MINI DISSERTATION

Data Protection in South Africa: the Impact of the Protection of Personal Information Act and Recent International Developments

submitted in partial fulfilment of the requirement for the degree LLM (law of contract)

by

ADRIAN NAUDE

(Student Number: 94120341)

prepared under the supervision of

SYLVIA PAPADOPOULOS

at the University of Pretoria

[December 2014]

Summary

Historically, when it comes to protection for individuals in respect of the processing of their personal data, South Africa has been lagging behind international trends. The South African legal framework recognised some form of data protection for individuals, albeit limited, under the common law, the Constitution and certain specific pieces legislation. On 17 November 2000, the South African Law Reform Commission took the first step towards enacting a separate piece of data privacy legislation by approving the inclusion in its programme of an investigation entitled "Privacy and Data protection". On 26 November 2013, approximately 13 years later, the President of South Africa assented to the Protection of Personal Information Act 4 of 2013. This study examines the three most influential international instruments upon which the Protection of Personal Information Act is based, insofar as they relate to the core data privacy principles and the rights of data subjects. These international instruments have also recently been the subject of amendments or are in the process of being amended in order to keep abreast with international technological advancements and trends. This study further considers potential amendments to the Protection of Personal Information Act in respect of the core data privacy principles and the rights of data subjects in order to align the Protection of Personal Information Act with these latest trends and developments.

Table of Contents

Data Protection in South Africa: the Impact of the Protection of Personal Information Act and Recent International Developments

1. General Introduction

1.1 Background Information

It has taken South Africa 40 years since Sweden (the first nation in the world to enact national data privacy legislation)[1] to enact its own national data privacy legislation in the form of the Protection of Personal Information Act 4 of 2013 (hereinafter the "POPI Act" or the "Act"),[2] despite the fact that the South African Law Reform Commission (hereinafter the "SALRC") already took the first steps towards enacting data privacy legislation in South Africa in November of 2000.[3]

According to Greenleaf, as of mid-2013 there were already 99 countries worldwide that already had enacted data privacy legislation.[4]

---

1 Sweden enacted the Data Act (1973:289) in 1973. Cf Greenleaf "Global Data Privacy Laws: Forty Years of Acceleration" 2011 *Privacy Laws and Business International Report* No. 112 11-17. Available at http://ssrn.com/abstract=1946700 (accessed 2014-08-20); Roos "Data Protection: explaining the international backdrop and evaluating the current South African position" 2007 *SALJ* 402.

2 The *POPI Act* was enacted in terms of GN 912 in GG 37067 of 26 November 2013.

3 On 17 November 2000 the SALRC approved the inclusion in its programme of an investigation entitled "Privacy and Data protection". In 2001 the SALRC appointed a project committee to consider privacy and data protection legislation. The committee produced an issue paper in 2003 (SALRC "Privacy and Data Protection Project 124" issue paper 24 (2003)). The issue paper was followed by a discussion paper (SALRC "Privacy and Data Protection Project 124" discussion paper 109 (2005)) and thereafter the discussion paper was followed by a final report (SALRC "Privacy and Data Protection Project 124" Report (2009), (hereinafter referred to as the "*SALRC PDP Report*").

4 Greenleaf "*Global Data Privacy Laws 2013: 99 Countries and counting*" 2013 *Privacy Laws and Business International Report* 10. Available at: http://ssrn.com/abstract=2305882 (accessed 2014-09-16).

The SALRC in 2009 in its *PDP Report*[5] made eight recommendations and prepared a draft bill to be adopted by Parliament, in order to align "protection of information privacy" in the South African legal framework with other international instruments.[6] The most influential international instruments will be discussed in more detail later in this study.

In April 2014 the some of the provisions of the POPI Act relating to the information regulator and the Act's regulations came into effect.[7] Once the remainder of the provisions of the Act become operational, parties that process personal information will be required to conform to the provisions of the Act within one year of the commencement such provisions.[8] To date hereof the President of South Africa has not yet announced the commencement of the balance of the provisions of the Act. Therefore the bulk of the provisions discussed in this study will only come into effect on the publishing of the enactment date by the President, in the South African Government Gazette.

This study seeks to compare the South African data protection legal framework with some of the approaches that have been adopted in other international data protection instruments as well as to evaluate whether or not South Africa is on par with the international community, when it comes to data privacy legislation, insofar as it relates to the core data privacy principles and the rights of data subjects.

---

5 See n 3 above.

6 These recommendations included *inter alia*: (a) Privacy and information should be regulated by a general statute (applicable to private and public bodies) and to be supplemented by codes of conduct for various sectors; (b) That the eight core data privacy principles be included in the proposed legislation together with additional provisions for sensitive personal information; (c) A regulatory agency should be established to implement and monitor both the proposed *POPI Act* and the Promotion of Access to information Act, 2 of 2000 (hereinafter "*PAIA*"); (d) Enforcement of the proposed *POPI Act* provisions should occur mainly through the proposed Regulator; (e) A flexible approach should be followed in which industries develop their own codes of conduct based upon the core data privacy principles contained in the proposed *POPI Act*; (f) Provision has been made to protect data subject's rights insofar as they relate to unsolicited electronic communications and automated decision making; and (f) Transfer of personal information to countries that do not have adequate levels of data protection should be prohibited. Cf *SALRC PDP Report* viii.

7 Sec 1, Part A of chapter 5, sec 112 and sec 113 came into operation in accordance with the provisions of Proclamation No. R. 25 in GG 37544 of 11 April 2014. The remainder of the provisions of the Act are not yet operational.

8 Sec 114 *POPI Act*.

If it is found that there are shortcomings in the South African legal framework, this study will attempt to examine what improvements, if any, could be considered.

1.2 Definitions, Terms and Key References

Data protection refers to the legal protection afforded to a person (called the "data subject") in respect of the processing[9] of data concerning him- or herself (called "personal data") by another person, institution or organisation (called the "data controller"). A third party processing personal data on behalf of the data controller is referred to as a "data processor".[10]

[9] Sec 1 of the *POPI Act* defines "**processing"** 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."

[10] Neethling *et al Law of Personality* (2005) 276. Cf Roos "Core principles of data protection law" 2006 *CILSA* 104.

The *POPI Act* uses the term "personal information"[11] instead of "personal data", "responsible party"[12] instead of the term "data controller" and "operator"[13] instead of the term "data processor". However, in essence these terms bear the same meaning as ascribed above.

The international instruments that will be discussed herein refer to data privacy "principles" which are to be applied when processing personal data; however, the *POPI Act* instead refers to "conditions for lawful processing".[14] Again, data privacy "principles" and "conditions" refer essentially to the same concept.

1.3 Delineations and Limitations

Whilst acknowledging that there are many exemplary international data privacy instruments,[15] this study will mainly focus on the instruments that shaped the *POPI Act*'s

---

11 Sec 1 of the *POPI Act* defines "**personal information**" 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."

12 Sec 1 of the *POPI Act* defines **"responsible party"** as: "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."

13 Sec 1 of the *POPI Act* defines **"operator" as**: "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."

14 Chapter 3, *POPI Act*.

15 E.g Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 on 15 December 1989, and contained in a document E/CN.4/1990/72 (Available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement) and the APEC Privacy Framework (Available at: http://www.ag.gov.au/RightsAndProtections/Privacy/Documents/APECPrivacyFramework.pdf).

existence such as the Council of Europe's (CoE) *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (hereinafter the "*CoE Convention*"),[16] the Organisation for Economic Cooperation and Development's (hereinafter the "OECD") *Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data* (hereinafter the "*OECD Guidelines*"),[17] and the *Directive 95/46/EC* of the European Parliament 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* (hereinafter the "*EU Directive*").[18] These three international instruments have all recently been affected by amendments or proposed amendments. At the heart of this study is an examination of whether these amendments or proposed amendments should be taken note of in the South African legal framework insofar as they relate to the core data privacy principles and the rights of data subjects.

However, prior to taking a look at these recent international developments, this study will consider the South African data protection legal framework.

2. The data protection legal framework in South Africa

2.1 Introduction

Bygrave states that data privacy law are as those rules or laws that regulate the different stages in the processing of data and accordingly address the way in which data is gathered, registered, stored, exploited and disseminated. Furthermore, data privacy law is aimed at safeguarding the rights and interests of individuals, in their role as data subjects, when their

16 Convention No 108 of 1981, Strasbourg 28 Jan 1981.
Available at: http://conventions.coe.int/Treaty/EN/treaties/html/108.htm (accessed 2014-09-20).

17 OECD Guidelines 23 September 1981. Available at:
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 2014-09-20).

18 Available at:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (accessed 2014-09-20).

data is being processed by others. These individual rights and interests are often expressed in terms of privacy and sometimes in terms of integrity.[19]

In what follows this study will briefly look at how the South Africa law deals with the protection of data subjects, when it comes to the processing of personal information, in terms of the common law and other material pieces of legislation, including the Constitution.[20]

2.2 Data Privacy in South Africa Prior to the POPI Act

2.2.1 Protection of Privacy under the Common Law

2.2.1.1 Privacy and Identity

According to Roos, it is generally accepted that data processing of an individual's personal information poses a threat to the individual's right to privacy.[21] Neethling defines privacy as:[22]

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

This definition of privacy was confirmed by the Supreme Court of Appeal in *National Media Ltd v Jooste*.[23] It can accordingly be said that the right to privacy therefore entails an individual's right to control his personal information free from unwanted intrusions.[24] If one

19 Bygrave *Data Privacy Law an International Perspective* (2014) 1.
20 Constitution of the Republic of South Africa, 1996.
21 Roos 2007 *SALJ* 421.
22 Neethling *et al* (2005) 32.
23 1996 (3) SA 262 (A) at 271 - 272. Cf Neethling "The concept of privacy in South African Law" 2005 *SALJ* 18, 20. Cf Bernstein & Others v Bester & Others NNO 1996 (2) SA 751 at 788 par [C] where the Constitutional Court applied a more strict definition to the concept of privacy by limiting privacy only to the "inner sanctum of a person" e.g. family life, sexual preference and home environment.
24 *SALRC PDP Report* 2, par 1.2.1

has regard to Neethling's definition of privacy, the processing of a data subject's personal data can primarily be infringed in one of two ways:[25]

(a) by unlawfully processing true and correct personal data about an individual; or

(b) by processing false and misleading data about an individual.

In the former instance the data subject's privacy is infringed and in the latter an individual's identity is infringed.[26]

Historically, privacy has often been equated with a right to dignity. However, the common law has developed to give recognition to the independent right to privacy.[27] The *locus classicus* for support for this view is *O' Keeffe v Argus Printing and Publishing Co Ltd*[28] where the Plaintiff complained that her photograph and name had been used for advertising purposes without her consent. The Court held that the question that needed to be decided was:[29]

> "… whether the publication of the plaintiff's photograph and name… is capable of constituting a violation of the plaintiff's 'real rights related to personality', and in particular, of those rights relating to her dignity."

