UNIVERSITY OF KWAZULU-NATAL

INYUVESI YAKWAZULU-NATALI

AN ANALYSIS OF THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA) AND THE EUROPEAN DATA PROTECTION FRAMEWORK: SUGGESTIONS FOR SOUTH AFRICA

by

Andi William Lee

216011652

A dissertation submitted in partial fulfilment of the requirements of the Master of Laws in Business Law (LLM) degree

at the

University of KwaZulu-Natal

July 2021

TABLE OF CONTENTS

DECLARATION OF ORIGINALITY

I, Andi William Lee declare that:

i. The research report in this dissertation, except where otherwise indicated, is my original work.

ii. This dissertation has not been submitted for any degree or examination at any other university.

iii. This dissertation does not contain other persons' data, pictures, graphs, or other information, unless specifically acknowledged as being sourced from other persons.

iv. This dissertation does not contain other persons' writing, unless specifically acknowledged as being sourced have been quoted, then:

   a) their words have been re-written, but the general information attributed to them has been referenced;

   b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

v. Where I have reproduced a publication of which I am author, co-author, or editor, I have indicated in detail which part of the publication was written by myself alone and have fully referenced such publications.

vi. This dissertation does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the dissertation and in the references section.

……..

Andi William Lee

216011652

ACKNOWLEDGEMENT

I would like to thank my supervisor Dr Lee Swales for his patience, dedication and sound advice, which has proved continuously invaluable throughout the process of undertaking this study.

To Pa, my best friend and father, I thank you for your eternal and unconditional love and support. You are my compass when I am lost, the light in the dark. Without you, I would not be. Thank you.

Clear Eyes, Full Heart, Can't Lose.

CHAPTER ONE: INTRODUCTION AND OVERVIEW

1.1. INTRODUCTION

There is a positive obligation on the State to respect, protect, promote, and fulfil the rights contained in the Bill of Rights.[1] This includes the right to privacy. The right to privacy is protected in terms of the common law and section 14 of the Constitution.

Section 14 provides:

> "Everyone has the right to privacy which includes the right not to have—
>
> (a) their person or home searched;
>
> (b) their property searched;
>
> (c) their possessions seized; or
>
> (d) the privacy of their communications infringed."

It is trite that constitutional rights are not absolute and thus the right to privacy, may be limited in accordance with section 36 of the Constitution (known as the limitations clause), if it is, in the particular circumstances, "reasonable and justifiable to do so in an open and democratic society based on human dignity, equality and freedom."[2]

The authority for the recognition of an independent right to privacy in South African law is considered to be the case of *O'Keeffe v Argus Printing and Publishing Co Ltd*[3] wherein the court held that the right to dignity includes the right to privacy.[4]

In 1996, Harms JA agreed with Neethling's definition[5] of privacy and accepted the following definition of privacy, in the case of *National Media Ltd v Jooste*.[6]

> "Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private."[7]

---

[1] Chapter 2 of the Constitution. The Constitution of the Republic of South Africa, 1996 (The Constitution).
[2] Section 36 of the Constitution. For a discussion of s 36, see IM Rautenbach 'Proportionality and the limitation clauses of the South African Bill of Rights' (2014) 17 (6) *PELJ* 2229-2267.
[3] 1954 (3) SA 244 (C).
[4] *Ibid* at 248 – 249.
[5] J Neethling 'The concept of privacy in South African Law' (2005) 122 (1) *SALJ* 18 – 28.
[6] 1996 (3) SA 262 (A) at 271.
[7] See Neethling op cit note 5 at 19.

Society's interest in the right to privacy, and what it means in the context of data protection, or the protection of personal information was described by Roos[8] stating:

> "… the essence of an individual's interest in privacy is his or her power of self-determination over the scope of the information to be excluded from the knowledge of others. Therefore, a person's right to privacy entails that he or she should have control over his or her personal information."[9]

The Constitutional right to privacy includes 'informational privacy'[10] which can be described as a person's right to control and decide when, how, and under what conditions their personal information or data may be made public.[11]

The protection of personal information therefore lies at the intersection of facilitating the free flow of data, which is absolutely necessary in the digital age in which we live.

However, this must be done in such a manner that ensures the protection an individual's information and safeguards against interferences of such an individual's right to privacy whilst not posing burdensome barriers to the free flow of information.

1.2. WHAT IS DATA PROTECTION?

Data protection refers to the legal protection of a person as it relates to the processing of data or personal information concerning himself or herself by another person or institution.[12]

The scope of the information that falls under the class of data or personal information is wide. For this reason, none are immune from requiring adequate data protection legislation, given the nature of the free flow of personal information which can range from names; to identity numbers to bank account numbers, to contact details, even information relating to one's employer.

---

[8] A Roos 'Data Protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 (2) *SALJ* 400-433.
[9] *Ibid* at 421- 22.
[10] I Currie & J D De Waal *The Bill of Rights Handbook* 6 ed (2013) at 302.
[11] See Neethling op cit note 5. See further *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others* 2001 (1) SA 545 (CC) at para 16.
[12] A Roos 'Core principles of data protection law' (2006) *Comparative and International Law Journal of South Africa* at 104. See further L Bygrave *Data protection law: approaching its rationale, logic and limit* (2002) at 2.

The unauthorised access, use, destruction, modification or disclosure of an individual's personal information related to the above, like financial or personal information, clearly has the possibility of creating inroads on the right to privacy.

1.3. PROTECTION OF PERSONAL INFORMATION PRIOR TO POPIA

South Africa did not have comprehensive data protection legislation prior to 2013; as a result, privacy issues had to be resolved using the common law and the Constitution.

This meant that the remedies available to a person whose privacy had been infringed, and personal information compromised, were limited to common law remedies and delictual remedies.[13]

There were, however, provisions in legislation covering aspects of informational privacy and the protection of personal information which are worth mentioning; most notably in the Promotion of Access to Information Act[14] (PAIA); the Electronic Communications and Transactions Act[15] (ECTA), and the Consumer Protection Act[16] (CPA).[17]

1.3.1. *PAIA*

PAIA is concerned with the fulfilment of a South African citizen's constitutional right of access to information[18] and is not primarily focussed on the protection of personal information. However, it promotes protection by permitting individuals access to both manual and computer records, containing personal information about them, held by both private and public bodies.[19]

Most notably, section 9 (a) (i) identifies the objective of PAIA as being:

> "…to give effect to the constitutional right of access to any information that is held by another person and that is required for the exercise or protection of any rights."

[13] The recognised remedies for common law infringements of privacy include the *actio iniuriarum*, the *actio legis Aquiliae* and the interdict. See also J Neethling, PJ Visser & JM Potgieter *Neethling's Law of Personality* (2005) 2 ed at 51.
[14] Act No 2 of 2000.
[15] Act No 25 of 2002.
[16] Act No 68 of 2008.
[17] A Naude & S Papadopoulos 'Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)' (2016) *THRHR* at 56-57.
[18] Section 39 of the Constitution.
[19] See Roos op cit note 8 at 424.

1.3.2. *ECTA*

The purpose behind the promulgation of ECTA is, *inter alia*, to facilitate and regulate electronic communications and transactions, to promote universal access to electronic communications and transactions, and to prevent abuse of information systems.[20]

ECTA deals with the protection of personal information in a limited manner through Chapter VIII. The limitation becomes clear in that "this protection is only applicable to personal information that has been obtained through electronic transactions."[21]

Section 51 aims to address the privacy concerns of consumers by outlining principles that must be adhered to when a data controller electronically collects personal information. However, this is only applicable if the data controller has chosen to adopt them and has recorded them in an agreement with the data subject.[22]

1.3.3. *CPA*

The CPA has focus on consumer protection by aiming to "promote a fair, accessible and sustainable marketplace for consumer products and services and, for that purpose, to establish national norms and standards relating to consumer protection."[23]

However, in the context of consumer protection against direct marketing, the CPA has provisions that relate to a consumer's privacy and the protection thereof. This is seen most notably through section 11 (1), which provides that:

> "The right of every person to privacy includes the right to—
>
> (a) refuse to accept;
>
> (b) require another person to discontinue; or
>
> (c) in the case of an approach other than in person, to pre-emptively block, any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing."

[20] Preamble of ECTA.
[21] Section 50 of ECTA, which has been repealed through s 110 of POPIA.
[22] See Roos op cit note 8 at 426. See also Section 51 of ECTA, which has been repealed through s 110 of POPIA. See further, Schedules of POPIA.
[23] Preamble of the CPA.

To date, there is not a plethora of case law dealing with the protection of personal information or data protection. However, Burchell notes in relation to the case of *Mistry v Interim Medical and Dental Council of South Africa*,[24] that although the case was decided under the Interim Constitution[25] the Constitutional Court "took the view that, even though it was not specifically mentioned in the Constitutional right to privacy, the protection of informational privacy was included."[26]

However, a question arises, if privacy is protected by the common law and the Constitution and various disconnected pieces of legislation mentioned above, why is it necessary to promulgate legislation in South Africa to regulate the protection of personal information?

1.4. WHY IS LEGISLATION PROTECTING PERSONAL INFORMATION NECESSARY?

The answer to this, according to Burns and Burger-Smidt, lies in the rapid explosion in technology, particularly the Internet, the globalisation and inter-dependence of economies, the convergence of information and communications technology, and its ability to swiftly transfer communication from one country to another.[27]

To put this explosion of technology and data into context, the Australian Productivity Commission estimated that five billion gigabytes of data was generated globally in 2002. The world, in 2017, generated that amount every two days.[28]

This explosion of technology has been confirmed by our courts, as seen in *Heroldt v Wills*,[29] where the court noted that:

> "The pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill not only from the courts,

[24] 1998 (4) SA 1127 (CC). This case concerned a challenge to the search and seizure powers given to inspectors by section 28 (1) of the Medicines and Related Substances Control Act (No 101 of 1965) on the basis that the provision is inconsistent with section 13 of the Interim Constitution. Section 13 being the right to privacy.
[25] Constitution of the Republic of South Africa Act 200 of 1993 (Interim Constitution).
[26] J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) *EJCL* 13 (1) 14.
[27] Y Burns & A Burger-Smidt *A commentary on the Protection of Personal Information Act* (2018) Durban: LexisNexis.
[28] Australian Government Productivity Commission 'Data Availability and Use' (2017) at 4. Available at: *https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf.* Accessed 2 February 2021.
[29] 2013 (2) SA 530 (GSJ).

> which must respond appropriately, but also from the lawyers who prepare cases such as this for adjudication."[30]

It was also confirmed in *Delsheray Trust and Others v ABSA Bank Limited*[31] where the court said:

> "Modern technological developments have brought about a revolution in the way that information, including legal information, is captured and disseminated."[32]

The need for data protection was recognised early on by the South African Law Reform Commission (SALRC). In 2005 in their Discussion Paper 109[33] they recommended that formal legislation on the protection of information be enacted.[34]

Neethling[35] emphasises the need for data protection legislation by identifying that activities of the data industry create a huge threat, or potential threat, to personality interests.

These threats have played out before our very eyes. South Africa, in 2020 alone has seen 24 million South Africans have their information breached in the recent Experian breach, which will be explored in further detail in Chapter Four.

Several months prior, Nedbank was breached and according to news reports, over one million active Nedbank customers were compromised which included the release of information such as "… full names, identity numbers, physical and/or e-mail addresses and phone numbers."[36]

It is critical to understand that without adequate legislation regulating the protection of personal information, the established common law avenues protecting privacy and identity are unable to deal effectively with the problems in this ever-evolving field.[37]

---

[30] Supra para 8.
[31] [2014] 4 All SA 748 (WCC).
[32] *Ibid* at para 18.
[33] South African Law Reform Commission (SALRC) Discussion Paper 109 (Project 124) *Privacy and data protection*. October 2005.
[34] *Ibid* at 39.
[35] See Neethling et al op cit note 13.
[36] Sunday Times – Business Times, 'Nedbank data breach may leave victims open to fraudulent attacks, say experts' Available at: *https://www.businesslive.co.za/bt/money/2020-03-08-nedbank-data-breach-may-leave-victims-open-to-fraudulent-attacks-say-experts/*. Accessed 3 November 2020. According to the IBM 'Cost of a Data Breach 2020' the average cost of a data breach in South Africa in 2020 was $2.14 million (R32 million). Available at: *https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/* Accessed: 25 January 2021.
[37] See Naude & Papadopoulos op cit note 17 at 59.

Globally more than 120 countries, independent jurisdictions and territories have adopted comprehensive data protection privacy laws to protect personal data held, or processed, by public or private bodies.[38]

Further, many countries may require adequate data protection in South Africa for the continuous free cross border flow of personal information from them to us. Therefore, to remain on the international stage as it relates to the free flow of data, the adoption of legislation is necessary. Moreover, it is necessary to give effect to the right to privacy in the modern digital age.[39]

1.5. PROMULGATION OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

In late 2013, the Protection of Personal Information Act[40] (POPIA) was promulgated, however only certain sections became effective, these were; the 'Definitions' in section 1, which does not create any laws itself, but is necessary for other sections.

Further, Part A of Chapter 5 of POPIA became effective, which deals with the establishment, staffing, powers and meetings of the Information Regulator (the Regulator), the supervisory authority as it relates to the protection of personal information.

Section 112 also became effective, which empowers the Minister and the Information Regulator to make POPIA Regulations. Logically connected to this is the last section which also became effective, which is section 113, the procedure for making such Regulations.[41] These Regulations were finalised and published in late 2018.[42]

---

[38] J Botha, M Grobler, J Hahn & M Eloff 'A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws' (2017) *The 12th International Conference on Cyber Warfare and Security (ICCWS)* 2. See further United Nations Conference on Trade and Development (UNCTAD) 'Data Protection and Privacy Legislation Worldwide' Available at: *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*. Accessed 20 February 2021.

[39] See Neethling op cit note 13 at 273.

[40] Act No 4 of 2013. POPIA was enacted in terms of GN 912 in GG37067 on 26 November 2013.

[41] Michalsons, June 2020 'POPI Commencement Date or POPI Effective Date starts the Clock' Available at: *https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109.* Accessed 18 July 2020.

[42] Regulations Relating to the Protection of Personal Information Act (Act No. 4 of 2013) in GN 1383 *GG* 42110 of 14 December 2018.

POPIA aims to give effect to the right to privacy by regulating the processing[43] of personal information by public and private bodies, in harmony with international standards.[44]

This involves:

(i) "balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders."[45]

1.6. RECENT DEVELOPMENTS

The most recent development in the protection of personal information came on 22 June 2020. The President of South Africa, Cyril Ramaphosa proclaimed further sections of POPIA to come into effect, hereby proclaiming:

> "Under section 115 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013), I hereby determine—
>
> (a) 1 July 2020 as the date on which—
>
> (i) sections 2 to 38;
>
> (ii) sections 55 to 109;
>
> (iii) section 111; and
>
> (iv) section 114(1), (2) and (3); and
>
> (b) 30 June 2021 as the date on which sections 110 and 114 (4) of the said Act shall commence."[46]

Given such proclamation, parties that process personal information were required to adhere to POPIA, within one year of the commencement of such provisions, thus the final deadline being 1 July 2021.[47]

---

[43] In terms of Section 1 of POPIA, 'processing' is defined as "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—
(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information."

[44] Preamble of POPIA.

[45] POPI Act Compliance. Available at*: https://www.popiact-compliance.co.za/gdpr-information/25-article-1-subject-matter-and-objectives.* Accessed 3 November 2020.

[46] 'Commencement of certain sections of the Protection of Personal Information Act' in Proc R21 *GG* 43461 of 22 June 2020.

[47] Section 114 of POPIA.

1.7. STATEMENT OF PURPOSE

This study seeks to compare the South African data protection framework with the approaches of foreign jurisdictions, namely the United Kingdom (UK) and European Union (EU), specifically as it relates to the enforcement provisions, particularly focusing on the considerations for civil remedies and administrative fines, for breaches of personal information.

