/Article/196/751/207083.html accessed 15 September 2020

Department of Justice 2006 https://www.justice.gov.za/salrc/dpapers/dp109.pdf.

Department of Justice 2006 *South African Law Reform Commission Privacy and Data Protection Discussion Paper 109* https://www.justice.gov.za/salrc/dpapers/dp109.pdf accessed 15 August 2020

Department of Justice date unknown http://www.justice.gov.za/inforeg/about.html.

Department of Justice date unknown *Information Regulator (South Africa)* http://www.justice.gov.za/inforeg/about.html accessed 20 August 2020

Heale 2018 https://www.sapiens.com/blog/additional-popi-challenges-for-insurers-in-south-africa/.

Heale B 2018 *Additional POPI challenges for Insurers in South Africa* https://www.sapiens.com/blog/additional-popi-challenges-for-insurers-in-south-africa/ accessed 14 May 2020

Holton 2016 http://www.moonstone.co.za/popi-and-your-fsp/.

Holton A 2016 *POPI and your FSP* http://www.moonstone.co.za/popi-and-your-fsp/ accessed 15 June 2020

Janse van Rensburg 2019 https://www.werksmans.com/legal-updates-and-opinions/conduct-of-financial-institutions-bill/.

Janse van Rensburg T 2019 *Conduct of Financial Institutions Bill* https://www.werksmans.com/legal-updates-and-opinions/conduct-of-financial-institutions-bill/ accessed 14 November 2020

Jefferson and Stephens 2019 https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/.

Jefferson M and Stephens S 2019 *South African data protection law and third-party processors* https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/south-african-data-protection-law-and-third-party-processors/ accessed 5 September 2020

Kruger 2016 http://www.moonstone.co.za/popi-and-the-general-code-of-conduct/.

Kruger P 2016 *POPI and the General Code of Conduct* http://www.moonstone.co.za/popi-and-the-general-code-of-conduct/ accessed 3 June 2020

Leon and Ripley-Evans 2019 https://financialregulationjournal.co.za/2019/04/10/financial-services-litigation-in-south-africa/.

Leon P and Ripley-Evans J 2019 *Financial Services Litigation in South Africa* https://financialregulationjournal.co.za/2019/04/10/financial-services-litigation-in-south-africa/ accessed 1 September 2020

Masthead 2018 https://www.masthead.co.za/newsletter/commencement-of-the-insurance-act/.

Masthead 2018 *Commencement of the Insurance Act* https://www.masthead.co.za/newsletter/commencement-of-the-insurance-act/ accessed 14 November 2020

Nicole O 2019 http://www.privacypolicies.com/blog/popi-act/.

Nicole O 2019 *South Africa's PoPi Act* http://www.privacypolicies.com/blog/popi-act/ accessed 15 August 2020

Parliamentary Monitoring Group 2018 https://pmg.org.za/call-for-comment/784/.

Parliamentary Monitoring Group 2018 *Conduct of Financial Institutions (COFI) Bill 2018 - draft* https://pmg.org.za/call-for-comment/784/ accessed 14 November 2020

Privacy International 2019 https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa.

Privacy International 2019 *State of Privacy South Africa* https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa accessed 1 August 2020

Rodrigues 2012 www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286.

Rodrigues C 2012 *PoPi and Insurance* www.fanews.co.za/article/fanews-fanuus-magazine-archives/60/regulatory/1316/popi-and-insurance/15286 accessed 21 May 2020

The Presidency 2020 www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013.

The Presidency 2020 *Commencement of certain sections of the Protection of Personal Information Act, 2013* www.thepresidency.gov.za/press-statements/commencement-certain-sections-protection-personal-information-act%2C-2013 accessed 10 July 2020

Van Eeden 2016 https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/.

Van Eeden J 2016 *How PoPi can develop an edge for insurance companies* https://www.hrfuture.net/future-of-work/digital-economy/how-popi-can-develop-an-edge-for-insurance-companies/ accessed 23 May 2020

Unknown 2003 https://www.itweb.co.za/content/Gb3BwMWom3OM2k6V.

Unknown 2003 *The implications of the FAIS Act* https://www.itweb.co.za/content/Gb3BwMWom3OM2k6V accessed 15 November 2020

Unknown 2018 https://businesstech.co.za/news/business/255519/the-new-insurance-act-takes-effect-today-in-south-africa-heres-what-you-need-to-know/.

Unknown 2018 *A new Insurance Act takes effect today in South Africa – here's what you need to know* https://businesstech.co.za/news/business/255519/the-new-insurance-act-takes-effect-today-in-south-africa-heres-what-you-need-to-know/ accessed 14 November 2020