In holding that the above conduct did violate the Plaintiff's dignity (*dignitas*), the Court by implication identified the right to privacy as being one of those "… real rights related to personality" and rejected the view that insult (*contumelia*) is the basis of an injury to personality (*iniuria*).[30]

---

25 Roos 2007 *SALJ* 403, 422.

26 Roos "Personal data protection in New Zealand: Lessons for South Africa" 2008 *PER* 89.

27 Neethling *et al* "*Law of Personality"* (2005) 217. Cf also National Media v Jooste 1996 3 SA 262 (A).

28 1954 3 SA 244 (C).

29 1954 3 SA 244 (C) at 247 F.

30 Similarly, in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 375 (T) it was held that held that identity is an independent personality interest worthy of delictual protection, but it was in *Grutter v* Lombard 2007 4 SA 89 (SCA) that it was finally determined that: "…The interest that a person has in preserving his or her identity against unauthorised exploitation seems to me to be qualitatively indistinguishable and equally encompassed by that protectable 'variety of personal rights'".

Accordingly both the right to privacy and the right to identity currently form part of the South African common law as part of the law of personality.[31] Remedies for infringement are dealt with under the law of delict.[32]

Privacy and identity should; however, be distinguished from each other with Neethling defining identity as:[33] "… a person's uniqueness or individuality which identifies him as a particular person and thus distinguishes him from others." Examples of identity include an individual's life history, name, credit worthiness and appearance.

Given the aforesaid, identity entails an individual's right to have control over the accuracy of his or her information.[34]

2.2.1.2 Common Law remedies for infringement of privacy or identity

Delictual actions can generally be classified into one of three categories: [35]

(a) the wrongful causing of patrimonial loss (referred to as an *damnum iniuria datum)*;

(b) the wrongful infringement of interests of personality (referred to as an *iniuria*);[36] and

(c) the wrongful infliction of pain and suffering associated with bodily injury. .

Damages are claimed, in the case of patrimonial loss, upon the *actio legis Aquilae* and, in the case of non-patrimonial loss, upon the *action iniuriarum* for compensation as satisfaction (referred to as *solatium*) for the injury caused to the Plaintiff's personality.[37]

---

31 Neethling *et al* (2005) 219, 273. Neethling et al *Law of Delict* (1993) 332 - 335.Cf also *SALRC PDP Report* 24 par 2.1.22.
32 Neethling *et al* (1993) 5, 250-251.
33 Neethling *et al* (2005) 32; Roos 2004 *PER* 91.
34 Roos 2007 *SALJ* 422.
35 Neethling *et al Law of Delict* (2006) 5.
36 The unlawful infringement of privacy and identity would fall under this category of a delict.
37 Neethling *et al* (2006) 5.

In the context of data privacy, Roos correctly states that where the privacy of a person has been infringed by the processing of personal information (by unlawfully processing true and correct data about an individual or by processing false and misleading data about an individual)[38] the aggrieved party can rely on the principles of the law of delict to exercise his or her remedies.[39] Such remedies will be limited to the following:

(a) an interdict to prevent the wrongful processing of personal data or further processing of personal data; and / or

(b) a claim based on the *actio iniuriarum* for *solatium* for non-patrimonial loss for the injury caused to the Plaintiff's personality as a result of the wrongful intentional processing of personal data;[40] or

(c) a claim for compensation under the *action legis Aquiliae* for patrimonial loss (*damnum iniuria*) sustained due to the wrongful, negligent processing of personal data.[41]

In order to found delictual liability for the infringement of a protected right (such as privacy or identity), the conduct in question (such as the processing of personal information) must be wrongful. Wrongfulness is determined by using the criterion of reasonableness (or the norm of *boni mores*). Therefore, in common law, before it can be said that processing of personal data constituted a wrongful invasion of privacy and / or identity, it must not only be shown that there was a factual violation of the plaintiff's interest, but that such violation was also unreasonable (*contra bonos mores*) or wrongful.[42]

2.2.2 Protection of privacy under the Constitution

The Constitution of the South Africa is the supreme law of the country and any conduct or law which is inconsistent with the Constitution is invalid.[43] The Bill of Rights, set out in Chapter 2 of the Constitution, contains the entrenched rights which are binding on the executive, the legislature, organs of state as well as natural and juristic persons.[44] The

38 Roos 2007 *SALJ* 422 n 172.
39 Cf n 32 above.
40 Cf n 35 above.
41 Cf n 32 above.
42 Neethling et al (2005) 273.
43 Sec 2 Constitution.
44 Sec 8(1); 8(4) Constitution.

entrenchment of fundamental rights in the Constitution fortifies their protection and gives the fundamental rights a higher status in that they apply to all law.[45] Any law or action by the state or person may therefore be tested with reference to an entrenched fundamental right. A limitation of a fundamental right may only occur if it complies with the requirements of the limitation of rights clause contained in section 36 of the Constitution.[46]

Section 14 in the Bill of Rights, entrenches the fundamental right of privacy.[47] Identity is not recognized *eo nomine* in the Bill of Rights. Neethling; however, argues that many of the personality rights that are not mentioned *eo nomine* in the Constitution (such as identity, feelings, etc.) fall under the right to human dignity, which by implication means that these unspecified rights are also recognised as constitutionally entrenched human rights.[48] The right to identity can therefore be considered to be protected under the right to human dignity, which is explicitly mentioned in section 10 of the Constitution.[49]

As a consequence of the recognition of the right to privacy in our Constitution, the legislature and the executive may not pass any law or take any action which infringes or unreasonably limits the right to privacy. In addition, Roos submits that the government is obliged to adopt legislation for the adequate protection of data privacy where the common law is unable to do so.[50] One could also possibly therefore argue that the government has a constitutional

---

45 *SALRC PDP Report* 20 par 2.1.11.

46 Sec 36 of the Constitution states that: "(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including -
(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose; and
(e) less restrictive means to achieve the purpose.
(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights."

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

48 Neethling et al (2005) 18 n 147.

49 Roos 2007 *SALJ* 422; ibid.

50 Roos 2007 *SALJ* 423.

responsibility to prioritise the enactment of the remainder of the provisions of the *POPI Act*,[51] as it will later transpire in this study that the common law is clearly inadequate to deal with data privacy when it comes to the processing of personal information.[52] One cannot but help but to agree with Roos' assertion that it seems that the "political will" to drive the enactment of the *POPI Act* to conclusion is absent in South Africa.[53]

Initially, it would appear, that the Constitutional Court adopted a more restrictive interpretation to the constitutional right to privacy (referred to as an informational right to privacy).[54] In *Bernstein v Bester*[55] the Constitutional Court applied a more strict definition to the concept of privacy by limiting privacy only to the "inner sanctum of a person" (e.g. family life, sexual preference and home environment).[56] Ackermann, J stated that:[57]

> "Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly."

Neethling, argues that this concept is too narrow as it ignores other private facts relating to one's person, which are also worthy of protection.[58] In *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd,*[59] the informational right to privacy was interpreted to come into play whenever an individual has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected, is reasonable.[60]

---

51 Cf n 7 above.
52 See par 2.2.3 below.
53 Roos 2004 *PER* 91.
54 Cf n 23 above.
55 Bernstein & Others v Bester & Others NNO 1996 (2) SA 751 at 788 par [C].
56 Cf n 23 above.
57 Bernstein & Others v Bester & Others NNO 1996 (2) SA 751 at 789 par [A].
58 Neethling 2005 *SALJ* 20.
59 In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 (1) SA 545 (CC) 557 Par [16].
60 Cf n 23 above.

When it comes to interpreting fundamental rights and their limitation, Ackerman J, warned that caution must be exercised.[61] He drew a distinction between the two stage constitutional enquiry into whether a right (such as privacy) has been infringed and then whether the infringement is justified, when deciding on the constitutionality of a statute or conduct. However, under the common law there is a single enquiry as to whether an unlawful or wrongful infringement has taken place.[62]

2.2.3 Limitations to the protection of data privacy under the common law and the Constitution

The traditional common law principles of delict are useful in determining whether the processing of personal information has taken place lawfully or not, but only provide limited protection where an individual's personal information is processed. The same holds true for constitutional infringements to the informational right to privacy. Traditional delictual principles do not give active control to the individual and therefore do not cater for instances where the data subject is unaware: [63]

(a) that his or her personal information is being collected or being processed by a third party; or
(b) that he or she has access to his or her personal information; or
(c) that he or she may correct personal information which is incorrect.

Neethling proposes that in order for the individual to exercise active control over his or her personal information an individual must be:[64]

(a) aware of the existence of a data record concerning him or her that is being stored by the data controller;
(b) aware of the purpose(s) for which such data is being processed;

---

61 Bernstein & Others v Bester & Others NNO 1996 (2) SA 751 at 790 par [D] – [E]; Burchell *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* (1998) 388; *SALRC PDP Report* 21 par 2.1.14.
62 Cf *SALRC PDP Report* 34 par 2.3.5.
63 Roos 2007 *SALJ* 423.
64 Neethling *et al* (2005) 278.

(c) legally entitled to have access to such data records;

(d) legally entitled to know who has had access to his data records; and

(e) legally entitled to procure a correction or deletion certain data.

Only once an individual has active control over his or her own personal data does the traditional common law principles discussed above play a more meaningful role.[65]

Another limitation to the common law is that trans-border data flows (hereafter "TBDFs") are not regulated.[66]

2.2.4 Data protection under South African legislation

Prior to the promulgation of the *POPI Act* the South African law did not have an omnibus of data privacy legislation.[67] Currently, within South African legislation there are predominantly three statutes that contain data protection provisions (albeit limited) that are worth mentioning; namely, the *Promotion of Access to Information Act* (hereinafter "*PAIA*")[68], the *Electronic Communications and Transactions Act* (hereinafter the "*ECTA*)[69] and the *National Credit Act* (hereinafter the "*NCA*").[70]

2.2.4.1 PAIA

PAIA is essentially a law that has been enacted to give effect to an individual's constitutional right of access to any information[71] held by the State or any another person and that is

65 Neethling *et al* (2005) 280.
66 Cf par 4.1 below for a discussion on TBDFs.
67 Cf n 2 above. Not all the sections of the *POPI Act* have as yet not been enacted and therefore the position regarding data privacy under the common law and under legislation, as discussed above, still applies.
68 Act 2 of 2000.
69 Act 25 of 2005.
70 Act 32 of 2005.
71 Sec 32 of the Constitution states that: "Everyone has the right of access to -
(a) any information held by the state; and

required for the exercise or protection of any rights.[72] This Act, to a limited extent, addresses the active control principles as well as other data protection principles by:

(a) giving individuals access to records containing personal information about themselves in the public and private sector;[73]

(b) requiring public and private bodies to take reasonable steps to establish adequate internal measures which provide for the correction of personal information (if such measures do not exist) until legislation providing for such correction comes into effect;[74] and

(c) prohibiting the disclosure of a record if it would involve the unreasonable disclosure of personal information relating to a third party.[75]

2.2.4.2 ECTA

ECTA was enacted to regulate electronic commerce and therefore it only operates in the electronic communications environment.[76] Chapter VIII of *ECTA*[77] contains provisions which relate to the protection of personal information, of an individual, that has been obtained through electronic transactions.[78] *ECTA* further states that a data controller may voluntarily subscribe to the data privacy principles outlined in *ECTA* by recording such fact in any agreement with a data subject. [79] When subscribing to the voluntary data privacy principles the data controller is obliged to subscribe to all nine principles, contained in *ECTA*, and not just to parts thereof.[80] The rights and obligation of the parties, in the event of a breach of the

(b) any information that is held by another person and that is required for the exercise or protection of any rights.
(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state."