The reasoning for selecting the UK and EU is noted by Greenleaf in that "nine out of the ten core principles, that should be incorporated in data privacy legislation to be effective, form part of the POPIA and the UK DPA 2018."[48]

If it is found that South Africa falls short of our foreign counterparts, this study will put forward possible improvements, to bring our law into harmony with more experienced jurisdictions and international standards.

1.8. RATIONALE

The significance of assessing the considerations of these provisions critically, is because it is the chapter dealing with the enforcement of POPIA, arguably the most important section for a person, (or as referred to in POPIA, a 'data subject') whose personal information has been compromised and is seeking recourse to enforce compliance with POPIA and vindicate their right to privacy.

Without a clear and effective avenue for enforcement, POPIA will not uphold what it seeks to achieve, which is "the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests."[49]

It is pertinent to assess legislation, and its potential impacts and efficacy, so that the downfalls, if any, do not become the living experience of people.

Since data protection in South Africa is still in its infancy, and POPIA is a newly promulgated piece of legislation,[50] there is currently no legal precedent in respect of its practical application.

---

[48] Greenleaf, G. (2013) 'Chapter 10: Data protection in a networked world.' In Brown, I. (ed). *Research handbook on governance of the Internet* Edward Elgar Publishing (2012) 221-259.
[49] See POPIA op cit note 44.
[50] See Commencement of certain sections of POPIA op cit note 46.

There is a wide range of academic discussion surrounding the topic of POPIA and the protection of information, however these works merely provide views and opinions of others and do not provide a judicially tested appreciation for how POPIA will be applied, nor do these works outline all of the important considerations at play.

It is therefore essential that the right to privacy and the protection of personal information is regulated, and such framework be constantly reviewed by the courts and the legislature considering changes in technology and the considerations and lessons of foreign jurisdictions.

This dissertation will therefore also aim to contribute to the discourse and interpretation of POPIA in its application with focus on the enforcement provisions, particularly as it relates to civil remedies and administrative fines and the factors considered.

1.9. RESEARCH QUESTIONS

a) What is the framework for the legal protection of personal information in South Africa?
b) What is the legal framework in the United Kingdom and European Union with regard to data protection?
c) In the event of a breach of personal information, what sections of POPIA are triggered and how will the enforcement framework of POPIA be applied?
d) Are there lessons to be learnt or suggestions to be made for South Africa from these foreign jurisdictions?

1.10. RESEARCH METHODOLOGY

This dissertation will be largely doctrinal with aspects of a comparative nature. The reason being that this study involves an analysis and review of legislation, both domestic and foreign, case law and literature concerning privacy, protection of personal information and civil remedies.

This desk-based study will aim to answer the research questions by gathering and analysing sources that are available in print or electronic format. The Internet and electronic search engines such as: LexisNexis, Sabinet, HeinOnline and Juta will primarily be utilised to aid this study.

However, an important caveat is the fact that this dissertation is being written during the COVID-19 pandemic and the accessibility of resources from any in person facility such as a law library, has been drastically reduced.

POPIA will be the primary piece of legislation examined in this dissertation as it regulates the processing of data and the protection of personal information in South Africa and contain enforcement provisions and considerations, to ensure compliance, which is at the heart of the focus of this paper.

Secondary sources such as journal articles, textbooks, academic writings, and other available online academic research papers will be utilised to examine the strengths and weaknesses of the enforcement provisions of POPIA, in order to amplify the findings and recommendations suggested in this study.

1.11. STRUCTURE OF THIS STUDY

Chapter One begins with an overview and introduction to the topic of this paper; it outlines the purpose and rationale for this study as well as the research questions and methodology that is to be used in answering such questions.

Chapter Two provides a deeper analysis of POPIA, by outlining the general framework, and the conditions for the lawful processing of personal information. Focus will be placed on the enforcement provisions which seek to ensure compliance.

Having explored South African law as it relates to the protection of personal information and the enforcement thereof; Chapter Three will turn to foreign approaches with respect to data protection. The focus will be on their framework, enforcement provisions and considerations, particularly looking at the EU instruments and the United Kingdom's Data Protection Act of 2018.

In doing so, this chapter will assess whether there are lessons to be learnt, for South Africa to improve and further structure the data protection framework established through POPIA.

Chapter Four will seek to analyse domestic breaches having occurred in South Africa to ascertain whether the lessons gleaned from the UK and EU can aid in the differentiation between breaches and further structure the South African data protection framework.

Chapter Five will discuss the findings of this paper as well as put forward conclusions and suggestions that can be made to strengthen POPIA, in light of the approach of the UK and EU specifically as it relates to the considerations involved in the enforcement of data protection legislation.

CHAPTER TWO: AN EXAMINATION OF THE PROTECTION OF PERSONAL INFORMATION ACT

2.1. INTRODUCTION

The focus of this chapter will be the principal piece of legislation governing the protection of personal information, in South Africa, the Protection of Personal Information Act 4 of 2013.

This chapter will provide insight into the background and objectives of POPIA, its scope and general application, generally outline the framework in which POPIA will operate and lastly, examine specific enforcement and offence provisions which give teeth to the bite that is compliance with POPIA.

Specifically, as it relates to the enforcement and offence provisions above, focus will be placed on the considerations when instituting and deciding a civil action[51] or issuing an administrative fine.[52]

2.2. BACKGROUND AND OBJECTIVES

POPIA is the product of a process that started in 2000, when the South African Law Reform Commission (SALRC) approved the inclusion in its programme, of an investigation entitled, *Privacy and Data Protection*.[53]

In October 2005, the SALRC published their findings and recommendations in the form of a Discussion Paper (109), which enclosed a draft Bill on the protection of information. The background of POPIA has deep roots in the SALRC Report.

The SALRC recognised that:

> "Privacy is a valuable aspect of personality. Data or information protection forms an element of safeguarding a person's right to privacy. It provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution."[54]

[51] Section 99 of POPIA.
[52] Section 109 of POPIA.
[53] See SALRC Discussion Paper op cit note 33 at 1.
[54] *Ibid* at vi.

Ultimately, the SALRC recommended[55] that formal legislation on the protection of personal information be enacted in South Africa.

It is important to note that both the discussion paper and the draft POPI Bill relied heavily on EU data protection laws as a source from which South Africa could base its data protection framework of.[56]

The need to develop the law as reflected in *Delsheray Trust* and *Herholdt* above was further echoed in the very year POPIA was promulgated. In 2013, the court in *H v W*[57] said the following:

> "The law has to take into account changing realities not only technologically but also socially or else it will lose credibility in the eyes of the people. Without credibility, law loses legitimacy. If law loses legitimacy, it loses acceptance. If it loses acceptance, it loses obedience. It is imperative that the courts respond appropriately to changing times, acting cautiously and with wisdom."[58]

2.3. KEY DEFINITIONS[59]

At the outset, it is crucial to have an understanding of who and what the various parties and mechanisms set out in POPIA are, so as to best understand the framework and the application thereof in the context of processing and protecting personal information.

'Consent' means **"**any voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her."

'Data Subject' is defined as "the person to which the personal information relates."

'Information Officer' – of, or in relation to, a—

> (a) "public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

[55] *Ibid* at 60.
[56] B Makulilo 'Privacy and data protection in Africa: a state of the art' (2012) 2(3) *International Data Privacy Law* at 163.
[57] [2013] 2 All SA 218 (GSJ).
[58] *Ibid* at para 31.
[59] Definitions, Section 1 of POPIA.

(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act (PAIA)."

'Operator' means "a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party."

'Personal Information' is defined comprehensively in POPIA[60] and bears full quotation as it is the central focus of this dissertation. It is defined as:

> "information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
>
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
>
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
>
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
>
> (d) the biometric information of the person;
>
> (e) the personal opinions, views or preferences of the person;
>
> (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
>
> (g) the views or opinions of another individual about the person; and
>
> (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."

[60] Elizabeth De Stadler & Paul Esselaar *A Guide to the Protection of Personal Information Act* (2015) 5.

'Responsible Party' – means "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information."

2.4. PURPOSE

The main objective of POPIA is found in its preamble, which states that it is to give effect to the right to privacy as espoused in section 14 of the Constitution. POPIA seeks to achieve this whilst being cognisant of the constitutional values of democracy and openness and the need for economic and social progress, in the framework of the information society in which we live.

POPIA further aims to regulate the processing of personal information in harmony with international standards;[61] prescribe minimum requirements for the lawful processing of personal information; provide rights and remedies to protect against abuses of personal information; and establish a Regulator to promote, enforce and fulfil the rights protected by POPIA.[62]

2.5. SCOPE AND GENERAL APPLICATION

POPIA applies to the exclusion of any other provision of any other legislation that relates to the processing of personal information and that is materially inconsistent with an object or specific provision of the POPIA.[63]

However, if any other legislation provides more extensive conditions for the lawful processing of personal information as provided for in Chapter 3 of the Act, that other legislation will apply.[64]

The scope of application of POPIA according to Van der Merwe[65] is that it applies, in general, to "any processing activity involving personal information either by a South

[61] See POPIA op cit note 44.
[62] M Heyink 'Protection of Personal Information for South African Law Firms (2013) *LSSA Guidelines Version 3* 10.
[63] Section 7 (1) of POPIA. See Burns & Burger-Smidt op cit note 27 at 8. See also F Coetzee 'The Press and POPI' (2014) 14 (4) *Without Prejudice* 11.
[64] Section 3 (2) (a) of POPIA.
[65] D Van der Merwe, S Eiselen, S Nel, A Roos *Information and Communication Technology Law* 2ed 2016 LexisNexis.

African responsible party or by a non-South African data controller using South African equipment."[66]

2.5.1. *Application and Interpretation of POPIA*

Further clarification is given through s 3 (1) (a) of POPIA. The Act applies to the processing of personal information that is entered in a record by or for a responsible party by making use of automated or non-automated means.

The application of POPIA is extended to include when personal information is processed by non-automated means, provided it forms part of a filing system or is intended to form part of a filing system.

POPIA takes a modern, encapsulating approach, given the nature of the free flow of personal information across borders. It states that it will apply to the processing of personal information where the responsible party is: -

(a) "domiciled in the Republic; or

(b) not domiciled in the Republic but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic."[67]

2.6. EXCLUSIONS

POPIA also expressly states what is excluded from its application, as it relates to the processing of personal information:

(a) "for purely personal or household activity;
(b) that has been de-identified to the extent that it cannot be re-identified again;
(c) processed by or on behalf of a public body for the purposes of:
    i. safeguarding national security;
    ii. the investigation and prosecution of criminal matters;
    iii. processed by the cabinet and its committees or the executive council of a province; or
    iv. relating to the judicial functions of a court."[68]

[66] *Ibid* at 434 – 35.
[67] Section 3 (b) (i) & (ii) of POPIA.
[68] Section 6 of POPIA.

Section 7 of POPIA goes further in its exclusion of application by stating that that the Act does not apply to processing for the purposes of journalistic, literary, or artistic expression.

Further that:

(b) "the exclusion for journalistic purposes requires the journalist to be subject to a code of ethics and provides adequate safeguards for the protection of personal information."[69]

2.7. RIGHTS OF DATA SUBJECTS[70]

Under POPIA, a data subject is granted several rights as it relates to their personal information and the use thereof, the most salient for the purposes of this dissertation are as follows:

a) The first is that a data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3 of the Act. This is also a requirement for compliance under POPIA.

   This right includes the right to be notified that—

   i. personal information about him, her or it is being collected;[71]
   ii. his, her or its personal information has been accessed or acquired by an unauthorised person;[72]

b) A data subject has the right to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information;[73]

   Moreover, the right to request, where necessary, the correction, destruction or deletion of his, her or its personal information;[74]

c) POPIA grants a data subject the ability to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information;[75]

[69] Section 7 of POPIA.
[70] Section 5 (a – i) of POPIA.
[71] Section 18 of POPIA.
[72] Section 22 of POPIA.
[73] Section 23 of POPIA.
[74] Section 24 of POPIA.
[75] Section 11 (3) (a) of POPIA.

d) As it relates to direct marketing, the data subject has the express right not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications, except as referred to in section 69(1) of POPIA;
e) A data subject has the right to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject; and
f) The right to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99."

2.8. CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

The following conditions must be met for the processing of personal information in terms of POPIA, to be deemed lawful, either in relation to employees or customers of a public or private body.

It is important to note, as pointed out by Heyink, that the conditions for lawful processing of personal information do not stand in isolation. They constitute what he calls "a constellation which interact with one another, sometimes overlapping and sometimes complementing and supplementing one another."[76]

2.8.1. *Condition 1: Accountability*

> "The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself."[77]

The effect of this is pointed out by Naude,[78] that the responsible party is ultimately held responsible for compliance, regardless of whether the personal information has been contracted out to an operator to process, for or on behalf of, the responsible party.[79]

[76] M Heyink 'Protection of Personal Information Guide.' (2018) *Law Society of South Africa Version 4* at12. It is important to note that the use of the word 'conditions' as it relates to processing personal information in terms of POPIA is essentially the same concept as 'principles' which is used by foreign jurisdictions.
[77] Section 8 of POPIA.
[78] Adrian Naude *Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments* (unpublished LLM thesis, University of Pretoria, 2014).
[79] *Ibid* at 46.

2.8.2. *Condition 2: Processing Limitation*[80]

> "Personal information must be processed: -
>
> (a) lawfully, and
>
> (b) in a reasonable manner that does not infringe the privacy of the data subject."

The element of 'lawfulness' in section 9 (a) is straight forward and the responsible party cannot act unlawfully in its collection or processing of personal information.

However, Heyink correctly notes that the element of 'reasonableness' in section 9 (b) imports notions of fairness, which suggests that there needs to be a consideration of balance and proportionality.

Responsible parties must therefore take into account the interests and reasonable expectations of data subjects as well as all of the provisions which are incorporated in these conditions.

Roos[81] states that the "application of this principle also implies that when data no longer serves the purpose for which it was originally collected, it should be erased or expressed in an anonymous form."

This condition also requires what Bygrave[82] described as the 'minimality principle' in the processing of personal information. This is confirmed in section 10 of POPIA which states that personal information may only be processed if, given the purpose for which it is processed, is adequate, relevant and not excessive.

2.8.3. *Condition 3: Purpose Specification*[83]

> "Personal information must be collected for a specific explicitly defined and lawful purpose and the data subject must be aware of that purpose."

There are three elements to this condition. Collection must be for a specific purpose; the data subject must be aware of such purpose and that retention of the personal information must not be for longer than it is required.

A practical, real-world example may include:[84] if a data subject creates an account with Takealot.com for the purpose of buying a product, any use of the credit card information

[80] Section 9 – 12 of POPIA.
[81] See Roos op cit note 12.
[82] See Bygrave op cit note 12 at 2.
[83] Section 13 & 14 of POPIA.
[84] L Swales 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam)' (2016) *SA Merc LJ* at 62.

of such data subject, for any reason other than processing a sale, would result in a contravention of POPIA.

Further, the personal information processed by Takealot.com "must not be retained for an unreasonably long period of time — this test is objective and will be determined with reference to the purpose for which the data was collected."[85]

2.8.4. *Condition 4: Further Processing Limitation*[86]

Any further processing must also be in line with the initial purpose for which the data was collected. Burns & Burger-Smidt describe this further processing limitation condition as determining, "whether the *further* processing of personal information is compatible with the *original* purpose of the processing of that information."[87]

With reference to the Takealot.com example above, the further processing of a data subject's name, contact information and physical address, for the purpose of processing a sale and subsequent delivery of a product, would be in line with the initial purpose for which the information was collected.

2.8.5. *Condition 5: Information Quality*[88]

The responsible party must take reasonably practical steps to ensure that the personal information is complete, accurate, not misleading and updated, where necessary.