72 Preamble to PAIA.

73 Sec 11 (re: public body) and sec 50 (re: private body) of *PAIA*.

74 For a discussion on the reason as to why PAIA does not contain a specific provisions for individual to correct incorrect data see Currie & Klaaren *The Promotion of Access to Information Act Commentary* (2002) 18 par 2.5.

75 Sec 34 (re: public body) and sec 63 (re: private body) of *PAIA*.

76 Preamble to *ECTA*; Roos 2007 *SALJ* 426.

77 Consisting of sec 50-51 of *ECTA*.

78 Sec 1 of *ECTA* gives a wide definition to "**Transaction**" which means: "a transaction of either a commercial or non-commercial nature, including the provision of information and e-government services."

79 Sec 50(2) *ECTA*.

80 Sec 50(3) Id.

said voluntary data privacy principles, are to be regulated by the agreement between the parties.[81] Once the *POPI Act* becomes fully enforceable these principles will only apply to the extent that they are more extensive than the conditions for lawful processing that are contained in the Act.[82]

The voluntary data privacy principles aim to ensure that:[83]

(a) a data subject's personal information is processed lawfully;[84]

(b) a data controller must have a lawful purpose(s) for the processing of personal information and the data processing must be necessary to fulfil such purpose;[85]

(c) the data subject has knowledge of the specific purpose(s) for which the personal information is being requested;[86]

(d) personal information is only used for the purpose(s) for which it was collected by the data controller, by requiring the data controller to obtain express written consent from the data subject to use such personal information for any other purpose than for what it was collected, unless permitted or required to do so by law;[87]

(e) a record of the personal information and the specific purpose(s) for which the personal information was collected is retained for as long as that the personal information is used and at least 12 months thereafter;[88]

(f) personal information that is held by a data controller is not disclosed to a third party, unless required or permitted by law or with the express written consent of the data subject;[89]

(g) in the event that personal information is disclosed to a third party, that a record of the third party to whom the personal information was disclosed and of the date on which

81 Sec 50(4) *ECTA*.
82 Sec 3(2)(b) of *POPI Act*.
83 Cf Roos 2007 *SALJ* 426 – 429.
84 Sec 51(1) *ECTA*.
85 Sec 52(2) id.
86 Sec 52(3) id.
87 Sec 52(4) id.
88 Sec 52(5) id.
89 Sec 52(6) id.

and the purpose for which it was disclosed is retained for as long as that the personal information is used and at least 12 months thereafter;[90]

(h) the data controller destroys all personal information once the information has become obsolete;[91] and

(i) data processing may take place for statistical purposes on the premises that anonymity of the data subject is ensured, by requiring the data controller to ensure that data profiles or statistical data cannot be linked to any specific data subject by a third party.[92]

Glaring deficiencies in the data protection provision of the *ECTA* include the fact that the data privacy principles are voluntary (and only binding if agreed to by both parties) as well as the fact that there is no provision for the establishment of a regulatory authority to enforce compliance.[93]

2.2.4.3 NCA

The *NCA* aims to promote a fair and non-discriminatory marketplace for access to consumer credit by providing for the general regulation of consumer credit and improved standards of consumer information (which inter alia includes the regulation of credit information).[94] The *NCA*, as with the other pieces of legislation already discussed herein, also has limited provisions relating to data privacy.

In respect to the right to confidentiality the *NCA* states that any person who receives, compiles, retains or reports any confidential information[95] relating to a consumer or prospective consumer must protect the confidentiality of that information.[96] Furthermore;

---

90 Sec 52(7) *ECTA*.
91 Sec 52(8) id.
92 Sec 52(9) id.
93 Cf discussion under par 4.1 below where Bygrave raises four general features which are characteristic of successful international instruments dealing with data privacy.
94 Preamble to *NCA*.
95 "**Confidential Information**" as defined in sec 1 of *ECTA* means: "personal information that belongs to a person and is not generally available to or known by others."
96 Sec 68 of *NCA*.

such information may only be used for a purpose permitted in terms of *NCA* or other legislation and may only be reported or released to the consumer, prospective consumer or third party as permitted in terms of the Act or other legislation or as directed by a consumer, prospective consumer, tribunal or order of court. Failure by a credit bureau to comply with an enforcement notice, issued by the National Credit Regulator[97] in respect of the right to confidentiality provisions is an offence in terms of the *NCA*.

Credit providers are also obliged to report certain information about consumers to credit bureaus or to the national register when a new credit agreement is concluded, amended, terminated or completed with a consumer.[98] Such information includes the name, address, and identifying number of the consumer as well as information about the credit provided such as credit limit, principal debt involved, etc.

In respect of consumer credit information[99] which is held by credit bureaus, the *NCA* stipulates that credit bureaus are obliged to inter alia take reasonable steps to verify the accuracy of consumer credit information, retain any consumer credit information reported to it for the prescribed period, erase from its records any consumer credit information that is not permitted to be entered in its records or is required to be removed from its records (as provided for in the regulations of the *NCA*) and to desist from knowingly or negligently provide a report to any person containing inaccurate information.[100]

The *NCA* also gives individuals the right to access and challenge credit records and information.[101]

---

97 Established under sec 12 *NCA*.

98 Established under sec 69 *NCA*.

99 **"Consumer credit information**" as defined in s70 includes a person's credit history (e.g. application for credit, credit agreements concluded, etc.), financial history (e.g. past and present income, Assets and liabilities, etc.), education, employment career, business history or identity (e.g. name, date of birth, marital status, family relationships, etc.).

100 Sec 70(2) *NCA*.

101 Sec 72 id.

If one has regard to the discussion above concerning data privacy and the common law,[102] it can be seen that some progress has been made in the legislation, discussed above, to address the aspect of active control and the rights of data subjects. However, the South African statutory framework, prior to the *POPI Act*, remained wholly inadequate to address the protection of individuals when it came to the processing of personal information. Below follows a discussion on the core data privacy principles that are contained, in one form or another, in all successful modern international data privacy instruments.

3. Data Privacy core principles

Authors and commentators agree that despite differences in legal structures, language, cultural and social values there is general agreement on the basic content and core rules (often referred to as "principles"[103] or "conditions"[104]) that should be embodied in data protection legislation.[105] These core data protection principles are contained, in one form or another, in all successful data protection laws. Bygrave[106] identifies the following core data protection principles that are included in all successful modern international instruments:

(a) Principle 1: Fair and lawful processing;

(b) Principle 2: Proportionality

(c) Principle 3: Minimality;

(d) Principle 4: Purpose limitation;

(e) Principle 5: Data quality;

(f) Principle 6: Data security;

(g) Principle 7: Data sensitivity; and

(h) Principle 8: Data subject influence.

Roos, identifies additional principles, such as: [107]

---

102 Cf par 2.2.3 above.
103 Cf for example, CoE Convention (Chapter II), the OECD Guidelines (Part Two) and EU Directive (Section I).
104 Cf *POPI Act* (Chapter 3).
105 Roos 2006 *CILSA* 107; Bygrave (2014) 2.
106 Bygrave (2014) 1; ch 5A-I.
107 Roos 2006 *CILSA* 107 – 129.

(i) Principle 9: Openness or transparency;[108]

(j) Principle 10: Accountability;[109] and

(k) Principle 11: Exceptions and exemptions[110]

The different data privacy principles are not hard and fast rules and significant overlap exists between them. Furthermore; it often occurs that a subset of multiple principles are grouped together in order to form one principle.[111] It is also important to note that the principles are seldom applied as absolutes and the instruments within which they are contained often provide for exceptions.[112] Below follows a short discussion on each of the core data privacy principles that are generally include in all successful modern data protection instruments.

3.1 Fair and lawful processing

This principle is reflected in Article 5(a) – (b) of the *CoE Convention* and Article 6(1)(a) – (b) of the *EU Directive*. This is the primary principle in that it "embraces and generates the other principles".[113] This principle dictates that a data subject's personal data must be processed fairly and lawfully. Roos submits that within the South African context it is sufficient to require that processing should be done lawfully as fairness is part and parcel of the concept of lawfulness when one has regard to the common law and more specifically the law of delict.[114]

---

108 This principle requires that there should be a policy of openness and transparency concerning developments, practices and policies of personal data (Roos 2006 CILSA 116). Examples of this principle are found in the *EU Directive*: (a) in the notification procedure (art 18 -19); (b) the DPA must keep a register of data processing operations about which it has been notified (art 21) and (c) the fact that data controllers have a duty to keep data subject informed (art 10 and 11(1)).

109 This principle requires that: (a) a data controller or processor is accountable to comply with the core data privacy principles which is contained in the applicable statutory law (e.g. art 8bis *Modernisation Proposa*l, par 14 *OECD Guidelines* and art 23 *EU Directive*); and (b) that data subjects have a judicial remedy, (by way of damages, compensation and / or sanctions) where their privacy rights have been infringed (e.g. art 22 and 24 *EU Directive*). Cf Roos 2006 *CILSA* 126.

110 This principle allows for exceptions or relaxation of the core data privacy principles which is contained in the applicable statutory law where the risks to the interests of the data subject is relatively small or where other interests (e.g. public interest, another parties interests or even the data subjects own interests) override the interests override the interest of the data subject (e.g. Art 3(2) and Art 13 of the EU Directive). Cf also Roos 2006 *CILSA* 127 - 128.

111 E.g. the principle of data quality discussed in par 4.4.1 below. Cf Bygrave (2014) ch 5A.

112 Bygrave (2014) ch 5A.

113 Id Ch 5B.

114 Cf par 2.2.1 above; n 35 above; Roos 2006 *CILSA* 111.

Regarding the element of "fairness", Bygrave states that this principal encompasses the following:

(a) data controllers must take into account the interest and reasonable expectation of data subjects;

(b) the collection and processing of personal data must not unreasonably interfere with a data subject's privacy interests (the requirement of balance and proportionality should be met);

(c) data subjects should not be unduly pressured into supplying personal data to others or agreeing to new uses of the data once it has been supplied (i.e. protection from abusive data controllers); and

(d) the processing of personal data must be transparent for the data subject in order to prevent the data subject being misled in respect of the nature of, and the purpose for, the processing (this may also entail that personal data be collected directly from a data subject and not from third parties or where personal data has been obtained for one purpose and it is subsequently used for another purpose, which the data subject would not reasonable foresee, whereupon the data controller may need to obtain the data subject's consent for the new use).[115]

3.2 Proportionality Principle

This principle is contained in Article 5(1) of the *Modernisation Proposal*[116] and Article 6(1)(c) of the *EU Directive*. This principle requires that personal data must be "relevant" and "not excessive" in relation to the purpose for which it was collected. Sometimes the criterion of "necessity" is also included in the requirement for proportionality (i.e. that the processing of personal data must be necessary for the purpose for which it has been collected).[117]

115 Bygrave (2014) ch 5B.
116 See n 149 below.
117 Bygrave (2014) ch 5C.

If one takes into account the element of "necessity" then it could be argued that the provisions of Article 7, 8 and 13 of the *EU Directive* also bear elements of this principle.

There is also considerable overlap between the proportionality principle and the purpose limitation principle, as will be seen below.

3.3 Minimality

This principle is reflected in Article 5(c) of the *CoE Convention* and Article 6(1)(c) of the *EU Directive*. The principle of minimality requires that:

(a) the amount of personal data collected must be limited to what is necessary in order to achieve the purpose for which it was collected;
(b) when data no longer serves the purpose for which it was originally collected it should be erased or anonymized; and
(c) that the processing of personal data be prohibited unless it is necessary for the achievement of specific goals.[118]

If one takes into account the prohibition on the processing of personal data unless it is processed for a specific purpose, it could be argued that Articles 7 and 8 of the *EU Directive* also display elements of this principle.

3.4 Purpose Limitation

This principle is reflected in Article 5(b) of the *CoE Convention*, Par 9 of the *OECD Guidelines* and Article 6(1)(b) of the *EU Directive*. The purpose limitation principle requires that personal data should be collected for a specified legitimate purpose and used in a manner that is not

[118] Bygrave (2014) ch 5D.

incompatible with the purpose for which it was originally collected.[119] The purpose limitation principle is a combination of three sub-principles; namely, that:[120]

(a) the purpose(s) for which data is collected must be defined and made explicit;
(b) the said purpose(s) must be lawful or legitimate; and
(c) if personal data is processed further, such processing should not be incompatible with the original purpose for which it was collected.

This principle is also concerned with addressing information quality and that data processing outcomes conform to the expectations of data controllers.[121]

3.5 Data Quality

This principle is reflected in Article 5(d) of the *CoE Convention* and Article 6(1)(c) to (d) of the *EU Directive*. The data quality principle requires that personal data must be valid (with respect to what it is intended to describe) and complete (with respect to the purpose for which it is intended to be processed).[122]

3.6 Data Security

This principle is reflected in Article 7 of the *CoE Convention* and Article 17 of the *EU Directive*. This principle entails the fact that personal data, held by data controllers or processors, should be protected against unauthorised attempts to disclose, delete or exploit such data.[123]

3.7 Sensitivity

This principle is reflected in Article 6 of the *CoE Convention* and Article 8(1) and (5) of the *EU Directive*. The sensitivity principle requires that the processing of certain types or categories

119 Roos 2006 *CILSA* 111.
120 Bygrave (2014) ch 5D.
121 Id.
122 Id ch 5G.
123 Id ch 5H.

of data (normally regarded as sensitive for the data subject) should be subject to more stringent controls than the controls that are applied to other personal data.[124]

3.8 Data subject influence

This principle entails that individuals should have a measure of influence and should be able to participate in the processing of personal data, relating to them, by third parties. This principle manifests itself through a combination of several rules:[125]

(a) rules aimed at making people aware of data processing activities;

(b) rules aimed at making data subjects aware of basic details relating to the data processing of personal information relating to themselves (e.g. requiring data controllers to collect data directly from the data subject; requiring data controllers to provide certain information on their data processing operation; rules prohibiting the processing of personal information without the consent of a data subject and rules making provision for mandatory notification of data security breaches); and

(c) rules granting data subjects the right to gain access to personal data kept on them by third parties;

(d) rules allowing data subjects to object to the processing of their personal data and to insist that data be rectified or erased where such data is invalid, irrelevant, inaccurate, etc.

Examples of some of these rules relating to data subject influence are reflected Par 10, 13 and 15(c) of the *OECD Guidelines* and Articles 7(a), 8(2(a) and 10 to 12 of the *EU Directive*.

This study will now turn to briefly look at the international instruments that have had a profound influence on the *POPI Act*.

124 Bygrave (2014) ch 5I.
125 Id ch 5F.

4. International instruments

4.1 Introduction

As already mentioned, in 1973 Sweden was the first country in the world to enact data privacy legislation.[126] However, by the 1980s data protection had become an international issue due to the emergence of a global market and the increase ease with which personal information could be transmitted outside the borders of the country of origin which lead to the increase in the exchange of personal information across national boundaries, known as "trans-border data flows" (TBDFs).[127] International data protection instruments that emerged post the 1980s, generally have two primary goals:[128]

(a) the setting of standards at an international level for the protection of personal data; and
(b) providing for the free flow of information across national boundaries (where there are adequate controls).

Bygrave raises four general features which are characteristic of most successful international instruments dealing with data privacy:[129]

(a) privacy law is largely statutory;
(b) data privacy legislation normally establishes independent regulatory bodies, often referred to as Data Protection Authorities (herein after "DPA" or "DPAs") to oversee its implementation;
(c) data privacy laws often take the form of "framework" laws;[130] and
(d) DPAs often play a lead role in how data privacy law is understood and applied, even where their views are only advisory.

126 Cf n 1 above.
127 Roos 2007 *SALJ* 403; *SALRC PDP Report* par 1.2.12.
128 Roos 2007 *SALJ* 404
129 Bygrave (2014) 1.
130 E.g. *EU Directive*.

There are three vital instruments that have had a profound effect on data privacy laws across the world relating to TBDFs; namely, the *CoE Convention,*[131] the *OECD Guidelines*[132] and the *EU Directive* that are dealt with in more detail hereinafter.[133]

4.2 CoE Convention

4.2.1 CoE Convection Principles

The *CoE Convention* contains a set of basic data protection principles in chapter two. Each member state undertakes to incorporate these principles into its domestic law in order to give effect to the data protection principles.[134] However the *CoE Convention* is not self-executing and no individual rights can be derived from it.[135] The basic data protection principles contained in chapter two are:

(a) duties of the parties;[136]

(b) quality of the data[137] (which includes provisions relating to the "fair and lawful processing",[138] "purpose limitation"[139] and "minimality"[140] principles);

---

131 The CoE has its headquarters in Strasbourg, France. It is Europe's leading human rights organisation and currently consists of 47 member states. South Africa is not a member of the CoE. Available at: http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en (accessed 2014-09-20).

132 The OECD was established in 1961 and currently has a membership of 34 countries, of which South Africa is not a member. The OECD provides a forum in which governments can work together to share experiences and seek solutions to common problems. They set international standards on a wide range of things, from agriculture and tax to the safety of chemicals. Available at: http://www.oecd.org/about/ (accessed 2014-09-20).

133 Roos 2007 *SALJ* 404.

134 Art 4 *CoE Convention*.

135 *SALRC PDP Report* 143 par 4.1.12.

136 Art 4 requires member states to implement the necessary measures in its domestic law to give effect to the basic principles for data protection that are contained with the *CoE Convention* within a specified period.

137 Art 5 of the *CoE Convention* stipulates that personal data undergoing automatic processing shall be: "(a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; and (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

138 Art 5(a) *CoE Convention*.

139 Art 5(b) Id.

140 Art 5(c) – (e) Id.

(c) special categories of data;[141]

(d) data security;[142]

(e) safeguards for the data subject,[143]

(f) sanctions and remedies;[144] as well as

(g) extended protection.[145]

Chapter three states that member states shall not prohibit the TBDFs to the territory of another member state unless such TBDFs are done in order to circumvent the national laws of the country of origin of the personal data (i.e. when TBDFs are made to a safe haven in order to bypass the national laws of a specific country) or where national legislation makes provision for such prohibition. [146]

In May 2001 the CoE Committee of Ministers adopted an additional Protocol[147] which made provision for member states to:

(a) establish DPAs; and

(b) to allow for TBDFs to recipients (state or organisation) which are not a party to the *CoE Convention* by requiring that such TBDFs may only take place where the recipient ensures an adequate level of protection for the intended data transfer.

---

141 Art 6 of the *CoE Convention* stipulates that: "personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions."

142 Art 7 of the *CoE Convention* stipulates that appropriate security measures shall be taken for the protection of personal data stored in automated data files.

143 Art 8 of the *CoE Convention* contains additional safeguard provisions relating to automated personal data file such as rights of access, rectification and erasure.

144 Art 10 of the *CoE Convention* provides for each party to establish appropriate sanctions and remedies for violations of provisions of domestic law.

145 Art 11 of the *CoE Convention* provides that local domestic law may grant data subjects a wider measure of protection than provided for in the *CoE Convention*.

146 Art 12 *CoE Convention*.

147 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS 181, Strasbourg 8 November 2001. Available at: http://conventions.coe.int/Treaty/en/Treaties/html/181.htm (accessed on 2014-10-18).

4.2.2 CoE Modernisation Proposal

The *CoE Convention* was the first, and still remains the only, legally binding international instrument in the field of data protection.[148] However, in order to respond to rapidly changing technological developments and globalisation trends that have brought new challenges for the protection of personal data, the CoE consultative committee adopted final proposals for the modernisation of the current *CoE Convention*, in December 2012 (hereinafter the "*Modernisation Proposal*").[149] The *Modernisation Proposal* seeks to build on the current data protection principles, with the addition of two further principles.

Only material changes proposed to the current *CoE Convention,* as introduced by the *Modernisation Proposal* are highlighted below.

4.2.2.1 Legitimacy of data processing and quality of data:

Two new requirements for data processing are proposed, thereby introducing the principle of proportionality, to underpin the legitimacy of data processing of personal data.[150]

Firstly, that such processing must be proportionate in relation to the legitimate purpose pursued and that there must be a fair balance between all interests concerned at all stages of the processing and secondly, that data processing may only be carried out with the consent of the data subject or on the basis of some other legitimate basis laid down by law.