It is important to note that this condition compliments the purpose specification condition. This is evident in that when a responsible party under this condition takes the steps to ensure that the personal information is complete, accurate and updated, the responsible party must have regard for the purpose for which the personal information is collected or further processed and the quality thereof.

POPIA does not provide further details on what reasonably practicable steps would mean and therefore each business will need to consider its operations and decide for itself which steps and processes it would implement to reasonably keep personal information complete, accurate and updated.

[85] *Ibid.*
[86] Section 15 of POPIA.
[87] See Burns & Burger-Smidt op cit note 27 at 63.
[88] Section 16 of POPIA.

2.8.6. *Condition 6: Openness*[89]

The requirements of openness and transparency underpin any democratic government. POPIA requires that:

> "The responsible party must take reasonable steps to ensure that the data subject is aware of the data collection process, the purpose for collecting the information, whether the information required is mandatory or voluntary, consequences of failure to provide information and the laws governing the collection of information."

The purpose of this condition is to ensure transparency and fairness in the processing of personal information.[90] This obliges the responsible party to ensure that the data subject is made aware of: the information that is being collected, the purpose of such collection as well as the name, address and contact information of the responsible party processing such information.

2.8.7. *Condition 7: Security Safeguards*[91]

> "A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—
>
> (a) loss of, damage to or unauthorised destruction of personal information; and
>
> (b) unlawful access to or processing of personal information."[92]

Viljoen et al[93] explain that:

> "POPIA makes provision for various security measures on integrity and confidentiality of personal information, the processing of information, security measures to be taken and the notification requirements in case of any security compromises."[94]

In order to give effect to this condition, the responsible party must take reasonable measures to: -

(a) "identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;

[89] Section 17 – 18 of POPIA.
[90] See Burns & Burger-Smidt op cit note 27 at 21.
[91] Section 19 – 22 of POPIA.
[92] Section 19 (1) of POPIA.
[93] M Viljoen, C de Villebois Castelyn, A Pope, M Botes 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa' (2020) *S Afr Bioethics Law* 13 (1).
[94] *Ibid* at 4.

(c) regularly verify that the safeguards that have been implemented are working as intended;

(d) ensure that the safeguards are continually updated in response to new risks, changes in technology, or flaws in previously implemented safeguards."[95]

However, it has been critically pointed out that "this provision is rather vague and is open to a number of interpretations on the scope and ambit of reasonably foreseeable risk."[96] It is likely that the consideration of reasonableness, as it relates to security measures, will be determined with reference to industry standards that are effective at the time of any review.

This is supported by Millard and Bascerano,[97] in that they contend that what is appropriate and reasonable in the context of security safeguards; will depend on the size and nature of the organisation in question.[98]

In so far as appropriate technical and organisational measures are concerned, these will vary across businesses. It will require organisations to view their operations and implement appropriate measures, technically, for example with the use of firewalls, encryption, access control, backups and hard copies. These measures go hand in hand with the organisational aspect, which could be, for example, ensuring adequate policies are implemented in an organisation, such as privacy policies, data breach management policies or POPIA policies. Further, it will require that the employees of any such organisation are trained and aware of such policies and the requirements imposed by this condition of POPIA.

2.8.8. *Condition 8: Data Subject Participation*[99]

"Data subjects can request access, correction, and deletion of their personal information."

This provision complements the condition above, openness, in that it gives a data subject the right to request that a responsible party confirm, at no charge, whether the responsible party holds personal information about the data subject.[100]

---

[95] See Burns & Burger-Smidt op cit note 27 at 71.
[96] See Swales op cit note 84 at 63.
[97] D Millard and EG Bascerano 'Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act' (2016) *Potchefstroom Electronic Law Journal (PELJ)* (19).
[98] *Ibid* at 13. The authors also suggest the ISO 27001 (international security standard) as an appropriate technical security standard that can be applied by public and private bodies.
[99] Section 23-25 of POPIA.
[100] Section 23 (1) (a) of POPIA.

Further, the data subject may request a record or description of the personal information held by the responsible party or by a third party within a reasonable time.[101]

Any fees charged for providing the data subject with the information required shall not be excessive. The responsible party should also advise the data subject of their right to request that the personal information be corrected.[102]

2.9. NOTIFICATION OF SECURITY COMPROMISE OR BREACH[103]

POPIA requires notification to be made in the event of a breach. This is triggered:

> "Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—
>
> (a) the Regulator; and
> *(b)* subject to subsection (3), the data subject, unless the identity of such data subject cannot be established."

With respect to the substance of what the notification must contain, POPIA requires that:

> "The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise[104], including—
>
> (a) a description of the possible consequences of the security compromise;
> (b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;
> (c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
> (d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information."

The notification must take place "as soon as reasonably possible after the discovery that information has been compromised, taking into account the legitimate interests or needs of law enforcement or any measure reasonably necessary to determine the scope of the

[101] Section 23 (1) (b) of POPIA.
[102] Section 24 (1) (a) of POPIA. See Naude op cit note 78 at 51.
[103] Section 22 of POPIA.
[104] Section 22 (5) (a - d) of POPIA.

compromise and to restore the integrity of the responsible party's information system."[105]

2.10. ENFORCEMENT PROVISIONS

2.10.1. *The Information Regulator*

POPIA makes provision for the establishment of a juristic person known as the 'Information Regulator.' (The Regulator). The Regulator is designed to be impartial and independent of government. The Regulator is subject only to the law and the Constitution and it is accountable to the National Assembly.[106] The Regulator must perform its functions and exercise its powers, without fear, favour or prejudice.[107]

The Regulator is, empowered to monitor and enforce compliance by public and private bodies with the provisions of POPIA.[108] The Regulator's powers, duties and functions are, *inter alia* to:

(a) provide education, including the promotion of understanding and acceptance of the conditions of lawful processing of personal information;[109]
(b) handle and investigate complaints;[110]
(c) issue code of conduct from time to time;[111]
(d) co-operate on a national and international basis with other persons and bodies concerned with the protection of personal information;[112]
(e) facilitate cross-border cooperation in the enforcement of privacy laws with other jurisdictions;[113] and
(f) generally, do everything necessary to fulfil these duties, which is conducive to the protection of personal information in South Africa.[114]

[105] Section 22 (2) of POPIA. See Burns & Burger-Smidt op cit note 27 at 73.
[106] Information Regulator, Available at: *https://justice.gov.za/inforeg/*. Accessed 1 October 2020. See also section 39 (d) of POPIA.
[107] Section 39 (b) of POPIA.
[108] Section 40 (1) (b) of POPIA.
[109] Section 40 (1) (a) (i) of POPIA.
[110] Section 40 (1) (d) (i) of POPIA.
[111] Section 60 (1) of POPIA.
[112] Section 40 (1) (c) (ii) of POPIA.
[113] Section 40 (1) (g) of POPIA.
[114] Section 40 (1) (h) (i) & (ii) of POPIA.

2.10.2. *Enforcement Committee*

POPIA enables the Regulator to establish an enforcement committee, the purpose of which is described in section 93 of POPIA as being to "consider all matters referred to by the Regulator in terms of the Act and PAIA."

After considering submissions made by parties, the enforcement committee must make findings which are to be reported to interested parties and may also make recommendations to the Regulator relating to further action which may be taken.

2.10.3. *Enforcement Notice*

If, after having considered the findings of the Enforcement Committee, the Regulator is satisfied that a responsible party is interfering with the protection of a data subject's personal information, it may serve an enforcement notice on the responsible party.[115]

The enforcement notice may require the responsible party to take specified steps or desist from actions specified by the Regulator within the period stipulated in a notice. Enforcement notices will have to be in the form provided for in the Act or as may be determined by the Regulator.[116]

2.11. CODES OF CONDUCT

The legislature has made provision for codes of conduct under POPIA which can be issued from time to time by the Regulator.[117] Burns & Burger-Smidt note that "these codes of conduct are to be applied by specific bodies, specific industries, professions or vocations to regulate or govern the conduct of such bodies, organisations or professions."[118]

Further, it has been identified that the Regulator plays an important role in the process of the issuing of codes of conduct by assuming a supervisory role, by reviewing the operation of such codes of conduct and amending or revoking them where necessary.[119]

[115] See Heyink op cit note 76 at 45.
[116] *Ibid.* See also section 95 & 96 of POPIA.
[117] Section 60 (1) of POPIA.
[118] See Burns & Burger-Smidt op cit note 27 at 10.
[119] *Ibid* at 11.

POPIA requires that a code of conduct must include all the conditions for the lawful processing of personal information as mentioned above.[120]

2.12. COMPLAINTS

POPIA provides that any person may submit a complaint to the Information Regulator in the prescribed manner and form,[121] alleging interference with the protection of personal information of a data subject.

The lodging of a complaint is one avenue available to enforce the provisions of the POPIA, however the complaint must relate to a breach of Chapter 3 of the Act or the non-compliance with section(s) 22, 54, 69, 70, 71 or 72, or the breach of a code of conduct.

2.12.1. *The Information Regulator's response to a complaint*

Upon receipt of a complaint in terms of POPIA, the Regulator has the discretion to take several actions. These actions include to:

(a) conduct a pre-investigation as outlined in section 79;
(b) act as conciliator at any time during the investigation, where appropriate, in relation to any interference with the protection of personal information of a data subject;
(c) decide in accordance with section 77 to take no action or as the case may be, require no further action in respect of the complaint;
(d) conduct a full investigation into the complaint as provided by section 76 (3);
(e) refer the complaint to the Enforcement Committee; and[122]
(f) take further action outlined in Chapter 10 of the Act.

2.13. THE INFORMATION OFFICER

The promulgation of POPIA has the consequence that public and private bodies that process personal information are required to appoint an Information Officer.[123]

---

[120] For example, see the code of conduct submitted by the Banking Association of South Africa (BASA) to the Information Regulator. Available at*: https://www.justice.gov.za/inforeg/docs/InfoRegSA-Notice-BASA-COC-20210614.pdf*. Accessed 21 June 2021.
[121] See 2.15. 'The Regulations' below.
[122] Section 92 of POPIA. See 2.10.2 above.
[123] See Chapter Two at 2.3 for the definition of an 'Information Officer'.

The Information Officer is by default, the chief executive officer (CEO), or equivalent officer (Director General) of a public body or private body. Accordingly, there is no obligation to appoint an information officer as the applicable legislation designates an information officer by default.[124] However, the above can be altered if companies elect to do so, through the delegation of an Information Officer's functions to any person at management level.

Section 55 of POPIA when read with section 4 of the Regulations[125] identify the duties and responsibilities of an Information Officer which include:

a) "encouraging compliance with the conditions for the lawful processing of personal information and POPIA as a whole;
b) handling requests made to the body (public or private) pursuant to this Act, for example enabling access[126] to or the correction of the personal information held by such body, concerning a data subject;
c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA."

Further duties and responsibilities include ensuring that:

a) "a compliance framework is developed, implemented, monitored and maintained; and
b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information…"[127]

Information Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator. Registration for which commenced on 1 May 2021.[128]

2.14. CIVIL REMEDIES

2.14.1. *Establishing a claim*

[124] Information Regulator 'Frequently Asked Questions (FAQs) – Who is the Information Officer?' Available at: *https://twitter.com/InforegulatorSA/status/1376446204536578049/photo/1.* Accessed 12 April 2021.
[125] See Chapter Two at 2.16.
[126] See section 17 of PAIA.
[127] Information Regulator 'Guidance Note on Information Officers and Deputy Information Officers' 1 April 2021 Available at *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf.* Accessed 12 April 2021.
[128] *Ibid.* See section 55 (2) of POPIA. See further, Regulation 4. See further, the Information Regulator Media Statement '*https://twitter.com/InforegulatorSA/status/1377647934536302593/photo/1*. Accessed 12 April 2021.

It is important to note that; because POPIA has only recently taken full force and effect in the Republic, there has not been any reported case law in terms of which a data subject has based a claim on POPIA.

However, given the inevitability and certainty of a data subject instituting a claim against a responsible party for failing to comply with the provisions of the POPIA, the civil remedies provision must be examined.

In terms of section 99 (1):

> "A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party."

What gives rise to a claim is outlined in section 73 as an interference with the protection of the personal information of a data subject. Such interference consists, in relation to that data subject, of—

(a) "any breach of the conditions for the lawful processing of personal information as explained above;
(b) non-compliance with any of sections 22, 54, 69, 70, 71 or 72; or
(c) a breach of the provisions of a code of conduct issued in terms of section 60."

This provides an avenue for a data subject to seek a judicial remedy against a responsible party for failure to protect personal information. This provision also identifies what gives rise to a valid claim against a responsible party in terms of the Act.

2.14.2. *Defences*

With a claim established, section 99 (2) outlines the possible defences available to a responsible party to negate liability for failing to protect personal information or comply with the provisions of POPIA.

In the event of a breach the responsible party may raise any of the following defences against an action for damages:

(a) "vis major;
(b) consent of the plaintiff;
(c) fault on the part of the plaintiff;

(d) compliance was not reasonably practicable in the circumstances of the particular case; or

(e) the Regulator has granted an exemption in terms of section 37."[129]

As previously mentioned, the use of the words 'reasonably practicable' in this provision also prove to be problematic. It must be said that POPIA does not elaborate further on what would or would not be considered 'reasonably practicable' in the circumstances. Further, the Regulations make no mention either of what would or would not be considered 'reasonably practicable'.

2.14.3. *Compensation*

A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable, including—

(a) "payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(b) "aggravated damages, in a sum determined in the discretion of the Court;

(c) interest; and

(d) costs of suit on such scale as may be determined by the Court."

This is significant as it reflects a similar position of the law in the UK, in that damages may be awarded for both patrimonial and non-patrimonial loss. This will be explored in greater detail in Chapter Three.

Where there has been a breach of POPIA, the data subject (or the Regulator acting on behalf of the data subject) will be entitled to claim damages. What amounts will ultimately be awarded remains to be seen.

Where the Regulator has instituted proceedings on behalf of the data subject, the Regulator may deduct all reasonable expenses in bringing the matter before court, including administration costs.[130]

2.15. OFFENCES, PENALTIES & ADMINISTRATIVE FINES

2.15.1. *Offences*

As it relates to offences, a brilliant analogy of a physical burglary is espoused by Myers, in which the author explains that what POPIA does, as it relates to protecting personal

[129] Section 99 (2) of POPIA.
[130] Section 99 (4) of POPIA.

information is, "to turn lax and irresponsible behavior, such as not having burglar guards on windows or alarm systems in the home, into a criminal offence."[131]

Sections 100 – 106 create offences under POPIA such as:

(a) obstruction of the Regulator;[132]
(b) breach of confidentiality by a person acting under the direction of the Regulator;[133]
(c) failure to comply with an enforcement or information notice;[134]
(d) unlawful acts by responsible parties in connection with account numbers of data subjects;[135] and
(e) unlawful acts by third parties in connection with account numbers of data subjects.[136]

2.15.2. *Penalties*

Heyink summarises the penalties in section 107 of POPIA that can be imposed in the event of contravention as being:

> "…for more serious offences like hindering, obstructing or unlawfully influencing the Regulator, failure to comply with an enforcement notice, giving false evidence, contravening the lawful conditions for the processing of personal information as it relates to an account number, are punishable by a fine or to a period of imprisonment not exceeding 10 years, or both fine and imprisonment."[137]

2.15.3. *Administrative Fines*

An administrative fine is collected by the Regulator and is paid to the National Revenue Fund referred to in section 213 of the Constitution. If a responsible party is alleged to have committed an offence in terms of the Act the Regulator may deliver an infringement notice by hand to that person (who is now referred to in POPIA as the infringer.)

The infringement notice must:

(a) "specify the name and address of the infringer;
(b) specify the particulars of the alleged offence; and

[131] C Myers 'The imminent Protection of Personal Information Act' 2017 *TFM Magazine* Issue 12 at 26.
[132] Section 100 of POPIA.
[133] Section 101 of POPIA.
[134] Section 103 of POPIA.
[135] Section 105 of POPIA.
[136] Section 106 of POPIA.
[137] See Heyink op cit note 76 at 47.

(c) specify the amount of the administrative fine payable, which amount may, subject to subsection (10), not exceed R10 million."[138]

POPIA through section 109 (3) (a – h) lays out the factors that the Regulator must consider when determining an appropriate administrative fine. These are:

(a) "the nature of the personal information involved;
(b) the duration and extent of the contravention;
(c) the number of data subjects affected or potentially affected by the contravention;
(d) whether or not the contravention raises an issue of public importance;
(e) the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;
(f) whether the responsible party or a third party could have prevented the contravention from occurring;
(g) any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and
(h) whether the responsible party has previously committed an offence in terms of this Act."

It is submitted that the above factors give some insight into the differentiation between on the one hand, responsible parties who have taken reasonable steps in line with industry standards and approved codes of conducts and have complied with the requirements of POPIA as far as reasonably practicable.

Then on the other hand, responsible parties who have failed to meet their obligations, like the lawful conditions for the processing of personal information, notification requirements or other provisions of POPIA which require compliance.

It has been noted by Swales that this Chapter of POPIA gives the Regulator 'the ability to bite' in terms of enforcing compliance with the provisions of POPIA. The author continues by noting that "the nature and scope of infringements are yet to be entirely clarified." In this regard, the author proffers that "we will have to wait until the Regulator publishes the codes of conduct and related material in terms of Chapter 7 and ss 60–68."[139]

[138] Section 109 (2) (a – c) of POPIA.
[139] See Swales op cit note 84 at 77.

However, although I agree with the author as it relates to the publishing of codes of conduct, to establish industry standards for the protection of personal information for different bodies, organisations and professions or vocations, I submit that the nature and scope of infringements can be clarified further.

This can be done by looking to foreign jurisdictions and assess their respective determinations regarding the nature and scope of infringements as well as the factors to be considered in such determination.

2.16. THE REGULATIONS

As provided for under section 112 (2) of POPIA, in December 2018, the Information Regulator published the 'Regulations Relating to the Protection of Personal Information' [140] (the Regulations).[141]

The Regulations are mainly administrative in nature and prescribe a number of forms to be used in order to take certain types of action under POPIA. These types of actions concern the following;

(a) the way an objection to the processing of personal information can be made;[142]
(b) requests for the correction or deletion of personal information or the destruction or deletion of a record of personal information;[143]
(c) duties and responsibilities of information officers (to be appointed by each responsible party), which includes obligations relating to impact assessments to be undertaken;[144]
(d) applications for the Regulator to issue industry codes of conduct;[145]
(e) the manner in which consent is requested for processing of personal information for direct marketing by means of unsolicited electronic communications;[146]
(f) submission of complaints or grievances;[147]

[140] See Regulations op cit note 42.
[141] Michalsons 'POPI Regulations 2018 published in final form' December 2018. Available at: *https://www.michalsons.com/blog/popi-regulations-popia-regulations/12417.* Accessed 12 October 2020.
[142] Section 2 of the Regulations.
[143] Section 3 of the Regulations.
[144] Section 4 of the Regulations.
[145] Section 5 of the Regulations.
[146] Section 6 of the Regulations.
[147] Section 7 of the Regulations.

(g) the Regulator acting as a conciliator during an investigation;[148]

(h) the notification requirements of the Regulator to provide notification and information to all affected parties to a complaint or investigation;[149] and

(i) the notification requirements of the Regulator to provide notification to affected parties of its intention to carry out assessments or relating to a request by a third party to do so.[150]

[148] Section 8 of the Regulations.
[149] Section 12 of the Regulations.
[150] Section 11 of the Regulations.

CHAPTER THREE: THE DATA PROTECTION FRAMEWORK OF THE UK AND EU

3.1. INTRODUCTION

With the framework of data protection in South Africa outlined in Chapter Two, a pertinent question arises. This question is whether there are lessons to be gleaned for South Africa and POPIA, as it relates to the enforcement of data protection legislation, from more mature, foreign jurisdictions.

For the purposes of this chapter, the focal point of the foreign comparative analysis will be on the data protection legislation in the UK and EU, given the fact that POPIA is heavily rooted in the European model of data protection.[151]

Consequently, the aim of this chapter is to examine the development of the international instruments emanating from Europe, which deal with data protection and the protection of personal information.

These include, briefly, the Council of Europe Convention (CoE Convention), the Organisation for Economic Co-operation and Development (OECD) Guidelines, the EU Directive and the General Data Protection Regulation (GDPR).

Given the similarities between South African law and the European model of data protection, this chapter will also examine the United Kingdom's Data Protection Act of 2018[152] (UK DPA 2018) in particular, and establish what, if anything, can be learnt from the abovementioned models of data protection, to improve and further structure the untested data protection framework of South Africa.

3.2. LEGAL BASIS FOR ANALYSING FOREIGN JURISDICTIONS

The starting point for looking beyond our borders, in terms of the law that is applied elsewhere, is found in the Constitution.[153]

First, through section 2, which provides that:

> "This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled."

Consequently, one must then turn to section 39 (b) and (c) of the Constitution which provides that:

[151] See Swales op cit note 84 at 59.
[152] 2018 c.12.
[153] The Constitution op cit note 1.

"When interpreting the Bill of Rights, a court, tribunal or forum—

(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;

(b) *must consider international law; and*

(c) *may consider foreign law*." (My emphasis).

Given the fact that the protection of personal information and the failure to protect such information can infringe on the right to privacy, found in the Bill of Rights, one, in interpreting this right, *must* consider international law and *may* consider foreign law.[154]

3.3. INTERNATIONAL INSTRUMENTS

As laid out by Roos,[155] the 1980s marked a significant period of growth in data protection. International organisations like the OECD, the Council of Europe as well as the EU recognised the growing need to harmonise data protection across borders and across nations.[156]

Their rationale was, on the one hand, if multi-national corporations, for example, Apple, had to conform to differing standards of data protection in every country in which they did business, that is to say, processed or stored data, this would have an overlapping effect, potentially create uncertainty and would impose an onerous burden on them.

Balanced on the other hand is the need to ensure that the liberties and rights, of the citizens of respective nations, are protected by ensuring there are no data havens.[157] (Countries where no data protection regulations exist).

This well-placed recognition subsequently resulted in the publication of the multiple significant international documents or instruments which concern data protection.

3.3.1. *The Council of Europe*

The Council of Europe (CoE) was formed in the wake of World War II to bring together the states of Europe. The aim of the CoE was to ensure the maintenance and realisation

[154] C Rautenbach 'The South African Constitutional Court's use of foreign precedent in matters of religion: Without fear or favour?' (2015) *Potchefstroom Electronic Law Journal (PELJ)* 18 (5) at 1547. See further Burns & Burger -Smidt op cit note 27 at 259.
[155] See Roos op cit note 12.
[156] *Ibid* 104.
[157] *Ibid.*

of human rights and fundamental freedoms.[158] These include promoting the rule of law, democracy, as well as social and economic development.

With the emergence of information technology in the 1960s, there was a growing need for more detailed rules to safeguard individuals by protecting their personal data.[159]

This need was addressed in 1980 when the CoE adopted the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' which is often shortened to the CoE Convention 108.[160]

According to the CoE, this Convention is the first binding international instrument which protects the individual against infringements which may arise through the collection and processing of personal data.[161]

The main principles espoused by this Convention require that when automatically processing[162] personal data it must be done in accordance with the following.[163] It must be:

a) "obtained and processed fairly and lawfully;
b) stored for specific and legitimate purposes; and not used in a way that is incompatible with those purposes;
c) adequate, relevant, and not excessive in relation to the purpose for which they are stored;
d) accurate, and where necessary, kept up to date;
e) preserved in a form which permits identification of data subjects for no longer than is required for the purpose for which the data are stored;
f) protected by appropriate security measures; and

[158] Article 1 (b) of the Convention.
[159] Lydia F de la Torre 'What is Convention 108?' 26 June 2019 Available at: *https://medium.com/golden-data/what-is-coe-108-3708915e9846.* Accessed 29 January 2021.
[160] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, 108 Council Eur. T.S.
[161] Council of Europe. 'Details of Treaty No.108' Available at: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.* Accessed 30 October 2020. As of December 2020, signatories included mostly European countries, however there are non-members of the CoE who have signed and ratified, such as Argentina, Senegal and Uruguay. South Africa has not signed to this Convention. The full list of signatories can be found at: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.* Accessed on 3 February 2021.
[162] Article 2 of the Convention defines "automatic processing" as including the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.
[163] See Van der Merwe et al op cit note 65 at 378-9.

g) accessible to individuals to enable checking the veracity of the information and enabling correction if necessary."[164]

The principles espoused in the CoE Convention have been the foundation of subsequent privacy regulation in Europe, significantly influencing the OECD Guidelines, which were adopted the following year.[165]

3.3.2. *The OECD Guidelines*

The second notable document was published by the OECD[166] and is known as the 'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data'.[167]

The purpose of the OECD Guidelines is to balance the protection of privacy and individual liberties against the advancement of the free flow of personal data across national boundaries.[168]

The OECD Guidelines apply to personal data, in the public or private sector, which, because of the manner in which they are processed by a data controller, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.[169]

3.3.2.1. *Principles of the OECD Guidelines*

The basic principles which underpin the OECD Guidelines include the following data protection principles, which are closely aligned with the CoE Convention above. POPIA has also adopted these guidelines in more or less the same form:[170]

---

[164] A Levin & M Nicholson 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground' (2005). *University of Ottawa Law & Technology Journal.* 2 (2). 374.
[165] Sahar Bhaimia, 'The General Data Protection Regulation: The Next Generation of EU Data Protection' (2018) 18(1) *Legal Information Management* at 22.
[166] The Organisation for Economic Co-operation and Development is an international organisation that works to build better policies and brings together member countries and a range of partners (of which South Africa is one) that collaborate on key global issues at national, regional and local levels across social, economic and environmental areas. See the OECD website at: *https://www.oecd.org/.* Accessed 17 February 2021.
[167] 'Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data' Paris, 1981 ("OECD Guidelines").
[168] Anneliese Roos 'The law of data (privacy) protection: A comparative and theoretical study' (unpublished LLD thesis, UNISA, 2009) 157.
[169] *Ibid.* See further Part One: Para 2 of the OECD Guidelines. Available at: *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.* Accessed 30 October 2020.
[170] See Burns & Burger-Smidt op cit note 27 at 264.

a) "Collection limitation principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[171]

b) Data quality principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.[172]

c) Purpose specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes.[173]

d) Use limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject; or by the authority of law.[174]

e) Security safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification, or disclosure of data.[175]

f) Openness: There should be a general policy of openness about developments, practices, and policies with respect to personal data.[176]

g) Individual participation: Individuals should have the right:

   i. to obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to them;

   ii. to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them;

h) Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above."[177]

---

[171] OECD Guidelines para 7. See Burns & Burger-Smidt op cit note 27 at 263.
[172] OECD Guidelines para 8.
[173] OECD Guidelines para 9. This principle also requires that when data no longer serves the purpose for which it was originally collected, it should be erased or given in anonymous form. See further Van der Merwe op cit note 64 at 374.
[174] OECD Guidelines para 10.
[175] OECD Guidelines para 11. These security measures can be physical, (locking doors, using identification cards); these measures can be organisational (limiting the number of people that have access) and these measures can be informational (enciphering and monitoring unusual activities). See further Van der Merwe op cit note 65 at 375.
[176] OECD Guidelines para 12.
[177] OECD Guidelines para 4.

It has been accurately asserted that the OECD Guidelines are not legally binding. They are merely recommendations made by the OECD to its member countries[178] for the adoption of good data protection practices, within their respective jurisdictions.[179] Despite it not being mandatory, many countries have taken them into consideration in drafting domestic legislation.[180]

It is important to note that at the time of the adoption of the OECD Guidelines, being in the early 1980s, information technology had not yet exploded and developed into what it is today.

As time has progressed, the need to update the existing data protection framework was realised in the form of EU Directive 95/46/EC[181] (EU Directive). It has been said that the EU Directive evolved from the abovementioned international data protection instruments, however, the EU Directive goes further than the CoE Convention and the OECD Guidelines, by setting a higher level of protection for data subjects.[182]

3.4. EUROPEAN INSTRUMENTS

3.4.1. *EU Directive 95/46/EC*

The EU Directive, adopted on 24 October 1995, seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between member states.[183]

According to the EU Directive, member states have an obligation to provide for the enforcement of the data protection principles.[184]

[178] As of December 2020, the OECD comprises of 37 members which include all of the European Union member states as well as Australia, Canada, Chile, Colombia, Israel, Japan, Korea, Mexico, New Zealand, Turkey, the United Kingdom and the United States.
[179] See Roos op cit note 8 at 404.
[180] Yasmeen Rasool *An Examination of how the Protection of Personal Information Act will Impact on Direct Marketing and the Current Legislative Framework in South Africa* (unpublished LLM thesis, University of KwaZulu-Natal, 2017) 20-1.
[181] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 1995 Official Journal L 281/31 (cited as Directive 95/46/EC). Reference will be made to this Directive.
as the 'EU Directive', given the fact that it operates between member states of the EU.
[182] See Naude op cit note 77 at 31. See further Roos op cit note 8 at 405.
[183] See SALRC Discussion Paper op cit note 33 at 617. See further Recital 3 of the GDPR.
[184] Article 6 of the EU Directive.

These principles determine that member states must provide that personal data[185] must be:

> (a) "processed fairly and lawfully;
> (b) collected for specified, explicit and legitimate purposes;
> (c) adequate and relevant;
> (d) accurate and up to date;
> (e) only kept for the necessary period."

The EU Directive sets itself apart from the CoE Convention and the OECD Guidelines. It does so through the inclusion, for the first time in European data protection, the right to a judicial remedy if the rights of a data subject are breached. Further, providing for compensation for any damage suffered as a result of unlawful processing.[186]

3.4.2. *The General Data Protection Regulation*[187]

On 6 April 2016, the EU agreed to a major reform of its data protection framework, by adopting the General Data Protection Regulation (GDPR) which repealed and replaced the EU Directive mentioned above.[188] The GDPR entered into force across all EU member states on 25 May 2018.[189]

The significance of adopting a 'regulation' rather than a 'directive' is apparent in that with a 'directive' it is a set of goals which member states must seek to strive toward achieving, with leeway in how each country legislates such goals domestically. A 'regulation' however, applies throughout without the need for domestic adoption or transposition.[190]

---

[185] Article 2 of the EU Directive defines 'personal data' to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
[186] Article 55 of the EU Directive.
[187] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[188] Razvan Viorescu '2018 Reforms of EU Data Protection Rules' (2017) *European Journal of Law and Public Administration* 4 (2) 27-39. At 27-8. See further Article 94 (1) of the GDPR.
[189] Michelle Goddard 'The EU General Data Protection Regulation (GDPR): European regulation that has a global impact' (2017) 59 (6) *International Journal of Market Research* at 703.
[190] Anneliese Roos 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles" (2020) CILSA 53 (3) at 2 – 3. See further European Union 'Regulations, Directives and other acts' Available at: *https://europa.eu/european-union/law/legal-acts_en*. Accessed 21 April 2021.

The GDPR is intended to respond to new technological developments that have affected the ways that we collect and hold data and the way in which individuals and organisations communicate and share information.

Beyond that, the GDPR aims to put in place a harmonised framework for the protection of personal information across the EU. The harmonisation is achieved due to the fact that the GDPR is a regulation, thus amending the fragmented data protection landscape created by the EU Directive, whereby member states were provided leeway in how they legislated data protection domestically.

3.4.2.1. *Key Definitions*[191]

As with POPIA, it is crucial to understand the distinctions between the parties involved as it relates to data protection under the GDPR.

'Personal data' - protected by the GDPR is defined as "any information relating to a data subject." This is synonymous with 'personal information' as defined in POPIA.