---

148 European Union Agency for Fundamental Rights et al *Handbook on European data protection law* (2014) 16.

149 The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS no. 108], Strasburg 18 December 2013. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp (accessed 2014-10-18). Cf European Commission press release: "Commission to renegotiate Council of Europe Data Protection Convention on behalf of EU" 19 November 2012 (Memo/12/877), available at: http://europa.eu/rapid/press-release_MEMO-12-877_en.htm (accessed 2014-10-18); Greenleaf "Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" 2013 Computer Law & Security Review (CLSR) 430, available at: http://ssrn.com/abstract=2280875 (accessed 2014-09-16)

150 Art 5 *Modernisation Proposal*.

In respect of data quality provisions a proposed change is that the data quality principles should apply to all personal data that it processed and not just personal data "undergoing automatic processing", as stipulated in the original provisions of the *CoE Convention*.[151]

4.2.2.2 Processing of sensitive data

It is further proposed that "genetic data", "identifying biometric data", and "trade union membership" be added to the categories of sensitive data. Appropriate safeguards to prevent the risk of discrimination against the data subject, in respect of sensitive data, are also required.[152] These provisions were lacking from the original *CoE Convention*.

4.2.2.3 Data security

This is a new principle proposed by the *Modernisation Proposal*. Chapter III requires member states to provide for the creation of DPAs.[153] Data controllers are further required to notify the relevant DPA of any data breaches that may seriously interfere with the rights of data subjects.[154] Interestingly, the *Modernisation Proposal* does not require the data subject to be notified of such breach.[155] The remainder of the data security provisions are similar to the original provisions contained in the *CoE Convention*.

4.2.2.4 Transparency of processing

This was not included in the original *CoE Convention*. This provision contains the minimum information that a data controller is required to provide to a data subject at the time of collecting personal data. This provision also applies when personal data is collected from third

151 Cf n 137 above.
152 Art 6 *Modernisation Proposal*.
153 Art 12bis id.
154 Art 7 id.
155 Although the Draft Explanatory Report to the *Modernisation Proposal* encourages notification to data subjects where a data breach has occurred (par 66).

parties, except where the processing is prescribed by law or it proves to be impossible or involves disproportionate efforts.[156]

4.2.2.5 Rights of the data subject and obligations of the data controller

Additional rights, in favour of the data subject, and obligations, for the data controller, are proposed to those contained in the original *CoE Convention*. These rights and obligations are similar to those contained in the *EU Directive* and the *EU Regulation,*[157] both of which are discussed in more detail below.[158] Another provision that was not included in the original *CoE Convention* is the requirement that member states should ensure that:[159]

(a) data controllers and / or data processors are required to:

i. Take "at all stages" of the processing process "all appropriate measures" which give effect to the data privacy principles and to be able to demonstrate compliance to the relevant DPA;[160] and

ii. Perform a risk analysis of the potential impact of the proposed data processing on the privacy rights of the data subject and design the data processing operations in such a manner so as to minimise the risk of interference with those privacy rights;

iii. take into account the rights of data subjects in respect of products and services, intended for data processing, from the stage of their design.[161]

156 Art 7bis *Modernisation Proposal*.

157 See the EU "Proposal for a Regulation of the European Parliament and of the Council on the protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" Brussels, 25 January 2012 (hereinafter the "EU Regulation") Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 2014-09-20).

158 For a discussion regarding the *EU Directive* refer to par 0 below and for a discussion regarding the *EU Regulation* refer to par 4.5.2 below.

159 Article 8bis *Modernisation Proposal*. Cf Greenleaf 2013 *CLSR* 5.

160 This is similar to accountability principle contained in art 5(f) and art 22(1) of the *EU Regulation*.

161 This obligation is similar to the "data protection by design" and "data protection by default" principles contained in Art 23 of the EU Regulation, however, this specific provision is not provided for in the *EU Regulation*. Cf par 6.3 below.

An interesting provision which has been included in order to reduce the cost of compliance allows for member states to take the measures needed in order to adapt the application of the provisions above, taking into account the size of the data controller and / or the data processor, the volume or nature of data processed and lastly the risks posed to the privacy rights of data subjects.[162]

4.3 OECD Guidelines

The *OECD Guidelines* were revised in 2013.[163] The 2013 revision to the 1981 version of the *OECD Guidelines* was required due to changing technologies, markets, user behaviour and the greater importance of digital identities over the past forty years.[164] The *OECD Guidelines* also contains a set of basic principles that apply to the processing of personal data where member countries and non-member countries are encouraged to implement the provisions contained in *OECD Guidelines*.[165] However, the 1981 version of the *OECD Guidelines* did not contain requirements as to how these principles are to be enforced by member nations. The revised *OECD Guidelines* explicitly make provision for the establishment of DPAs.[166] There are eight core principles contained in the revised *OECD Guidelines*.[167] They include the limitation principle,[168] quality principle,[169] specification principle,[170] use limitation principle,[171] security

162 Art 8bis(4) *Modernisation Proposal*.
163 Available at: oe.cd/privacy (accessed 2014-09-20).
164 The OECD 2013 Privacy Framework 4.
165 *OECD Guidelines* ch1.
166 Compare art 14 of the original *OECD Guidelines* with art 15 of the revised *OECD Guidelines*.
167 Annexure, Part Two *OECD Guidelines*.
168 Par 7 of the *OECD Guidelines* stipulates that there should be limits to the collection of personal data, which should be obtained by lawful means and, where appropriate, with the consent of the data subject.
169 Par 8 stipulates that personal data should be relevant to the purpose for which it is collected, accurate and kept up-to-date.
170 Par 9 of the *OECD Guidelines* requires the purpose for which personal data are collected to be specified at the time of collection and if the purpose is to change it should be specified for every time there is a change in purpose.
171 Par 10 of the *OECD Guidelines* states that personal data should not be disclosed for any other purpose than the purpose specified, unless the data subject has consented or required by law.

safeguards principle,[172] openness principle,[173] individual principle[174] and the accountability principle.[175]

Additionally, the revised *OECD Guidelines* contains three principles relating to TBDFs, namely, that:

(a) the data controller remains accountable for personal data despite the location of the data;[176]

(b) TBDFs should not be restricted where the other country substantially observes the *OECD Guidelines* or sufficient safeguards exist to ensure a level of protection consistent with the *OECD Guidelines*;[177] and

(c) restrictions to TBDFs should be proportionate to the risk taking into account the sensitivity of the data, the purpose and context of processing.[178]

Non-Member states are also invited to adhere to the *OECD Guidelines* and to collaborate with member countries in the implementation of the eight principles across borders.[179]

4.4 The EU Directive

The *EU Directive* evolved from the original *OECD Guidelines*, but seeks to set a higher level of protection for data subjects.[180] The *EU Directive* aims, on the one hand to protect the rights and freedoms of an individual (particularly the right to privacy) with respect to the processing

172 Par 11 of the *OECD Guidelines* requires personal data to be protected by reasonable security safeguards against loss, unauthorised access, modification, use or disclosure.

173 Par 12 of the *OECD Guidelines* requires a general policy of openness regarding policies and practices relating to personal data.

174 Par 13 of the *OECD Guidelines* gives individuals the right to know whether a data controller has data relating to them, the right to challenge a refusal by a data controller to provide such information and the right to have data erased, rectified, completed or amended.

175 Par 14 of the *OECD Guidelines* provides that a data controller should be accountable to comply with the other seven principles.

176 Par 16 OECD Guidelines.

177 Par 17 id.

178 Par 18 id.

179 Ch 1 id.

180 Roos 2007 *SALJ* 405.

of personal data and on the other hand to ensure the free flow of personal data between member states.[181] Member states are therefore obliged to adopt national legislation that conforms to the standards set out in the *EU Directive* within a specified period.[182] Once this has been achieved, member states may not restrict TBDFs to other member states for reasons connected with the protection of the rights of an individual. However, member states are required to prohibit TBDFs to non-EU member countries that don't provide an adequate level of data protection.[183] As a result, as with the *OECD Guidelines*, the *EU Directive* also has an influence, in respect of the transfer of personal data, on non-member states outside the EU.[184]

4.4.1 EU Directive Principles

The *EU Directive* also contains a set of principles, relating to the processing of personal data. Five of the principles relate to data quality and require that personal data is: [185]

(a) processed fairly and lawfully;

(b) collected for a "specified, explicit and legitimate purposes", further processing may not be incompatible with the initial purposes;

(a) "adequate, relevant and not excessive" in relative to the purposes for which it was collected;

(b) accurate and kept up to date, therefore data that is incomplete or inaccurate should either be erased or rectified; and

(c) not kept in a form that allows for the identification of the data subject for a period longer than is necessary.

There are further principles to ensure that the processing of data is legitimate, by providing that personal data may only be processed where:[186]

---

181 Art 1 of the *EU Directive* and preamble to *EU Directive* par 7.
182 Preamble par 8 and art 32 *EU Directive*.
183 Referred to as "Third Countries".
184 Art 25 *EU Directive*.
185 Art 6(1)(a) – (e) *EU Directive*.
186 Art 7(a) – (f) id.

(a) the data subject has given consent;

(b) the data processing is necessary in order to perform in terms of a contract with the data subject or at the request of the data subject prior to such contract;

(c) such processing is necessary in order for the data controller to comply with a legal obligation;

(d) such processing is necessary to protect the vital interests of the data subject;

(e) such processing is carried out in the public interest, in official authority vested in the data controller or in a third party to whom the data are disclosed;

(f) such processing is necessary for the purposes of the legitimate interests pursued by the data controller, the third party or parties to whom the data is disclosed.

When it comes to the processing of special categories of data there is a general prohibition on the processing of such data.[187] Exceptions to the general prohibition are: [188]

(a) where the data subject has given explicit consent for the processing of such data;

(b) where the data controller processes such data to carry out its obligations or rights in accordance with the field of employment law;

(c) where the data subject is physically or legally incapable of giving consent and the data controller processes such data to protect the vital interests of the data;

(d) where the processing of such data is carried out by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim, in the course of its legitimate activities; or

(e) where the processing of such data is necessary for the establishment, exercise or defense of legal claims or the data is made public by the data subject.

187 Special categories of data include data revealing the following in respect of a data subject: "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life (art 8(1) *EU Directive*).

188 Art 8(2) *EU Directive*.

4.4.2 Data Subject's rights in terms of the *EU Directive*

Rights afforded by the *EU Directive* include: [189]

(a) that personal data must be processed according to the data quality principles contained in the *EU Directive*;[190]

(b) the right to be informed of the identity of the data controller, the purpose for collection as well as any other relevant information;[191]

(c) the rights of access to one's own personal data, which includes the right to rectification, erasure[192] or the blocking of data processing where there is non-compliance with the provisions of the directive (data controllers are also required to notify third parties, to whom the data have been disclosed, of such rectification, erasure or blocking of data);[193]

(d) the right to object to the processing of personal information:

i. where such information is allegedly processed in the interest of the data subject, in the performance of a task carried out in the public interest or in order to peruse a legitimate interest of the data controller[194] on compelling legitimate grounds;[195] and

ii. for the purposes of direct marketing;[196]

(e) the right not to be subject to a decision which produces legal consequences or significantly affects the data subject and which is solely based on automated processing of data intended to evaluate certain personal aspects relating to the data subject (e.g. the data subject's performance at work , creditworthiness, reliability, conduct, etc.);[197] and

---

189 These rights are not absolute and must be enforced by member states. Cf art 13 *EU Directive*: Exception and Restrictions.