A 'data subject' is "the identified, or identifiable, person to whom the personal data relates." Personal data includes, among other things, personal details, financial details and contractual details.

'Processing' is widely defined in the GDPR and covers, "… any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

A **'**controller' is a "natural or juristic person who determines the purposes and means of processing personal data." This is comparable with the 'responsible party' as defined in POPIA.

A 'processor' means "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." This is comparable with an 'operator' as defined in POPIA.

[191] Article 4 of the GDPR.

3.4.2.2. *Application and Scope of the GDPR*

The scope of the application of the GDPR applies materially,[192] territorially and extraterritorially.[193] Each will be examined briefly:

a) *Materially*

In terms of application, the GDPR is similar to POPIA, in that Article 2 (1) states that the GDPR applies to the processing of personal data "wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."

b) *Territorially*

The territorial scope of the GDPR is determined by Article 3 and represents a significant evolution of the EU data protection law compared to the framework defined by the EU Directive.[194]

The GDPR applies when personal data is processed in the context of the activities of an establishment of a controller or processor in the EU and applies regardless of whether the data processing takes place in the EU or not.[195]

The GDPR has a wide jurisdictional reach in that it also provides for extraterritorial application. This has the effect that the GDPR can apply to organisations that are established outside of the territory of the EU. However, this is only triggered if the processing activities are related to:

(a)"the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b)the monitoring of their behaviour as far as their behaviour takes place within the Union."[196]

[192] Article 2 of the GDPR.
[193] Article 3 of the GDPR.
[194] The European Data Protection Board 'Guidelines 3/2018 on the territorial scope of the GDPR' November 2019. Available at: *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf*. Accessed 19 February 2021.
[195] Article 3 (1) of the GDPR. For example, a pharmaceutical company with headquarters in France funds a study into the efficacy of a COVID-19 vaccine in India and receives (coded) study data from the Indian institute. Although the data processing takes place in India, it is carried out in the context of the activities of the controller or operator established in France. Therefore, the provisions of the GDPR apply to such processing through Article 3 (1).
[196] Article 3 (2) of the GDPR.

3.4.2.3. *Exceptions to the Application of the GDPR*

The GDPR, subject to certain exceptions, prohibits the processing of personal data that reveals *inter alia*: racial or ethnic origin; political opinions; religious and philosophical beliefs; genetic data; sex life and sexual orientation and trade union membership.[197]

Processing of any of these special categories of personal data is prohibited under the GDPR unless one of several conditions applies including, *inter alia*, where the data subject has given explicit consent,[198] where there is a substantial public interest,[199] where the processing is necessary for the establishment, exercise or defence of legal claims,[200] or where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[201]

3.4.2.4. *Key principles of the GDPR*[202]

At the outset it is crucial to note, that "POPIA is similar to the GDPR."[203] The GDPR lays down several key principles which controllers and processors must comply with when processing personal data. These form the core of the obligations on controllers and include the following:

a) Lawfulness, fair and transparent processing:[204] Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This essentially means that the controller must:
    i. "have a legitimate ground for processing the personal data;
    ii. not use personal data in ways that have an unjustified adverse effect on the data subject concerned;
    iii. be transparent about how the controller intends to use the personal data, and give the data subject appropriate privacy notices when collecting their personal data;
    iv. handle a data subject's personal data only in ways they would reasonably expect and consistent with the purposes identified to the data subject; and

[197] Article 9 (1) of the GDPR.
[198] Article 9 (2) (a) of the GDPR.
[199] Article 9 (2) (g) of the GDPR.
[200] Article 9 (2) (f) of the GDPR.
[201] Article 9 (2) (j) of the GDPR.
[202] R El-Gazzar & K Stendal 'Examining How GDPR Challenges Emerging Technologies' (2020) *Journal of Information Policy* (10) at 244-245.
[203] C Staunton & E de Stadler 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) *S Afr Med J*; 109 (4) at 232.
[204] Article 5 (1) (a) of the GDPR.

v. make sure that nothing unlawful is done with the personal data."[205]

b) Purpose limitation:[206] Personal data must only be collected for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. This requirement aims to ensure that the controller is clear and open about their reasons for obtaining personal data, and that what they do with the data is in line with the reasonable expectations of the individuals concerned.

c) Data minimization:[207] Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d) Accuracy:[208] Personal data must be accurate and, where necessary, kept up to date. This entails that controllers take reasonable steps to ensure the accuracy of any personal data obtained, ensure that the source and status of any personal data is clear. Further the controller must carefully consider any challenges to the accuracy of information and whether it is necessary to periodically update the information.[209]

e) Storage limitation:[210] Personal data must not be kept in a form which permits data subjects to be identified for longer than is necessary for the purposes for which the data is processed. The exceptions to this principle are: if the processing is "solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)."

f) Integrity and Confidentiality:[211] Personal data must be processed in a way that appropriately ensures its security. This includes protection against unauthorised or unlawful processing; against accidental loss, destruction or damage and using appropriate technical or organisational measures.

g) Accountability:[212] The controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.[213] To this effect, the controller must implement appropriate technical and organisational measures to meet the requirements of accountability.

---

[205] W Long, G Scali & F Blythe 'Chapter 25 – United Kingdom' in Alan Charles Raul (ed) *The Privacy Data Protection and Cybersecurity Law Review* 6 ed (2019) 373 – 398.
[206] Article 5 (1) (b) of the GDPR.
[207] Article 5 (1) (c) of the GDPR.
[208] Article 5 (1) (d) of the GDPR.
[209] ICO 'Guide to the GDPR' Available at: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.* Accessed 28 October 2020.
[210] Article 5 (1) (e) of the GDPR.
[211] Article 5 (1) (f) of the GDPR. See further, Article 32 of the GDPR in so far as measures the minimum standards of security that data controllers and processors must meet.
[212] Article 5 (2) of the GDPR.
[213] *Ibid.*

There are several measures that can be taken as suggested by the ICO, including:

i. "adopting and implementing data protection policies, appropriate to the organisation in which it is intended;
ii. adopting an approach in which data protection is achieved by design and default;
iii. putting written contracts in place with organisations that process personal data on your behalf;
iv. maintaining documentation of processing activities;
v. implementing appropriate security measures;
vi. recording and, where necessary, reporting personal data breaches;
vii. carrying out impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
viii. appointing a data protection officer; and
ix. adhering to relevant codes of conduct and signing up to certification schemes."[214]

It must be noted that the GDPR widens the scope for the rights of data subjects as it relates to access and control over the use of their data. According to Daigle and Khan, some of these "enhanced measures include a data subject's right to be forgotten, to rectify their data … and to know what the data is being used for."[215]

3.4.3. *United Kingdom's Data Protection Framework*[216]

The protection of personal information is governed by UK DPA 2018 and is the UK's third generation of data protection legislation. Its main provisions came into force on 25 May 2018; the same day as the GDPR.

Due to the withdrawal of the UK from the EU, informally known as 'Brexit' the UK had to update its data protection regulations to ensure that the standards set out in the GDPR have effect in the UK by enshrining those standards, domestically, in the law of the UK.[217]

This was achieved through a myriad of legislative action which paved the way for the withdrawal of the UK and retention of the data protection legislation of the EU. As of

[214] ICO 'Guide to the GDPR' Available at: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/*. Accessed 27 October 2020.
[215] Brian Daigle and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) *Journal of International Commerce & Economics* at 4-5.
[216] The Data Protection Act 2018 (c.12). Available at: *https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted*. Accessed 3 November 2020.
[217] Cammrynn-Lea Larsen *Data Privacy Protection in South Africa: An Analysis of Vicarious Liability in Light of the Protection of Personal Information Act 4 of 2013*. (unpublished LLM thesis, University of KwaZulu-Natal, 2019) 58. See further the Agreement on the Withdrawal of the United Kingdom and Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (the Withdrawal Agreement) 2019/C 384 I/01.

31 January 2020, and pursuant to the European Union (Withdrawal) Act of 2018,[218] in combination with the European Union (Withdrawal Agreement) Act 2020,[219] the UK ceased to be an EU member state. Accordingly, the UK entered into a transition period until 31 December 2020[220] during which it continued to be subject to EU law, including the GDPR.

This transition period has expired, however, to ensure the continuous free flow of data between the UK and the EU, the UK has incorporated the EU GDPR into the UK's domestic law under section 3 of the EU Withdrawal Act 2018, and this is confirmed through the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations of 2019.[221] Therefore, lifting the EU GDPR and forming an equivalent called the UK GDPR.[222]

According to the ICO, data collected after the end of the transition period will need to comply with the UK GDPR alongside the UK DPA 2018.[223]

Apart from referring to the UK-GDPR instead of the EU's GDPR (since the UK has left the EU), the UK DPA 2018 creates additional provisions for the processing of personal data that go beyond both the UK-GDPR and the EU's GDPR. These are mostly found in the area of national security, law enforcement and immigration which go beyond the scope of this dissertation.[224]

In light of that, when examining the UK position as it relates to data protection, there is heavy reliance on the provisions of the EU GDPR mentioned above, due to the fact that the UK has incorporated it into the form of a UK GDPR, which is to be read alongside the UK DPA 2018.

---

[218] 2018 c.16.
[219] 2020 c.1.
[220] Article 126 of the Agreement on the Withdrawal of the United Kingdom and Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community.
[221] 2019 No.419. Regulation 2, which deals with interpretation and reads as follows: 'the UK GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.'
[222] Section 3 (1) provides that 'Direct EU legislation, so far as operative immediately before exit day, forms part of domestic law on and after exit day.'
[223] ICO 'Information rights after the end of the transition period – Frequently asked questions' *https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/* Accessed on 19 February 2021. See further Keumars Afifi-Sabet 'What is GDPR? Everything you need to know, from requirements to fines' 11 March 2020. Available at: https://www.itpro.co.uk/general-data-protection-regulation-gdpr. Accessed 29 October 2020.
[224] Cookiebot 'UK Data Protection Act 2018 – 2021 Update' 18 January 2020. Available at: *https://www.cookiebot.com/en/data-protection-act-2018/.* Accessed 20 February 2021.

3.4.3.1.*Purpose*

The UK DPA 2018 aims to serve the following purposes, first, it begins by repealing and replacing the UK DPA 1998[225] as the primary piece of data protection legislation in the UK and second, aims to provide a current and comprehensive framework for data protection in the UK.[226]

The terms used in the UK DPA 2018 have the same meaning as they have in the GDPR outlined above.[227]

3.4.3.2.*Information Commissioner*

The Information Commissioner in the UK assumes largely the same job in the protection of personal information as the Information Regulator does under POPIA in South Africa.

The Information Commissioner is an independent official whose role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.[228]

3.4.3.3. *Notification of Breach*

A "personal data breach" is a wide concept, defined as any "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."[229]

Under the GDPR, the controller is obligated to notify the supervisory authority[230] of any personal data breach "without undue delay and, where feasible, not later than 72

[225] 1998 c.12
[226] Department for Digital, Culture, Media & Sport. 'Data Protection Bill: Factsheet – The Information Commissioner and Enforcement' March 2018. Available at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685645/2018-03-05_Factsheet05_Bill_ICO.pdf*. Accessed 2 November 2020.
[227] Section 5 of the UK DPA 2018.
[228] See Department for Digital, Culture, Media & Sport op cit note 226.
[229] Article 4 of the GDPR.
[230] A "supervisory authority" is an independent public authority "responsible for monitoring the application" of the GDPR so as to protect data subjects' data protection rights, which are considered "fundamental rights." An example would be the UK data protection authority—the Information Commissioner's Office or ICO.

hours after having become aware of it, . . . unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[231]

When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay.[232]

An important consideration is that in terms of POPIA, the notification in the event of a breach or security compromise differs greatly from that of the GDPR.

POPIA provides that the notification made to the Regulator must:

> "…be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system."

Thus, further guidance is needed so as to clarify what is 'reasonable' in the context of a delay in the notification of a security compromise under POPIA, taking into consideration the circumstances, of the case as they may be.

3.4.3.4. *Enforcement Provisions*

a) *Complaint*

Similar to POPIA, the GDPR provides a route for a data subject to lodge a complaint with a supervisory authority.[233] The avenue to lodge a complaint under the GDPR has already been utilised across Europe. One example being in 2019, where complaints were filed against Google to the data protection regulators in France and Germany and seven other EU countries, on the issue of how data is being used in online advertising.[234]

Moreover, Articles 78 and 79 of the GDPR expressly provide for a right to an effective judicial remedy against either the supervisory authority or controller or processor.

---

[231] Article 33 (1) of the GDPR. See section 67 of the UK DPA 2018. See also, G Voss 'European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting' (2017) *The Business Lawyer* (72).

[232] Article 34 of the GDPR.

[233] Article 77 of the GDPR.

[234] Reuters 'Google faces privacy complaints in European countries' 4 June 2019. Available at: *https://www.reuters.com/article/us-eu-google-privacy/google-faces-privacy-complaints-in-france-germany-7-other-eu-countries-idUSKCN1T51G3*. For a comprehensive list of complaints see Nathan Trust 'GDPR Fines and Complaints' Available at: *https://www.nathantrust.com/gdpr-fines-penalties.* Accessed 19 February 2021.

b) *Civil Remedies*

Under Article 82 (1) the GDPR makes specific provision for individuals to bring private claims against controllers and processors. This is available to any person who has suffered material or non-material damage as a result of a breach of the GDPR. Such a person has the right to receive compensation from the controller or processor.

The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss. This is reflected through s 168 (1) of the UK DPA 2018 which deals with compensation for contravention of the GDPR and states that "the right to compensation for material or non-material damage, includes distress."

The landmark decision which confirms the above in the UK is *Google v Vidal Hall.*[235] It is important to note that this case was decided under the UK DPA 1998. The UK DPA 1998 was enacted to give effect to the EU Directive.[236]

The claimants, who were respondents to this appeal, involved three individuals who used Apple computers between summer 2011 and 17 February 2012 and used Apple's "Safari" browser to access the internet during that time.[237]

They claim that the defendant (here the appellant) collected their private information, namely their browser-usage, without their knowledge or consent by means of 'cookies'[238]. They claim the defendant then used this information in offering commercial services to advertisers.

On 12 June 2013, the claimants issued proceedings in England & Wales for misuse of private information, breach of confidence and breaches of the UK DPA 1998, including compensation for distress under section 13.

Section 13 of the UK DPA 1998 provides as follows:

[235] [2015] EWCA Civ 311. Available at: *https://www.bailii.org/ew/cases/EWCA/Civ/2015/311.html.* Accessed 25 November 2020.
[236] Mosley v Google Inc [2015] EWHC 59 (QB) at para 10. Available at: *https://www.bailii.org/ew/cases/EWHC/QB/2015/59.html.* Accessed 26 November 2020.
[237] Supra note 234 at para 3.
[238] 'Cookies' are text files with small pieces of data that are used to identify a computer as a computer network is used.

1. "An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.
2. An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if—

    (a) the individual also suffers damage by reason of the contravention, or

    (b) the contravention relates to the processing of personal data for the special purposes."

The key issue for the purposes of this dissertation, in this case was, whether the meaning of 'damage' in section 13 of the UK DPA 1998 provided for compensation without patrimonial loss.[239]

In reaching a decision, the court held that the UK DPA 1998 was intended to give effect to the EU Directive. Specifically, Article 23 which mandates that:

> "Member states shall provide that any person who has suffered damage as a result of an unlawful processing operation or any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage sufferance."

In contrast, section 13(2) of the UK DPA 1998 provided for compensation for distress, however, only if "(a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for special purposes." Special purposes being defined as one or more of journalistic, artistic or literary purposes.

The Court of Appeal decided that the meaning of the word 'damage' for the purposes of Article 23 does not distinguish between pecuniary and non-pecuniary damage.[240] Further the court held that the comments of Buxton LJ on this point in a prior case, *Johnson v Medical Defence Union*,[241] did not form binding precedent.

The court identified that the exclusion of the right to compensation for distress where the conditions stated in section 13 were not satisfied was a fundamental feature of the

[239] Supra note 234 para 13.
[240] Supra note 234 para 79.
[241] [2007] 96 BMLR 99.

UK DPA 1998, and the right to damages under section 13 could not be interpreted in a way compatible with the right under Article 23 of the EU Directive.[242]

The court instead disapplied[243] the domestic provisions on the grounds that Article 47 of the EU Charter of Fundamental Rights[244] guaranteed an effective remedy to violations of rights and freedoms under EU law, particularly the Charter's rights to respect for private and family life, home and communications[245] and right to the protection of personal data.[246]

The major effect of this decision is that it will be possible for data subjects who make claims for compensation for a breach under the recently updated UK DPA 2018 to claim damages for distress even where no pecuniary loss has been suffered.

What needs to be shown in order for a claim of distress by a data subject to be awarded compensation in the context of section 13 (2) of the UK DPA 1998 was laid out in *Halliday v Creation Consumer Finance Limited*[247] by Lady Justice Arden, where £750 (R15 000) was awarded for distress:

> "It is clear that the claimant has to be an individual, that he has to have suffered distress, and that the distress has to have been caused by contravention by a data controller of any of the requirements of the Act."[248]

This position has been reflected in POPIA through section 99 (3) whereby payment of damages as compensation can be sought for patrimonial and non-patrimonial loss. However, it must be critically pointed out that there has not been a case brought before a court which confirms this position into South African law.[249]

---

[242] Harry Kinmonth & Elizabeth Wiggin explain that given the fact that a directive provides leeway in how an EU member adopts the directive domestically, for example DPA 1998 in the UK, that the court found that s13 (2) had not transposed Article 23 of the Directive effectively. Available at: *https://www.lexology.com/library/detail.aspx?g=17b0d098-71a3-4925-a942-511d0bc52491*. Accessed 15 April 2021.

[243] To 'disapply' means to make (a law or legal requirement) not applicable or invalid. Collins English Dictionary. Available at: *https://www.collinsdictionary.com/dictionary/english/disapply*. Accessed 14 April 2021.

[244] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02. Available at *https://www.refworld.org/docid/3ae6b3b70.html*. Accessed 1 February 2021.

[245] Article 7 of the EU Charter of Fundamental Rights.

[246] Article 8 (1) of the EU Charter of Fundamental Rights.

[247] [2013] EWCA Civ 333. Available at: *https://www.bailii.org/ew/cases/EWCA/Civ/2013/333.html*. Accessed 3 February 2021.

[248] *Ibid* para 20.

[249] See Chapter Two at 2.14.

3.4.3.5.*Administrative Fines*

The most important provision of the GDPR for the purposes of this dissertation is found in Article 83. For this reason, the Article in its entirety bears quotation.

Article 83 provides that when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

a) "the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;
b) the intentional or negligent character of the infringement;
c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them;
e) any relevant previous infringements by the controller or processor;
f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
g) the categories of personal data affected by the infringement;
h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
i) where measures have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

These factors have been adapted and incorporated into the UK DPA 2018 and are found in section 155 (3).

A recent example of the UK ICO weighing up the considerations for determining the amount payable in a penalty notice, provided for by section 155 of the UK DPA 2018 and Article 83 of GDPR is evident in the breach involving Ticketmaster UK Limited.

In this matter the ICO fined Ticketmaster £1.25 million for failing to keep its customers' personal data secure.[250]

The data breach, which "included names, payment card numbers, expiry dates and CVV numbers, potentially affected 9.4 million of Ticketmaster's customers across Europe including 1.5 million in the UK."[251]

In the determination of whether to issue a fine and, if so, the amount, the ICO considered several factors, including:

(a) *The nature, gravity and duration of the failure*

The ICO characterized this breach as a significant contravention of the GDPR, which occurred between 25 May 2018 to 23 June 2018.[252]

(b) *Any action taken by the controller or processor to mitigate the damage suffered by data subjects*

Ticketmaster created a website where customers and media could receive information about the breach. Further, Ticketmaster arranged for 12 months of credit monitoring for individuals affected.[253]

(c) *The degree of responsibility of the controller or processor*

The ICO found that Ticketmaster failed in its obligations under Article 5 (1) (f) and Article 21 (1) of the GDPR and relevant sections of the UK DPA 2018.

These provisions require that personal data must be processed in a way that appropriately ensures its security. This includes protection against unauthorised or unlawful processing; against accidental loss, destruction or damage whilst using appropriate technical or organisational measures.

The ICO noted that this requires regard to considerations including "the likelihood of attack, its severity and what appropriate controls were available at the time." [254]

(d) *Any relevant previous infringements*

---

[250] ICO 'ICO fines Ticketmaster UK Limited £1.25million for failing to protect customers' payment details' 13 November 2020. Available at: *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/*. Accessed 20 February 2021.

[251] *Ibid.*

[252] ICO Penalty Notice – Ticketmaster UK Limited. Case Ref: COM0759008 at 52. 13 November 2020. Available at: *https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf*. Accessed 20 February 2021.

[253] *Ibid* at 54.

[254] *Ibid* at 55.

No other compliance matters or infringements were taken into account by the ICO when setting the amount of the penalty.[255]

(e) *Degree of cooperation with supervisory authority*

The ICO noted that "Ticketmaster has fully co-operated with the Commissioner during this investigation and has provided evidence upon request, save as to certain financial information." [256]

(f) *Categories of personal data affected*

The ICO noted that the personal data that was potentially affected was sensitive and "likely to have included … names and contact details … usernames and passwords … bank details, credit card, debit card and CVV numbers."

(g) *Manner in which the infringement became known to the Commissioner*

Ticketmaster reported this incident to the Commissioner on 23 June 2018. However, Barclays Bank, Monzo Bank and other third parties informed Ticketmaster of a potential personal data breach as early as February 2018.[257]

3.4.3.6. *Penalties*

Penalties under the GDPR, which are applicable in the UK are similar to the penalties provided for in POPIA, however exponentially greater in terms monetary value. For severe violations, listed in Article 83(5) of the GDPR,[258] the penalty takes the form of a fine.

The fine that can be levied may be up to €20 million Euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding financial year, whichever is higher.

For less severe violations, listed in Article 83(4) of the GDPR[259] fines of up to €10 million Euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding financial year, whichever amount is higher.

3.5. OBSERVATIONS

[255] *Ibid.*
[256] *Ibid.*
[257] *Ibid* at 2 and 56.
[258] Serious violations include failure to adhere to the basic principles for processing and infringement of a data subjects rights.
[259] Less serious violations include failure to meet the obligations on the controller and processor; failure to meet the obligations of certification or of the monitoring body.

When one compares POPIA with the international and foreign protection instruments discussed above and some of the approaches that have been adopted, namely in the UK and EU, there are striking similarities, especially in so far as it relates to the core privacy principles or conditions and the rights of a data subject.

Both establish the framework in which data can be processed, lawfully, and avenues for appropriate remedies and sanctions to be levied in the event of contravention.

However, it is submitted that the UK DPA 2018 and GDPR go further than POPIA, in the considerations or factors that must be considered when issuing an administrative fine (POPIA and GDPR) or penalty notice as it is referred to in the UK DPA 2018.

The inclusion of additional factors in our law, in the context of civil remedies, at the discretion of the court, or additional factors when issuing an administrative fine by the Regulator through s 109 (3), will further shape our law and differentiate between various breaches of personal information.

Given the fact that there has not been a case to date, brought before a court in terms of POPIA, the considerations of the court are yet to be seen. Moreover, there has yet to be an administrative fine, issued by the Regulator in terms of POPIA for non-compliance. There are pertinent factors which are absent from POPIA[260] which are relevant in the protection of personal information, and in the context of, either, the determination of a civil action, or, in the issuance of an administrative fine.

These factors are:

a) "any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;
b) the degree or responsibility of the controller or processor taking into account technical and organisational measures by the controller;
c) the degree of co-operation with the Commissioner;
d) the manner in which the infringement became known to the Commissioner;
e) adherence to approved codes of conduct or certification mechanisms; (although the certification mechanisms do not form part of South African law as it stands.)
f) any other aggravating or mitigating factor applicable to the circumstances of the case; and
g) whether the penalty would be effective, proportionate, and dissuasive."[261]

[260] See Chapter Two – at 2.15.3.
[261] Section 109 (3) of POPIA.

The next chapter will build on the submission above and explore domestic breaches, occurring in South Africa and analyse how the inclusion of additional considerations could improve POPIA and shape the determination in the event of a breach and subsequent administrative fine.

CHAPTER FOUR: APPLICATION OF POPIA TO RECENT DATA BREACHES IN SOUTH AFRICA

4.1. INTRODUCTION

South Africa has not been immune from breaches or the exposure of personal information. Breaches have continued to occur throughout the process of bringing data protection legislation into force in South Africa.

The aim of this chapter is to take what has been discussed in Chapter Two (POPIA) and the EU/UK interpretation of data protection in Chapter Three and contrast the two in order to ascertain whether there are lessons that can be gleaned for South Africa.

To identify what can be learnt with a focus on the enforcement of the respective data protection regimes, breaches local to South Africa will be viewed in light of the above.

Specifically breaches involving Ster-Kinekor, eThekwini Municipality and Experian, all of which have occurred prior to POPIA taking full force and effect.

The above breaches will be viewed through the lens of what is to be expected of a body in the event of a breach, from an internal and external point of view. The rationale is because POPIA and the Regulations now place obligations on both public and private bodies in the event of a breach, to take measures internally to ensure compliance.

The external measures in the event of a breach, are, for the purposes of this dissertation, when the public becomes aware of the occurrence of a breach for example, when the required notification is made to either the Regulator or data subjects or both.

Further, what lessons the EU/UK framework can teach South Africa in the context of the factors to be considered when levying an administrative fine (POPIA and GDPR) or penalty notice (UK DPA 2018).

4.2. POPIA IN THE EVENT OF A BREACH

As noted in Chapter Two, POPIA requires compliance with the eight conditions[262] when processing personal information for such processing to be deemed lawful:

(a) 'Accountability' as referred to in section 8;

(b) 'Processing limitation' as referred to in sections 9 to 12;

(c) 'Purpose specification' as referred to in sections 13 and 14;

[262] See Chapter Two at 2.8 for a deeper analysis of the conditions.

(d) ‘Further processing limitation’ as referred to in section 15;
(e) ‘Information quality’ as referred to in section 16;
(f) ‘Openness’ as referred to in sections 17 and 18;
(g) ‘Security safeguards’ as referred to in sections 19 to 22; and
(h) ‘Data subject participation’ as referred to in sections 23 to 25.[263]

4.2.1. INTERNAL MEASURES

In the context of what is required of a responsible party so as to safeguard against the occurrence of security compromises or breaches, POPIA and the measures required will be viewed from an internal and external aspect.

The starting point, internally, is the security safeguards, which is one of the eight essential conditions for the lawful processing of personal information and is referred to in sections 19 – 22 of POPIA.

Section 19 places an obligation on a responsible party to:

> “…secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:
>
> (a) loss of, damage to or unauthorised destruction of personal information; and
> (b) unlawful access to or processing of personal information.”

In practice, such measures likely already exist within a public or private body, depending on the type of personal information processed and nature thereof, through, for example: access control, the use of firewalls on a network, the encryption of devices and of information, pseudonymisation, utilising appropriate antivirus software, back-ups, and unique alphanumeric passwords.

POPIA does proffer guidance on how the above obligation may be met, stating that the responsible party must take measures to:

(a) “identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against the risks identified;

[263] See further, J Neethling, JM Potgieter, A Roos ‘Neethling on Personality Rights’ (2019) at 381.

(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards."[264]

Further guidance is given through section 19 (3) whereby POPIA states that the responsible party "must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."[265]

Section 20 extends such obligations by requiring similar compliance by bodies who have been instructed or authorised by a responsible party to process information on their behalf. Such parties are referred to as "operators" in terms of POPIA[266] and may only process personal information with the knowledge or authorisation of the responsible party and must treat such personal information as confidential. The responsible party, however, remains responsible for the conduct of the operator in its handling of the personal information.[267]

Section 21 (1) of POPIA requires that the responsible party, by way of a written agreement or contract, with the operator, ensures that the security measures implemented by the operator are sufficient and in accordance with the requirements of section 19 mentioned above.

The operator is further required to "notify the responsible party where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person."[268]

Moreover, at the forefront of ensuring compliance with POPIA, internally, is the Information Officer[269] of a public or private body. The duties and responsibilities of the

[264] Section 19 (2) of POPIA.
[265] See Chapter Two at 2.8.7. For example, see Control Objectives for Information Technologies (COBIT 2019) and ISO 27001.
[266] See Chapter Two at 2.3.
[267] Section 8 of POPIA, Condition 1: Accountability.
[268] Section 21 (2) of POPIA.
[269] Information Regulator 'Guidance Note on Information Officers and Deputy Information Officers' 1 April 2021 Available at *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf*. Accessed 12 April 2021.

Information Officer laid out in Chapter Two[270] provides an overview of the role they will play in an organisation.

It must be noted that the text of POPIA itself does not require any specific policies to be implemented into an organisation. However, given the nature of POPIA being more principle based rather than rule based, it provides to an extent, leeway, to public and private bodies to assess their own organisation and the nature, manner and extent of the personal information that they process and draft policies which are suited to their operations, to ensure compliance with POPIA.

In practice, this would place an obligation on public and private bodies to draft their own POPIA policies, which may include *inter alia*: privacy policies, data breach management policies, and cookie policies, as the case may be.

The response to a security compromise or breach, is headed by the Information Officer, in connection with other key parties within an organisation, for example the IT manager or head of human resources as the case may be.

In my view, an example of the likely steps that could be taken in a data breach policy, internally, may include:

a) *Identification and initial assessment of the incident*[271]

The Information Officer shall conduct an initial assessment of the incident by establishing:

i. if a personal data breach has taken place;
ii. what personal data is involved in the breach;
iii. the cause of the breach;
iv. the extent of the breach (how many individuals are affected);
v. the potential harm to affected individuals; and
vi. measures to contain the breach.

b) *Containment and recovery*

The organisation must take immediate and appropriate steps to limit the identified data breach. This entails that the Information Officer shall establish:

[270] See Chapter Two at 2.13.
[271] For example see Altorvox 'Data Breach and Security Incident Management Policy' Available at: *https://www.altorvox.co.za/wp-content/uploads/AV-DATA-BREACH-SECURITY-INCIDENT-MANAGEMENT-POLICY.pdf* Accessed 23 May 2022.

i. who within the organisation needs to be made aware of the breach? (For example, the legal department, IT department, human resources, and public relations.)
ii. what such persons are expected to do in order to contain the breach. (Which may include changing passwords, closing a compromised section of the network, finding lost equipment, contracting external experts.)
iii. whether measures can be taken to limit the damage caused by the breach. (This may include the use of backups or mirrored drives).
iv. whether circumstances dictate that affected individuals are to be notified immediately (where there is a high level of risk of serious harm to affected individuals).
v. whether it is appropriate to inform the South African Police Services. (For example in cases involving theft or other criminal activity.)

c) *Risk Assessment*[272]

Assessment of risk arising from a personal data security breach is to be conducted by the likelihood of consequences and the severity thereof.[273]

In assessing a risk arising from a personal data security breach, the Information Officer shall consider, in consultation with relevant stakeholders, the potential adverse consequences for individuals, i.e., how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

Risks to be assessed include, but are not limited to:

i. risks for the individuals affected;
ii. what are the potential consequences for individuals?
iii. how serious are these potential consequences?
iv. what is the likelihood of these consequences manifesting?[274]

d) *Incident Report*

Following the risk assessment, and irrespective of the level of risk, the Information Officer must compile an incident report detailing:

i. a summary of the breach;
ii. if known, employees and other persons involved in or responsible for the breach;

[272] This method is in accordance with the GDPR Article 29 - Working party guidelines and involves; the systematic approach of estimating the magnitude of risks (risk analysis); the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation). See further, Article 35 of the GDPR together with Recital 84 – 'Risk evaluation and impact assessment'.
[273] See Article 32 of the GDPR read with Recital 77 – 'Risk Assessment Guidelines'. In terms of POPIA, see s 19 (2) (a – d). See further Chapter Two at 2.8.7.
[274] Juta, 'POPIA Data Breach Policy and Response Plan' Available at: *https://jutacomplinews.co.za/media/filestore/2021/04/POPIA_breach_plan.pdf.* Accessed 6 February 2022.

iii. any details in respect of information, IT equipment or systems involved, lost or compromised in the breach;
iv. details as to how the breach occurred;
v. actions taken and proposed to resolve the breach and the consequences flowing therefrom;
vi. potential consequences yet to materialise; and
vii. recommendations to prevent the re-occurrence of the breach.[275]

4.2.2. EXTERNAL MEASURES

The requirements imposed by POPIA which can outwardly be seen by data subjects and the larger public when certain sections are triggered can be seen as the external measures which a responsible party or operator, must take in the event of a breach.