190 Cf art 6(1) *EU Directive* and discussion on par 4.4.1 above.

191 Art 10(1) and 11(1) *EU Directive*.

192 See n 224 below.

193 Art 12 *EU Directive*.

194 Art 7((e) – (f) id.

195 Art 14(a) id.

196 Art 14(b) id.

197 Art 15 id. Exceptions to this right are listed in art 15(2) *EU Directive*.

(f) the right of every person to a judicial remedy for any breach of the rights guaranteed by the national laws enacted by member states.[198]

Member states are required to appoint their own DPAs who have relatively wide powers, to monitor the application of the provisions of the *EU Directive*.[199]

Pitfalls to the *EU Directive* include the fact that it has not been able to prevent fragmentation in the manner in which personal data protection has been implemented across EU member states, legal uncertainty and widespread public perception that there are significant risks associated with online activity.[200] Another pitfall worth mentioning is the cost of compliance as there is no similar provision, as with the *Modernisation Proposal*, that allows member states to take into account the size of the data controller and / or the data processor, the volume or nature of data processed and the risks posed to the privacy rights of data subjects when considering compliance with the provisions of the *EU Directive*.[201] As a result of the above pitfalls the European Commission ("EC") proposed a more comprehensive data protection framework in the *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)* (hereafter the "*EU Regulation*")[202] that will:[203]

> "... allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities."

198 Art 22 *EU Directive*.
199 Art 28 id.
200 EU Regulation Explanatory Memorandum 2.
201 Cf par 4.2.2.5 above.
202 On 25 January 2012 the EC proposed a comprehensive reform of the EU Directive. See the EU "Proposal for a Regulation of the European Parliament and of the Council on the protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" Brussels, 25 January 2012. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 2014-02-13).
203 EU Regulation Explanatory Memorandum 2.

4.5 The EU Regulation

A press release of the EC states that:[204]

> "On 25 January 2012, the Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online data protection rights and boost Europe's digital economy. The Commission's proposals update and modernise the principles enshrined in the 1995 Data Protection Directive, bringing them into the digital age and building on the high level of data protection which has been in place in Europe since 1995."

Although the *EU Regulation* has yet to be passed into law by the European Parliament it would seem that progress on EU data protection reform is now irreversible.[205]

4.5.1 EU Regulation Principles

Material changes or improvement to the *EU Directive* insofar as they relate to the core data principles will be briefly mentioned below.

---

204 European Commission press release "Progress on EU data protection reform now irreversible following European Parliament vote" 12 March 2014 (Memo/14/186) (hereafter "Memo/14/186") available at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (accessed 2014-09-22)

205 Following a European Parliament vote in favour of the *EU Regulation* on 12 March 2014. Cf Memo/14/186; Cf n 204 above.

4.5.1.1 Data Quality

The *EU Regulation* contains essentially the same principles as the *EU Directive* relating to data quality;[206] however, the *EU Regulation*s introduces additional elements in respect of the transparency,[207] minimality[208] and accountability principles.[209]

4.5.1.2 Lawful processing

Also, on the principle of lawful processing the *EU Regulation* is similar to the *EU Directive*.[210] The balance of interest criterion is, however, clarified in that the *EU Regulation* specifically states that where a data controller is processing personal data in pursuance of a legitimate interest, such processing will only be lawful where the interest of the data subject outweighs the interest of the data controller, especially where the data subject is a child.[211] The conditions for valid consent,[212] as well as verifiable consent (where consent is given on behalf of a child under 13 years old)[213] as a valid legal ground for lawful processing, are also amplified in the *EU Regulation*.

4.5.1.3 Special categories of data

The general prohibition for processing special categories of personal data has been expanded in the *EU Regulation* by adding "genetic data", "criminal convictions" and "related security

206 Cf par 4.4.1 above.
207 Art 5(a) states that personal information, in addition to being processed lawfully and fairly, must be processed in a manner that is transparent in relation to the data subject.
208 Art 5(c) clarifies the minimality principle by requiring that personal data is limited to the minimum necessary in relation to the purpose for which they are processed and that such purposes could not be fulfilled by processing information that does not contain personal data.
209 Art 5(f) states that the processing of personal data must be processed under the responsibility and liability of the data controller who must comply with the processing provisions contained in the regulation.
210 Cf par 4.4.1 above.
211 Exceptions include where processing is carried out by public authorities in the performance of their tasks (art 7 *EU Regulation*).
212 Art 7 *EU Regulation*.
213 Art 8 Id.

measures" to the definition of special categories of data.[214] Exceptions to the general prohibition to the processing special categories of personal data have also been expanded.[215]

4.5.2 Data Subject's rights in terms of the *EU Regulation*

Chapter 3 of the *EU Regulation* deals with the rights of a data subject and are briefly discussed below.

4.5.2.1 Transparency and modalities:

Data controllers are required to:

(a) have transparent and easily accessible policies relating to the processing of personal data as well as for the exercising of data subjects' rights;[216]

(b) provide any information and communication in an understandable form, using plain language, adaptable to the circumstances of a data subject, especially where the data subject is a child;[217]

(c) provide procedures and mechanisms to enable data subjects to exercise their rights, this includes means for electronic requests, responding to a data subject's request within a defined period (generally one month) and the motivations of a refusal to action a request by a data subject.[218]

The *EU Regulation* further builds on the *EU Directive* by requiring data controllers to notify third parties, to whom personal data has been disclosed, of any right of rectification or erasure of personal data that has been carried out by a data subject, [219] unless this involves disproportionate effort.[220]

---

214 Art 9 *EU Regulation*.
215 Art 9(a) – (j) id.
216 Art 11(1) id.
217 Art 11(2) id.
218 Art 12 id.
219 Cf par 0 above and n 193 above.
220 Art 13 *EU Regulation*.

4.5.2.2 Information and access to data:

The *EU Regulation* expands on the data subjects' right to be informed about his or her personal data that is being processed[221] as well as the data subjects' right to access personal information, by providing for additional information that must be provided to the data subject (e.g. the right to lodge a complaint, storage period of data, etc.).[222]

4.5.2.3 Rectification and erasure:

In a recent decision of the EU Court of Justice,[223] based on the current provision of the *EU Directive*, the Court found that a data subject, when it comes to the processing of personal information, has the "right to be forgotten" where a data subject's personal information is inaccurate, inadequate, irrelevant or excessive.[224] The *EU Regulation* expounds on this right by specifically providing for the data subject's right to rectification, right to be forgotten (especially where the data subject's data was made available while he or she was a child) and right to erasure.[225] Data controllers that have made personal data public are also obliged to inform third parties of a data subject's request to erase any links to or copy of that personal data.

4.5.2.4 Right to portability

The *EU Regulation* introduces the right to portability which entails a data subject's right to transfer data from one electronic processing system to another without being prevented from

---

221 Cf par 0 above; n 191 above.

222 Art 14 - 15 *EU Regulation*.

223 C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* [2014] (hereafter "Google Case"). Available at: http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

224 The facts of the case, briefly, were that in "2010 a Spanish citizen lodged a complaint against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc. The citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results." (EU "Factsheet on the *'Right to be forgotten'* Ruing (C-131/12).

225 Art 16 - 17 *EU Regulation*.

doing so by the data controller. Data controllers are obliged to provide the data subject's data in a structured and commonly used electronic format.[226]

4.5.2.5 Right to object and profiling:

The rights of a data subject to object to the processing of data and direct marketing are similar to those contained in the *EU Directive,*[227] with additional safeguards.[228]

4.5.2.6 Right to notification

The *EU Regulation* also affords the data subject the right to be notified of a data breach where the data breach is likely to adversely affect the protection of the privacy of the data subject.[229]

4.5.3 Restrictions:

As with the *EU Directive*, the *EU Regulation* empowers member states to restrict the application of the core data privacy principles[230] as well as certain data subject right's, when such a restriction constitutes a necessary and proportionate measure in a democratic society.[231]

Given the discussion above it is submitted that the *EU Regulation,* when finalised*,* will be the most comprehensive data protection instrument, of those instruments that have already been discussed herein, insofar as it relates to the core data privacy principles as well as the rights afforded to data subjects.

---

226 Art 18 *EU Regulation*.
227 Cf par 0; n 195; n 196 above.
228 Art 19 – 20 *EU Regulation*.
229 Cf Art 32 *EU Regulation*; n 155 above.
230 Cf Art 5 *EU Regulation*; par 4.4.1 above.
231 Art 21 of the *EU Regulation* provides for the following examples: to safeguard public security, the prosecution of criminal offences, other public interests, the persecution and breaches of ethics for regulated professions, a regulatory function, the protection of the data subject or the rights and freedoms of others.

This study will now turn to take a look at the provisions of the *POPI Act* and thereafter will follow a critical analysis of how the *POPI Act* compares with the international instruments that have been discussed herein.

5. The Protection of Personal Information Act 4 of 2013

5.1 Introduction

If one has regard to the shortcomings of data protection, as provided for in terms of the South African legal framework, prior to the *POPI Act*,[232] it is evident that a massive overhaul of the statutory framework was required in order to ensure that legislation provides an adequate level of data protection that is comparable with other international instruments.[233]

Below follows a discussion on the provisions of the *POPI Act*. Thereafter this study will examine whether the *POPI Act* is comparable with other international instruments insofar as it relates to the rights of data subjects and the core data privacy principles.

5.2 Purpose, Application and Exclusions of the Act

5.2.1 Purpose

The Act has the following purposes:[234]

(a) to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party; [235]

(b) to regulate the manner in which personal information may be processed, subject to certain conditions for lawful processing, which accord with international standards;

---

232 See par 2.2.3.
233 *SALRC PDP Report* ix.
234 Sec 2(a) – (d) *POPI Act*.
235 Cf n 12 above.

(c) to provide rights and remedies to persons to protect their personal information from unlawful processing; and

(d) to establish an information regulator (hereinafter the "Regulator"), to promote, enforce and fulfil the rights envisaged and protected by the Act.

5.2.2 Application

The *POPI Act* applies to the processing of personal information that is entered in a record by (or on behalf of) a responsible party: [236]

(a) by making use of automated means or non- automated means, where such responsible party is domiciled in South Africa;

(b) where personal information is processed by non-automated means (e.g. paper and text, photograph, x-rays, etc.) such processing only falls under the ambit of the Act if the personal information forms part of a filing system[237] or is intended to form part thereof; or

(c) by making use of automated means or non- automated means, where such responsible party is not domiciled in South Africa, unless those means are used solely to forward personal information.