4.2.2.1. Notification of security breach

It has been noted that "Organisations previously had no legal obligation as it relates to notification of individuals and companies, when they experienced data breaches, whose data has been compromised."[276] However, the promulgation of POPIA has changed this position.

Section 22 of POPIA is concerned with the notification of security breaches. This requires that:

(1) "Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—
(a) the Regulator; and
(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established."

In so far as when notification of the breach must be made, POPIA provides:

(2) "The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise…"

With respect to the manner in which the notification must be made, POPIA states that:

[275] *Ibid.*
[276] Louise Muller 'Are you working on the protection of personal information?' (2020) *Chartered Institute of Government, Finance, Audit & Risk Officers (CIGFARO)* 21 (2) at 29.

The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

a) "mailed to the data subject's last known physical or postal address;
b) sent by e-mail to the data subject's last known e-mail address;
c) placed in a prominent position on the website of the responsible party;
d) published in the news media; or
e) as may be directed by the Regulator."[277]

The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise. This includes:

a) "a description of the possible consequences of the security compromise;
b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;
c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information."[278]

4.3. LOCAL BREACHES[279]

Background of a few breaches having occurred in South Africa will be examined, and then viewed, hypothetically, through a lens of potential lessons to be learnt from the European data protection framework.

4.3.1. *Ster-Kinekor*[280]

In 2016, prior to the establishment of the Information Regulator and commencement of the majority of the provisions of POPIA, Ster-Kinekor suffered a breach of personal information. Ster-Kinekor had a security vulnerability on its website which resulted in the personal information of 6 million users being leaked. The personal information included: names; addresses; birth dates; genders and plain text passwords.

[277] Section 22 (4) (a – d) of POPIA.
[278] Section 22 (5) (a - d) of POPIA.
[279] For an overview of additional breaches and the nature thereof, see Van Niekerk 'An Analysis of Cyber-Incidents in South Africa' (2017) *The African Journal of Information and Communication (AJIC)* 20 at 118.
[280] Tefo Mohapi 'South Africa's notable data breaches and data leaks in the past half-decade' iAfrikan 27 October 2020. Available at: *https://iafrikan.com/2020/10/27/south-africa-biggest-top-data-breaches-leaks/* Accessed 15 February 2021.

4.3.2. *eThekwini Municipality*[281]

That same year, eThekwini municipality launched its new eServices website. Another security vulnerability on the website allowed anyone with an internet connection and a web browser to view the municipal account information and personal records of over 98,000 residents of the municipality.

It is crucial to point out that often people willingly put out their personal information, such as their names, cell phone numbers and email addresses, for example, on various social media platforms like Facebook and LinkedIn. However, seldom is information like ID numbers, physical addresses or passwords made publicly available, willingly.

4.3.3. *Experian*

The breach involving Experian occurred after the proclamation of commencement of POPIA, but before the Act took full force and effect. Therefore, there is more information available publicly to test against the provisions of POPIA, which came into force in July 2021. This is because businesses, during the one-year grace period, had begun putting in measures to ensure compliance with the provisions of POPIA.

The background to this breach is that Experian, a consumer credit reporting company, said on 19 August 2020 that it "experienced a breach of data which has exposed some personal information of as many as 24 million South Africans, and 793,749 business entities."[282]

The Information Regulator released a media statement on 20 August 2020 regarding the breach, in which it said the following:[283]

> "… The Regulator became aware of the breach on 6 August 2020 when Experian sent an email to the Regulator requesting an urgent meeting to discuss a matter." [284]

[281] *Ibid*. See Kyle Venktess 'eThekwini shuts down e-services after user data leak' Fin24 8 September 2016. Available at: *https://www.news24.com/fin24/tech/news/ethekwini-shuts-down-e-services-after-user-data-leak-20160908.* Accessed 17 February 2021.

[282] Business Tech. 'Personal information of South Africans posted online after major data breach – here's what leaked' 4 September 2020. Available at: *https://businesstech.co.za/news/technology/431484/personal-information-of-south-africans-posted-on-dark-web-after-major-data-breach-heres-what-leaked/* Accessed 3 October 2020.

[283] Provided through s 40 (1) (a) (iii) of POPIA.

[284] Media Statement of the Information Regulator on the Experian Security Breach. Available at: *https://justice.gov.za/inforeg/docs/ms-20200820-Experian.pdf*. Accessed 1 October 2020.

Experian sent a report to the Regulator on 14 August 2020 in which it advised the Regulator that it was a victim of a fraudulent misrepresentation that occurred in *May 2020.*[285] (My emphasis).[286]

Thus, if hypothetically, POPIA were in full force and effect when the above-mentioned breaches took place and the Regulator after conducting any and all relevant investigations into such breaches, found that:

a) the body concerned did not have adequate policies or security measures in place; or
b) the body did not comply with any one of the eight conditions for lawful processing of personal information; or
c) the body did not comply with any provision of the Act which constitutes an interference with the protection of personal information of a data subject as referred to in section 73; for example, the notification requirement of section 22.

The Regulator would then be empowered through section 109[287] to impose an administrative fine on such body, up to a maximum of R10 million. The Regulator in doing so would rely on section 109 (3); which contains the factors that must be weighed up in deciding the amount payable in the administrative fine.

4.4. OBSERVATIONS AND LESSONS

The analysis of POPIA coupled with the facts of Ster-Kinekor, eThekwini and Experian give credence to the need for legislation protecting personal information. Further, it gives insight into what is expected of responsible parties in the event of a breach both internally and externally.

More specifically, when one views the breaches of Ster-Kinekor, eThekwini and Experian through the lens of the factors found in s 109 (3), it becomes clear that POPIA provides the Regulator with appropriate considerations to weigh up when levying an administrative fine.

[285] *Ibid.*
[286] In terms of POPIA, credit bureaus are private bodies and would be classified as responsible parties. They are obligated to comply with the eight conditions for lawful processing of personal information.
[287] See Chapter Two at 2.15.3.

Section 109 (3) (c) differentiates between the breaches above; in that it is concerned with the number of data subjects affected or potentially affected by contravention of POPIA. Ster-Kinekor and Experian involved millions of South Africans, however, eThekwini involved less than 100 000 people.

Section 109 (3) (a) further highlights the nuances in being able to make a distinction between breaches, as this provision is concerned with the nature of the personal information involved. Thus, even though the Ster-Kinekor breach involved millions of people, the information that was exposed was not as sensitive or invasive on the privacy of a data subject as compared with Experian and eThekwini which reportedly contained ID numbers and physical addresses.

I submit that there are lessons to be gleaned for South Africa from the UK and EU framework of data protection. As identified in Chapter Three,[288] the UK DPA 2018 and the GDPR go further than POPIA as it relates to the factors or considerations when levying an administrative fine.

For example, in Article 83 (2) of the GDPR and s 155 (3) of the UK DPA 2018, factors to be considered include:

a) "the manner in which the infringement became known to the Commissioner";
b) "the degree of co-operation with the Commissioner"
c) "any action taken by the controller or processor to mitigate the damage suffered by data subjects"

In light of the facts surrounding Experian, the inclusion of additional factors like "the manner in which the infringement became known" as well as "the degree of co-operation" will clearly provide a contrast between on the one hand, a responsible party who notifies the Regulator of their own accord, which Experian have done, and co-operates with such authority and on the other hand, a responsible party who does not notify the Regulator and the Regulator becomes aware of a breach through third parties.

For example, in relation to (c) above, if one bears in mind the facts of Ticketmaster discussed in Chapter Three,[289] the ICO noted that Ticketmaster took action to mitigate

[288] See Chapter Three at 3.4.4
[289] See Chapter Three at 3.4.3.5.

the damage suffered by data subjects through arranging 12 months of credit monitoring for individuals affected.

Experian similarly have put measures into place to allow consumers to view their Experian credit report. The inclusion of "any action taken by the responsible party to mitigate the damage suffered by data subjects" would allow for further consideration and appreciation of responsible parties and their conduct subsequent to a breach.

Therefore, the inclusion of additional factors in so far as it relates to the considerations when imposing an administrative fine, would allow the Regulator (when going through the balancing process of s 109) to further differentiate and appreciate the scale and severity of a breach and the conduct of a responsible party in responding to a breach and their conduct with the Regulator.

Further, as there is no precedent, meaning no case has been brought in terms of POPIA before a court in terms of section 99, the above-mentioned factors could further contrast cases involving breaches and leaks of personal information. The contrast being either in the determination of a civil case or, in deciding an appropriate amount for compensation. This, however, is solely at the discretion of the court.

4.5. CONCLUSION

If, hypothetically, the Experian breach proceeded, for example, to a place where a data subject instituted a civil action in terms of section 99, and a court found that Experian had interfered with the personal information of a data subject in terms of section 73. For example, failure to comply with the eight conditions for the lawful processing of personal information, compensation will be awarded at the discretion of the court.

Further if the Regulator investigates and determines that Experian has committed an offence in terms of POPIA, an infringement notice coupled with an administrative fine may be levied against Experian.

An effect of such patrimonial sanction has been noted by Milo and Ampofo-Anti, in that "tightening-up security measures only after a breach has occurred will become an expensive luxury."[290]

[290] D Milo & O Ampofo-Anti 'A Not So Private World' (2014) *Without Prejudice* 14 (9) at 30-2.

With that in mind, being able to determine appropriate amounts to be awarded by courts or levied by the Regulator that is commensurate with the scale and severity of the breach and the conduct of the responsible party, is vital.

It is therefore submitted that there are additional factors which must be incorporated into South African law, to further guide and differentiate between cases and breaches and the conduct of public and private bodies to such breaches, in the context of civil remedies, and further, in the context of administrative fines.

CHAPTER FIVE: CONCLUSION AND SUGGESTIONS FOR SOUTH AFRICA

5.1. INTRODUCTION

POPIA is an excellent start at legislating the protection of personal information, in harmony with international standards.[291]

Roos notes that:

> "POPIA is a comprehensive, general law that governs the processing of personal information by both the public and the private sectors. It provides for a set of data privacy principles; provides heightened protection for sensitive information; establishes an independent oversight body to ensure compliance; and gives data subjects such rights as the right to be informed of the processing of personal information relating to them, of access to that information and to have incorrect information rectified and provides subjects with civil remedies to enforce their rights."[292]

The promulgation of POPIA gives credence to the constitutional right to privacy and provides various mechanisms for a data subject, to hold the responsible party accountable and liable for failing to protect personal information, and therefore infringing on their right to privacy.

However, it has been critically pointed out that reference to international standards in the preamble of POPIA "implies that the legislature had considered international conventions and precepts."[293]

This is true to an extent, however, upon closer inspection it is clear that the considerations of the UK DPA 2018 and GDPR, in the context of enforcement provisions, go further than POPIA as far as the factors to be considered are concerned.

5.2. SUGGESTIONS FOR SOUTH AFRICA

Consequently, I submit that there are areas which must be further clarified, and further structure given, most notably for the purpose of this dissertation, is the inclusion of the following factors into POPIA, when either awarding compensation in terms of the civil

[291] See Lea Larsen op cit note 217 at 32. See further, Roos in Van der Merwe op cit note 65 at 478.
[292] *Ibid.*
[293] See Millard & Bascerano op cit note 97 at 37.

remedies provision of section 99 or, in the context of administrative fines under section 109 (3).

These factors are found in section 155 (3) of the UK DPA 2018 and Article 83 of the GDPR, which, if adapted into our legal framework for the protection of personal information, can prove beneficial.

These are:

a) any action taken by the responsible party or operator to mitigate the damage or distress suffered by data subjects;
b) the degree of responsibility of the responsible party or operator taking into account technical and organisational measures of the responsible party;
c) the degree of co-operation with the Information Regulator;
d) the manner in which the infringement became known to the Information Regulator;
e) any other aggravating or mitigating factor applicable to the circumstances of the case;
f) whether the administrative fine would be effective, proportionate, and dissuasive.

The incorporation of the factors of the UK DPA 2018 and GDPR; as adapted to the South African context will bring about the following;

a) Give further structure to our very young protection of personal information framework, and as a consequence of that, naturally, it will aid in the development of South African data protection law.
b) It is in step with the aims and objectives of POPIA, which in the preamble states is to:

> "regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests."[294]

c) It will align our law with the UK and Europe which is logical given their maturity with respect to data protection. Moreover, the established fact that our law, through POPIA, is significantly based on the same principles as the UK and EU respectively. This is confirmed again, by De Bruyn,[295] where the author tabulates the principles which underpin POPIA and the UK DPA 2018 and continues by saying that:

[294] See POPIA op cit note 44.
[295] M De Bruyn 'The Protection of Personal Information (POPI) Act – Impact on South Africa' *International Business & Economics Research Journal.* (2014) 13 (6) at 1319.

> "It is apparent … that the core principles on which both of the acts are based are significantly similar. It could therefore be deduced that it is reasonable to expect the enforcement of both acts will lead to similar outcomes."[296]

d) Given the fact that the principles are largely the same, it makes sense to also consider largely the same factors when deciding a civil claim or with respect to the Regulator issuing an administrative fine.
e) Moreover, it will clearly distinguish between responsible parties who suffered a breach or security compromise but did everything reasonably practical as required by POPIA. Compared with responsible parties who fall short of the requirements of POPIA as it relates to the conditions for the lawful processing of personal information, notification requirements and other provisions of POPIA.

With the above proffered; exactly how this would be implemented remains to be seen. However, there are avenues available to incorporate the factors of the UK DPA 2018 or GDPR into South African law.

i. Although it is not the discretion of the court to make legislation, the Constitutional Court has accepted that whilst the primary vehicle for law reform in South Africa should be the legislature, South African courts are under a general obligation to develop the common law when it deviates from the spirit, purport and objects of the Bill of Rights.[297]

   Therefore, when a data subject institutes a civil action against a responsible party in terms of POPIA, the court could at their discretion, incorporate any of the abovementioned factors in deciding the matter, as the case may be.

ii. The more likely avenue is for the Regulator, who is empowered through s 40 (1) (b) (iv) of POPIA which states:

> "The powers, duties and functions of the Regulator in terms of this Act, are to monitor and enforce compliance by, reporting upon request or on its own accord, to Parliament from time to time on any policy matter affecting the protection of the personal information of a data subject**,** *including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the personal information of a data subject.*" (My emphasis).

[296] *Ibid.*
[297] See Lea Larsen op cit note 217 at 20. See also *Carmichele v Minister of Safety and Security and Another* 2001 (4) SA 938 (CC) at 39.

iii. This is further supported by s 40 (1) (e) (ii) of POPIA, which provides the Regulator the ability to:

> "To conduct research and report to Parliament – on any other matter, including necessary legislative amendments, relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention."

POPIA and the promulgation thereof has and will change the data protection landscape in South Africa, forever. It is without a doubt that POPIA will have to be amended and updated to keep the legal arena of protecting personal information abreast with the ever-marching technological advancements.