The Act applies to the exclusion of any other legislation unless the other legislation provides for conditions of lawful processing of personal information that are more extensive or onerous than those conditions specified in the Act.[238]

---

236 Sec 3(1)(a) – (b) *POPI Act*. Cf Heyink 2012 *LSSA Guidelines* 8

237 Sec 1 *POPI Act* defines a "**filing system**" as: "any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria".

238 Sec 2(a) – (b) *POPI Act*.

5.2.3 Exclusions

5.2.3.1 General exclusions

The *POPI Act* does not apply where the processing of personal information: [239]

(a) is for a personal or household activity; or

(b) where the personal information has been sufficiently de-identified (anonymised) ; or

(c) has been processed by or on behalf of a public body for the purposes of national security or for the prevention of unlawful activities, the investigation of offences or the prosecution of offenders only to the extent that adequate safeguards have been established in legislation for the protection of such personal information; or

(d) is processes by the Cabinet; or

(e) relates to the judicial functions of a court.

5.2.3.2 Journalistic, literary or artistic exclusions

POPI does not apply to the processing of personal information where it relates solely to the purpose of journalistic, literary or artistic expression and where the responsible party is subject to a code of ethics that provides adequate safeguards for the protection of personal information.[240]

5.2.3.3 Other exclusions

Other exclusion include:

(a) regulatory exclusions, where the Regulator may grant an exemption to the responsible party where the processing of personal information is in the public interest[241] or there is a clear benefit to the data subject; [242] and

---

239 Sec 6(1)(a) – (e) *POPI Act*.

240 Sec 7(1) – (2) id.

241 Sec 37(2) of the *POPI Act* states that "**public interest**" includes national security interests; detection, prevention and prosecution of offences; material economic and financial interest of a public body; historical, statistical or research activity or the importance of the interest in freedom of expression.

242 Sec 37 *POPI Act*.

(b) while performing a relevant function,[243] where personal information is processed for the purpose of discharging such function.

5.3 Conditions for lawful processing of information

5.3.1 Introduction

The *POPI Act* as with other data protection legislation worldwide, contains a set of conditions (or principles) which contains the basic content and core rules that govern the processing of personal information.[244] These conditions are largely based on the principles contained in the *CoE Convention*, *OECD Guidelines* and the *EU Directive* that have been discussed above.

5.3.2 Conditions when processing personal information

The conditions do not stand in isolation and often interact and overlap with one another and therefore need to be viewed holistically, as is the case with the principles in other jurisdictions.[245] Processing of personal information by the responsible party, falling within the ambit of the Act,[246] must comply with the conditions specified in the Act, unless the Regulator has granted an exemption or where processing is for the purpose of the discharge of a relevant function.[247]

The conditions are listed below and will be discussed briefly thereafter.[248]

---

243 Sec 38(2) of the *POPI Act* states that a **'Relevant function'** means a function performed by a public or private body: "which is performed with the view to protecting members of the public against-
(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or
(ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity."

244 Cf *POPI Act* Chapter 3, Part A; Roos 2007 *SALJ* 405.

245 Cf Heyink 2012 10; *SALRC PDP Report* 161.

246 See par 0 regarding instances where processing of personal information is excluded from the Act.

247 Cf par 5.2.3.3 above.

248 Sec 4(1) *POPI Act*.

(a) Condition 1: Accountability;[249]

(b) Condition 2: Processing limitation;[250]

(c) Condition 3: Purpose specification;[251]

(d) Condition 4: Further processing limitation;[252]

(e) Condition 5: Information quality;[253]

(f) Condition 6: Openness;[254]

(g) Condition 7: Security safeguards;[255] and

(h) Condition 8: Data subject participation.[256]

5.3.2.1 Condition 1: Accountability

The *POPI Act* states that:[257]

> "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."

249 Sec 8 *POPI Act*.
250 Sec 9 - 12 id.
251 Sec 13 - 14 id.
252 Sec 15 id.
253 Sec 16 id.
254 Sec 17 - 18 id.
255 Sec 19 - 22 id.
256 Sec 23 - 25 id.
257 Sec 8 Id.

It is evident that the responsible party remains responsible for the processing of personal information regardless of whether the personal information has been handed to an operator to process personal information on behalf of the responsible party.[258]

Two critical measures are required to be established and maintained in order for the responsible party to comply with the accountability condition:[259]

(a) The personal information that will be processed should be identified; and
(b) The responsible party must identify and appoint a person(s) to safeguard personal information.

The *POPI Act* caters for these requirements in that it allows for the appointment of an Information Officer who is able to satisfy both these measures.[260]

5.3.2.2 Condition 2: Processing limitation

The processing limitation is based on the principle that personal information:

(a) must be processed in a lawful and reasonable manner so as not to infringe the privacy of the data subject;[261]
(b) may only be processed if it is adequate, relevant and not excessive;[262]
(c) may only be processed with the data subject's consent (although numerous exceptions apply);[263] and

258 Heyink 2012 11.
259 id.
260 Chapter 5, Part B (S55 - 56) *POPI ACT*.
261 Sec 9 *POPI Act*.
262 This is known as the minimality principle, which requires that when personal information no longer serves the purpose for which it was originally collected it should be erased or expressed in an anonymous form. Cf Roos 2006 *CILSA* 113.
263 Sec 11(1)(a) *POPI Act*. However, the Act does allow for the processing of personal information without consent from the data subject where: the processing is necessary in terms of a contract to which the data subject is a party, the processing complies with an obligation imposed by law on the responsible party, the processing protects a legitimate interest of the data subject, processing is necessary for the proper performance of a public law duty by a public body or where the processing is necessary to pursue a legitimate interest of the responsible party or a third party to whom the information was supplied (sec

(d) must be collected directly from the data subject (although numerous exceptions apply).[264]

5.3.2.3 Condition 3: Purpose specification

The purpose specification requires that personal information must be collected for a specific, explicitly defined and lawful purpose which is related to an activity of the responsible party.[265] The *POPI Act* compels the responsible party to take reasonable steps[266] to ensure that the data subject is aware of the purpose of the collection of personal information, unless the responsible party is exempt.[267]

Another requirement is that records of personal information may not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed. [268]

11(1)(b)-(f) *POPI Act*). It is evident that the *POPI Act* is not consent driven and that personal information may be processed without the data subject's consent in a number of instances (Heyink 2012 14).

264 An exception to this requirement includes instances where: the information is contained in a public record or has been deliberately made public by the data subject, the data subject has consented to collection from another source, collection from another source does not prejudice a legitimate interest of the data subject, or collection from another source is necessary to avoid prejudice to the maintenance of law by any public body, to comply with an obligation imposed by law, to enforce the collection of revenue by SARS, for the conduct of proceedings in court, where it is in the interest of national security, to maintain the legitimate interests of the responsible party, where compliance would prejudice a lawful purpose of the collection or where compliance is not reasonable practicable in the circumstances of a particular case (sec 12 *POPI Act*).

265 Sec 13 *POPI Act*.

266 Sec 18(1)(a) - (h) of *POPI Act*, requires the responsible party to ensure that that data subject is aware of the information being collected, the name and address of the responsible party, the purpose for which the information is being collected, whether the supply of the personal information by the data subject is voluntary or mandatory, the consequences of failure to provide the information, whether any particular law authorises the collection of the personal information, the fact that the responsible party (where applicable) intends to transfer the personal information to another country (referred to as a third country) and any other relevant information

267 Sec 18(4) of the *POPI Act*., stipulates that the responsible party is not required to ensure that the data subject is aware of the information specified in s18(1), where the data subject has provided consent for non-compliance, non-compliance would not prejudice the legitimate interest of the data subject or non-compliance is necessary (a) to avoid prejudice to the maintenance of law by any public body, (b) to comply with an obligation imposed by law, to enforce the collection of revenue by SARS, (c) for the conduct of proceedings in court, (d) where it is in the interest of national security or where compliance would prejudice a lawful purpose of the collection, where compliance is not reasonable practicable in the circumstances of a particular case, the information will be used in a form in which the data subject is not identified or lastly where the personal information will be used for historical, statistical or research purposes.

268 Sec 14(2) - (3) *POPI Act*. Exceptions are contained in sec 14(1)(a) - (d) and sec 14(2) - (3) *POPI Act*.

5.3.2.4 Condition 4: Further processing limitation

This condition requires that further processing of personal information must be compatible with the purpose for which it was collected (in terms of the purpose specification principle).[269] In order to assess whether further processing is compatible with the initial purpose for which it was collected, the Act requires the responsible party to take the following into account:

(a) the relationship between the purpose for which the information was originally collected and the intended purpose of any further processing;
(b) the nature of the information concerned;
(c) the consequences of further processing;
(d) the manner in which the information was collected; and
(e) contractual rights and obligations between the parties.

Specific instances where further processing, by the responsible party, is considered to be compatible with the initial purpose for which it was collected are also mentioned in the Act.[270]

5.3.2.5 Conditions 5: Information quality

This condition requires the responsible party to have regard to the purpose for which personal information was collected and to take reasonable practical steps to ensure that personal information that has been collected is complete, accurate, not misleading and updated where necessary.[271] It is interesting to note that the *King Code on Corporate Governance for South Africa* [272] recognised the information quality principle as an important governance principle, even before the *POPI Act* was promulgated. In dealing with IT governance, *King III* states that:[273]

---

269 Sec 15 *POPI Act*.
270 These instances of further processing, contained in sec 15(3)(a)-(f) of the *POPI Act*, are similar to the grounds upon which information may be processed as specified in sec 9(1)(a) - (f) *POPI Act*.
271 Sec 16 *POPI Act*.
272 More commonly known as King III (hereinafter "*King III*").
273 *King III* Principle 5.6 (37)

"The board should ensure that there are systems in place for the management of information assets and the performance of data functions including… establishing processes to ensure the maintenance and monitoring of data quality…"

5.3.2.6 Condition 6: Openness

The responsible party is obliged to maintain the documentation of all its processing operations under its responsibility as provided for in the relevant sections[274] of the PAIA.[275] The responsible party is also obliged to take reasonable steps to ensure that the data subject is aware of:[276]

(a) the information being collected and the source from which it is collected, if not collected from the data subject;
(b) the name and address of the responsible party;
(c) the purpose for which the information is being collected;
(d) whether the supply of information is mandatory or voluntary;
(e) the consequences of failure to provide the information;
(f) if applicable, the law authorising collection of the information;
(g) if applicable, the fact that the responsible party intends to transfer the information to a third country or international organisation and the level of protection that will be afforded to the information by the third country or international organisation; and
(h) any further relevant information.

The Act also states when it will not be necessary to obtain consent from the data subject.[277]

---

274 Sec 14 (relating the manual of records held by public bodies) and sec 51 (relating to the manual of records held by private bodies) *PAIA*.
275 Sec 17 *POPI Act*.
276 Sec 18(1)(a) - (h) id.
277 E.g. where the data subject has provided consent for non-compliance or compliance is not necessary to avoid prejudice to the maintenance of law by any public body, to comply with an obligation imposed by law, to enforce the collection of revenue by SARS, for the conduct of proceedings in court, where it is in the interest of national security, where compliance would prejudice a lawful purpose of the collection, where compliance is not reasonable practicable in the circumstances of a particular case or the information will not be used in a form in which the data subject is identified (S18(4)(a) - (f) *POPI Act*).