The submission made in this dissertation, of the inclusion of the above factors as it relates to the considerations at play when imposing an administrative fine, is merely one aspect, and one contention, which will inevitably be followed by more to come in the future from the courts, the Regulator and academics in the field.

6. BIBLIOGRAPHY

6.1. PRIMARY SOURCES

6.1.1. *Legislation*

Commencement of certain sections of the Protection of Personal Information Act in Proc R21 *GG* 43461 of 22 June 2020.

Consumer Protection Act No 68 of 2008.

Constitution of the Republic of South Africa Act 200 of 1993 (Interim Constitution).

Constitution of the Republic of South Africa, 1996. ("The Constitution").

Electronic Communications and Transactions Act No 25 of 2002.

The Promotion of Access to Information Act No 2 of 2000.

The Protection of Personal Information Act No 4 of 2013.

Regulations Relating to the Protection of Personal Information Act (Act No. 4 of 2013) in GN 1383 GG 42110 of 14 December 2018.

6.1.2. *Foreign Legislation*

Data Protection Act 1998. c.29.

Data Protection Act 2018. c.12.

Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations of 2019. No. 419.

European Withdrawal Act of 2018 c.16.

European Withdrawal Agreement Act of 2020. c.1.

6.1.3. *Case Law*

Carmichele v Minister of Safety and Security and Another 2001 (4) SA 938 (CC).

Delsheray Trust and others v ABSA Bank Limited [2014] JOL 32417 (WCC).

H v W [2013] 2 All SA 218 (GSJ).

Herholdt v Wills 2013 (2) SA 530 (GSJ).

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others 2001 (1) SA 545 (CC).

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC).

National Media Ltd v Jooste 1996 (3) SA 262 (A).

O'Keeffe v Argus Printing and Publishing Co Ltd [1954] 3 All SA 159 (C).

6.1.4. *Foreign Case Law*

Google Inc v Vidal Hall [2015] EWCA Civ 311.

Mosley v Google Inc [2015] EWHC (QB).

Johnson v Medical Defence Union [2007] 96 BMLR 99.

Halliday v Creation Consumer Finance (Pty) Ltd [2013] EWCA Civ 333.

6.1.5. *International Instruments*

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, 108 Council Eur. T.S. ("CoE Convention")

Organisation for Economic Co-operation and Development "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981. ("OECD Guidelines").

6.1.6. *European Instruments*

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data 1995 Official Journal L 281/31. ("EU Directive").

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation).

6.2. SECONDARY SOURCES

6.2.1. *Books*

Burns, Y & Burger-Smidt, A. *A Commentary on the Protection of Personal Information Act* Durban: LexisNexis. (2018).

Bygrave, L. *Data protection law: approaching its rationale, logic and limit* (2002).

Currie, I & De Waal, J. *Bill of Rights Handbook* 6 ed Cape Town: Juta, (2013).

De Stadler, E & Esselaar, P. *A Guide to the Protection of Personal Information Act* Cape Town: Juta, (2015).

Greenleaf, G. (2013) 'Chapter 10: Data protection in a networked world.' In Brown, I. (ed). *Research handbook on governance of the Internet* Edward Elgar Publishing (2012) 221-259.

Long, W. Scali, G. & Blythe, F. *The Privacy Data Protection and Cybersecurity Law Review* Law Business Research Ltd 6ed (2019).

Neethling, J. Potgieter, JM. & Visser, PJ. *Neethling's Law of Personality* Butterworths. Durban. (2005).

Neethling, J. Potgieter, JM & Roos, A. 'Neethling on Personality Rights' (2019).

Van der Merwe, D P. … et al. *Information and Communications Technology Law* 2 ed (2016).

6.2.2. *Journal Articles*

Bhaimia, S 'The General Data Protection Regulation: The Next Generation of EU Data Protection' (2018) 18 (1) *Legal Information Management* 21 – 27.

Botha, J. Grobler, M Hahn, J & Eloff, M. 'A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws' (2017) *The 12th International Conference on Cyber Warfare and Security (ICCWS)*.

Burchell, J. 'The legal protection of privacy in South Africa: A transplantable hybrid' (2009) 13(1) *Electronic Journal of Comparative Law (EJCL)* 1 – 26.

Coetzee, F. ‘The Press and POPI’ (2014) 14(4) *Without Prejudice* 69 – 71.

Daigle, B and Khan, M. 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities' (2020) *Journal of International Commerce & Economics* 1 – 38.

De Bruyn, M. ‘The Protection of Personal Information (POPI) Act – Impact on South Africa’ *International Business & Economics Research Journal.* (2014) 13 (6) 1315-1340.

El-Gazzar, R. & Stendal, K. ‘Examining How GDPR Challenges Emerging Technologies’ (2020) Journal of Information Policy (10) 237 – 275.

Goddard, M ‘The EU General Data Protection Regulation (GDPR): European regulation that has a global impact’ (2017) 59 (6) *International Journal of Market Research* 703 – 705.

Levin, A. & Nicholson, M. ‘Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground’ (2005). *University of Ottawa Law & Technology Journal*. 2 (2) 357 - 395.

Makulilo, B.A. ‘Privacy and data protection in Africa: a state of the art’ (2012). 2 (3) *International Data Privacy Law* 163 – 178.

Milo, D. & Ampofo-Anti, O. ‘A Not So Private World’ (2014) *Without Prejudice* 14 (9) at 30 – 32.

Millard, D & Bascerano, EG. 'Employers' statutory vicarious liability in terms of the Protection of Personal Information Act' (2016) 19 (1) *PELJ* 1 – 38.

Muller, L. ‘Are you working on the protection of personal information?’ (2020) *Chartered Institute of Government, Finance, Audit & Risk Officers (CIGFARO)* 21 (2) 28 – 32.

Myers, C. ‘The imminent Protection of Personal Information Act’ 2017 *TFM Magazine* 2 (12) 26 – 27.

Naude, A & Papadopoulos, S. ‘Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments (1)’ (2016) 79 (1) *THRHR* 51 – 68.

Rautenbach, C. ‘The South African Constitutional Court's use of foreign precedent in matters of religion: Without fear or favour?’ (2015) *Potchefstroom Electronic Law Journal (PELJ)* 18 (5) 1545 – 1570.

Rautenbach, I.M. 'Proportionality and the limitation clauses of the South African Bill of Rights' (2014) 17 (6) *PELJ* 2229-2267.

Roos, A. 'Core principles of data protection law' (2006) 39 (1) *CILSA* 102 – 130.

Roos, A. 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 (2) *SALJ* 400 - 437.

Roos, A. 'The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles" (2020) *CILSA* 53 (3) 1 – 37.

Staunton, C & de Stadler, E. 'Protection of Personal Information Act No. 4 of 2013: Implications for biobanks' (2019) *S Afr Med J*; 109 (4) 232 – 234.

Swales, L. 'Protection of personal information: South Africa's answer to the global phenomenon in the context of unsolicited electronic messages (spam).' (2016). *SA Merc LJ* 49-84.

Van Niekerk, B. 'The Cybersecurity Dilemma: considerations for investigations in the Dark Web.' (2018) *African Journal of Criminology & Victimology* 31 (3) 132 – 148.

Van Niekerk, B. 'An Analysis of Cyber-Incidents in South Africa' (2017) *The African Journal of Information and Communication (AJIC)* 20 113 – 132.

Viljoen, M de Villebois, C Castelyn, Pope, A & Botes, M 'Contact tracing during the COVID-19 pandemic: Protection of personal information in South Africa.' (2020) *S Afr Bioethics Law* 13 (1) 20 – 25.

Viorescu, R. '2018 Reforms of EU Data Protection Rules' (2017) *European Journal of Law and Public Administration* 4 (2) 27-39.

Voss, G. 'European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting' (2017). *The Business Lawyer* 72 (1) 221 – 234.

6.2.3. *Online Sources*

Altorvox 'Data Breach and Security Incident Management Policy' Available at: *https://www.altorvox.co.za/wp-content/uploads/AV-DATA-BREACH-SECURITY-INCIDENT-MANAGEMENT-POLICY.pdf* Accessed 23 May 2022.

Australian Government Productivity Commission 'Data Availability and Use' (2017) at 4. Available at: *https://www.pc.gov.au/inquiries/completed/data-access/report/data-access-overview.pdf.* Accessed 2 February 2021.

Business Tech 'Personal information of South Africans posted online after major data breach – here's what leaked' 4 September 2020. Available at: *https://businesstech.co.za/news/technology/431484/personal-information-of-south-africans-posted-on-dark-web-after-major-data-breach-heres-what-leaked/.* Accessed 3 October 2020.

Collins English Dictionary – 'disapply' Available at: *https://www.collinsdictionary.com/dictionary/english/disapply.* Accessed 14 April 2021.

Cookiebot 'UK Data Protection Act 2018 – 2021 Update' 18 January 2020. Available at: *https://www.cookiebot.com/en/data-protection-act-2018/.* Accessed 20 February 2021.

Council of Europe. 'Details of Treaty No.108' Available at: *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.* Accessed 30 October 2020.

Department for Digital, Culture, Media & Sport. 'Data Protection Bill: Factsheet – The Information Commissioner and Enforcement' March 2018. Available at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685645/2018-03-05_Factsheet05_Bill_ICO.pdf.* Accessed 2 November 2020.

European Union (Withdrawal Agreement) Act (2020 c.1). Available at: *https://www.legislation.gov.uk/ukpga/2020/1/contents.* Accessed 2 November 2020.

Harry Kinmonth & Elizabeth Wiggin 'Google v Vidal – Hall: the rise and rise of data protection rights' Available at: *https://www.lexology.com/library/detail.aspx?g=17b0d098-71a3-4925-a942-511d0bc52491.* Accessed 15 April 2021.

Information Commissioner's Office, Guide to the GDPR. Available at: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.* Accessed 27 October 2020.

Information Commissioner's Office, Guide to the GDPR. Available at: *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/.* Accessed 28 October 2020.

Information Commissioner's Office 'ICO fines Ticketmaster UK Limited £1.25 million for failing to protect customers' payment details' 13 November 2020. Available at: *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/.* Accessed 20 February 2021.

Information Commissioner's Office 'Information rights after the end of the transition period – Frequently asked questions' *https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/.* Accessed 19 February 2021.

Information Commissioner's Office Penalty Notice – Ticketmaster UK Limited. Case Ref: COM0759008. 13 November 2020. Available at: *https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf*. Accessed 20 February 2021.

Information Regulator, Available at: *https://justice.gov.za/inforeg/.* Accessed 1 October 2020.

Information Regulator 'Guidance Note on Information Officers and Deputy Information Officers' 1 April 2021 Available at *https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf.* Accessed 12 April 2021.

Information Regulator Media Statement *https://twitter.com/InforegulatorSA/status/1377647934536302593/photo/1.* Accessed 12 April 2021.

Information Regulator 'Frequently Asked Questions (FAQs) – Who is the Information Officer?' Available at: *https://twitter.com/InforegulatorSA/status/1376446204536578049/photo/1*. Accessed 12 April 2021.

Juta, 'POPIA Data Breach Policy and Response Plan' Available at: *https://jutacomplinews.co.za/media/filestore/2021/04/POPIA_breach_plan.pdf*. Accessed 6 February 2022.

Keumars Afifi-Sabet, 'What is GDPR? Everything you need to know, from requirements to fines' 11 March 2020. Available at: *https://www.itpro.co.uk/general-data-protection-regulation-gdpr*. Accessed 29 October 2020.

Kyle Venktess 'eThekwini shuts down e-services after user data leak' Fin24, 8 September 2016. Available at: *https://www.news24.com/fin24/tech/news/ethekwini-shuts-down-e-services-after-user-data-leak-20160908*. Accessed 17 February 2021.

Lydia F de la Torre 'What is Convention 108?' 26 June 2019 Available at: *https://medium.com/golden-data/what-is-coe-108-3708915e9846*. Accessed 29 January 2021.

Media Statement of the Information Regulator on the Experian Security Breach. Available at: *https://justice.gov.za/inforeg/docs/ms-20200820-Experian.pdf*. Accessed 1 October 2020.

Media Statement of the Information Regulator on the Experian Security Breach. Available at: *https://www.justice.gov.za/inforeg/docs/ms-20200903-ExperianUpdate.pdf*. Accessed 24 October 2020.

Michalsons, June 2020. "POPI Commencement Date or POPI Effective Date starts the Clock" Available at: *https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109*. Accessed 18 July 2020.

Michalsons 'POPI Regulations 2018 published in final form' December 2018. Available at*: https://www.michalsons.com/blog/popi-regulations-popia-regulations/12417*. Accessed 12 October 2020.

Nathan Trust 'GDPR Fines and Complaints' Available at: *https://www.nathantrust.com/gdpr-fines-penalties.* Accessed 19 February 2021.

Part One: Para 2 of the OECD Guidelines. Available at: *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*. Accessed 30 October 2020.

POPI Act Compliance. Available at: *https://www.popiact-compliance.co.za/gdpr-information/25-article-1-subject-matter-and-objectives.* Accessed 3 November 2020.

Reuters 'Google faces privacy complaints in European countries' 4 June 2019. Available at: *https://www.reuters.com/article/us-eu-google-privacy/google-faces-privacy-complaints-in-france-germany-7-other-eu-countries-idUSKCN1T51G3.* Accessed 19 February 2021.

Sunday Times – Business Times, 'Nedbank data breach may leave victims open to fraudulent attacks, say experts' Available at: *https://www.businesslive.co.za/bt/money/2020-03-08-nedbank-data-breach-may-leave-victims-open-to-fraudulent-attacks-say-experts/.* Accessed 3 November 2020.

Tefo Mohapi 'South Africa's notable data breaches and data leaks in the past half-decade' iAfrikan 27 October 2020. Available at: *https://iafrikan.com/2020/10/27/south-africa-biggest-top-data-breaches-leaks/* Accessed 15 February 2021.

The Banking Association of South Africa (BASA) 'Code of Conduct for the Processing of Personal Information by the Banking Industry' Available at*: https://www.justice.gov.za/inforeg/docs/InfoRegSA-Notice-BASA-COC-20210614.pdf*. Accessed 21 June 2021.

The Data Protection Act 2018 (c.12). Available at: *https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.* Accessed 3 November 2020.

The European Data Protection Board 'Guidelines 3/2018 on the territorial scope of the GDPR' November 2019. Available at:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf. Accessed 19 February 2021.

OECD website at: *https://www.oecd.org/*. Accessed 17 February 2021.

United Nations Conference on Trade and Development (UNCTAD) 'Data Protection and Privacy Legislation Worldwide' Available at: *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide*. Accessed 20 February 2021.

6.2.4. *Discussion Papers*

South African Law Reform Commission (SALRC) Discussion Paper 109 (Project 124) '*Privacy and data protection*.' October 2005.

6.2.5. *Theses*

Larsen, C. 'Data Privacy Protection in South Africa: An Analysis of Vicarious Liability in Light of the Protection of Personal Information Act 4 of 2013.' (LLM Thesis, University of KwaZulu-Natal, 2019).

Naude, A. 'Data Protection in South Africa: The Impact of the Protection of Personal Information Act and Recent International Developments' (LLM Thesis. University of Pretoria, 2014).

Rasool, Y. 'An Examination of How the Protection of Personal Information Act Will Impact on Direct Marketing and the Current Legislative Framework in South Africa' (LLM Thesis, University of KwaZulu-Natal, 2017).

Roos, A. 'The law of data (privacy) protection: A comparative and theoretical study' (LLD Thesis, University of South Africa, 2009).

6.2.6. *Other sources of reference*

M Heyink 'Protection of Personal Information for South African Law Firms'. (2013) *Law Society of South Africa (LSSA).*

M Heyink 'Protection of Personal Information Guide.' (2018) *Law Society of South Africa (LSSA).*