5.3.2.7 Condition 7: Security safeguards

In respect of this condition the Act distinguishes between the responsible party and the operator.

Responsible party

A responsible party is required to secure the integrity and confidentiality of personal information, having regard to generally accepted information security practices and procedures[278] and by taking appropriate reasonable technical and organisation measures to prevent loss of, unauthorised destruction, unlawful access to or processing of personal information.[279] Accordingly the responsible party must take reasonable measures to:[280]

(a) identify reasonable foreseeable risks to personal information in its possession or under its control;
(b) establish and maintain appropriate safeguards against identified risks;
(c) verify that safeguards are effectively implemented; and
(d) ensure that safeguards are continually updated.

Operator

An operator must be authorised by the responsible party to process personal information and must treat such information as confidential and may not disclose it, unless required by law or in the course of the performance of its duties.[281] The responsible party must have a written contract with the operator and is also obliged to ensure that the operator complies with the security measures contained in section 19 of the Act to secure the integrity and confidentiality of personal information. The operator must immediately notify the responsible party where there are reasonable grounds to believe that that personal information of a data subject has been accessed or acquired by an unauthorised person.[282]

278 Sec 19(3) *POPI Act*.
279 Sec 19(1) id.
280 Sec 19(2) id.
281 Sec 20 id.
282 Sec 21 id.

Notification of security compromises

Where there are reasonable grounds to believe that that personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify the Regulator and the data subject.[283]

5.3.2.8 Condition 8: Data subject participation

Access to personal information

A data subject has the right to request the responsible party:

(a) to confirm, at no charge to the data subject, whether or not the responsible party holds personal information relating to the data subject;[284] and

(b) the record or a description of the personal information held by the responsible party, as well as the identities of all third parties that have had access to the information.

In the case of the latter, the responsible party is entitled to charge the data subject a fee for such a request.[285] A responsible party is also required to advise the data subject of his or her right to request a correction of information. A responsible party is entitled, where applicable, to refuse to disclose any information to the data subject on the same grounds as those contained in PAI Act. [286]

Correction of personal information

A data subject may request the responsible party to correct or delete personal information that is inaccurate, out of date or obtained unlawfully. Furthermore, where the responsible party is no longer authorised to retain the personal information the data subject may request the responsible party to destroy or delete the personal information.[287] Once the responsible

283 Unless the regulator or a public body has determined that the notification of the data subject may impede a criminal investigation by the public body concerned (sec 22 *POPI Act*).
284 Sec 23(1)(a) *POPI Act*.
285 Sec 23(1)(b) id.
286 Ch 4 (Part 2) and ch 4 (Part 3) *PAIA*, which relates to grounds for refusal of access to records held by public and private bodies respectively.
287 Sec 24(1) *POPI Act*.

party has received a request, as contemplated above, the responsible party must comply with such request within a reasonable time. In the event that the responsible party and the data subject cannot reach agreement, relating to the accuracy of personal information, the responsible party is required to attach to the personal information (in a manner that it will be read with the personal information) an indication that a correction has been requested, but has not been made by the responsible party.[288] Where decisions have or will be made concerning the data subject, based on personal information that has been or will be corrected the responsible party must inform third parties of the steps that have been taken to correct the personal information.[289]

Manner of Access

Sections 18 and 53 of PAI Act, which regulates the form of access for information for public and private bodies; respectively, apply to requests made by a data subject to a responsible party.

5.3.3 Provisions relating to the processing of special personal information

Special personal information is information that relates to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. Special information also includes the criminal behaviour of a data subject insofar as it relates to the alleged commission of an offence or any proceedings in respect of such alleged offence by a data subject. [290] The Act contains a general prohibition against the processing of personal information by a responsible party where it relates to special personal information, except where:

(a) consent of the data subject has been obtained or the data subject has deliberately made the information public;

288 Sec 24(2) *POPI Act*.
289 Sec 24(3) id.
290 Sec 26 id.

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) processing is for historical, statistical or research purposes (subject to certain further criteria);

(e) the Regulator has authorised the responsible party to process such special personal information, subject to relevant safeguards or conditions to protect the personal information, by notice in the government gazette, upon application from the responsible party and such processing is in the public interest.[291]

In addition to the aforesaid exceptions, the Act the contains further specific circumstances relating to each category of special personal information when the responsible party is authorised to process special personal information relating to: religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour or biometric information.[292]

5.3.4 Processing of personal information relating to children

There is also a general prohibition on the processing of personal information relating to children,[293] except where:

(a) consent of a competent person has been obtained or the data subject has deliberately made the information public with the consent of a competent person;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

---

291 Sec 27 *POPI Act*
292 Sec 28-33 id.
293 Sec 34 id.

(d) processing is for historical, statistical or research purposes (subject to certain further criteria);

(e) the Regulator has authorised the responsible party to process such special personal information, subject to relevant safeguards or conditions to protect the personal information, by notice in the government gazette, upon application from the responsible party and such processing is in the public interest.[294]

A child is defined as a natural person under the age of 18 years (who is not legally competent).[295]

5.4 Enforcement of data privacy provisions

5.4.1 Information Regulator

The Act makes provision for the establishment of an information Regulator which is impartial and independent of government. The Regulator is accountable to the National Assembly and is subject to the Constitution and the law of the Republic of South Africa. The Regulator must perform its functions and exercise its powers without fear, favour or prejudice.[296]

5.4.2 Powers, duties and functions of the Regulator

The *POPI Act* grants the Regulator, inter alia, the following powers, duties and functions:[297]

(a) to provide education by promoting an understanding and acceptance of the conditions contained in the Act, undertaking education programmes, giving advice to data subjects regarding their rights, etc.;

(b) monitoring and enforcing compliance by public and private bodies;

294 Sec 35 *POPI Act*.
295 Sec 1 id.
296 Sec 39 id.
297 Sec 40 id.

(c) consulting with interested parties on any matter affecting the personal information of a data subject, co-operating on a national and international basis with bodies concerned with the protection of personal information;
(d) acting as a mediator between opposing parties where action is required by a responsible party concerning personal information relating to a data subject;
(e) handle complaints concerning alleged violations of the rights of data subjects;
(f) conduct research and report to parliament;
(g) establish and develop codes of conduct;
(h) to facilitate cross-border cooperation in the in the enforcement of privacy laws; and
(i) in general to exercise and perform functions, powers and duties imposed by the Act or other legislation.

The Regulator is also empowered to regulate both privacy matters, under the *POPI Act*, as well as access to information matters, under the PAI Act.[298]

5.4.3 Enforcement

5.4.3.1 Interference with protection of personal information of data subject.

The Act stipulates that interference with protection of personal information of data subject consists of:[299]

(a) any breach of the conditions for lawful processing of personal information;
(b) non-compliance with the provisions relating to:
    i. notification of security compromises;[300]
    ii. duty of confidentiality;[301]

[298] Sec 40(1)(h)(iv) and sec 110 *POPI Act* which amends the PAIA with the insertion of new provisions (i.e. sec 77A – 77K *PAIA*) relating to complaints lodged with the Regulator in ch 5A of the *POPI Act*.
[299] Sec 73 *POPI Act*.
[300] Sec 22 id.
[301] Sec 54 id.

iii. direct marketing by means of unsolicited electronic communications;[302]

iv. directories (printed or electronic) available to the public;[303] or

v. the prohibition related to automated decision making (also known as profiling)[304] and transfers of personal information outside the Republic of South Africa (i.e. TBDFs); or

(c) A breach of the provisions of code of conduct issued by the Regulator.[305]

5.4.3.2 Complaints

Any person may submit a claim, in writing, to the Regulator in the prescribed manner and form where it is alleged by the complainant that there has been an interference with the protection of personal information of a data subject.[306] Upon receipt of the complaint the Regulator may:[307]

(a) conduct a pre-investigation in terms of section 74;
(b) act as a conciliator;
(c) take no further action relating to the complaint, in accordance with section 77;
(d) conduct a full investigation of the complaint in accordance with the provisions of section 81 to 88;
(e) refer the complaint to the Enforcement Committee in terms of section 92;
(f) refer the complaint to another regulatory body, with jurisdiction;[308] or
(g) take any other action as allowed for in terms of Chapter 10 of the Act relating to enforcement.

5.4.3.3 Pre-investigation proceedings and settlements of complaints

302 Sec 69 *POPI Act*.
303 Sec 70 id.
304 Sec 71 id.
305 Sec 60 id.
306 Sec 74 id.
307 Sec 76 id.
308 Sec 78 id.

Before proceeding to investigate a complaint in terms of the Act the Regulator must inform the complainant, the data subject, any other alleged aggrieved party as well as the responsible party of the Regulator's intention to conduct an investigation. The Regulator should also provide the responsible party with the details of the complaint and inform the responsible party of its right to submit a written response, to the Regulator, within a reasonable time concerning the complaint.[309] If it appears to the Regulator that it may be possible to secure a settlement between the parties and, where applicable, secure a satisfactory assurance against repeated offences the Regulator may without further investigation attempt to settle such matter and obtain such assurance.[310]

5.4.3.4 Investigation proceedings by the Regulator

The Act gives the Regulator a wide range of powers to investigate a complaint. These rights include the summoning and appearance of persons before the Regulator to compel oral or written evidence in the same manner as in the High Court, administration of oaths, search and seizure rights of premises occupied by the responsible party, conducting private interviews with any person in any premises entered where a warrant has been issued[311] and executed[312] and to carry out any inquiries at such premises.[313] Following an investigation, the Regulator is obliged to inform the complainant and the responsible party of the outcome of the investigation as well as any developments relating to its failure to take any action due to its belief that there was no inference with the personal information of a data subject, enforcement notices that have been served, cancellation of served enforcement notices or appeals against enforcement notices as well as the outcome of such an appeal.[314]

309 Sec 79 *POPI Act*.
310 Sec 80 id.
311 Sec 82 id.
312 Sec 84 id.
313 Sec 81 id.
314 Sec 94 id.

5.4.3.5 Assessments and Information Notices

The Regulator also has the right to *meru moto* or on request of any party to make an assessment of whether an instance of processing of personal information complies with the provisions of the Act. The Regulator is obliged to conduct the assessment, if it seems appropriate. Where the Regulator has received a request for an assessment it is obliged to provide feedback in respect of such request. [315]

If the Regulator is of the view that it requires further information in order to determine whether a responsible party has, or is, interfering with the personal information of a data subject,[316] the Regulator may serve the responsible party with an information notice requiring the responsible party to provide the Regulator with a report indicating that the processing of personal information is compliant with the Act.

Once the assessment is completed, the responsible party must be notified of the outcome of the assessment as well as any recommendations that have been specified by the Regulator. The Regulator's report is deemed to be the equivalent of an enforcement notice.[317]

5.4.3.6 Enforcement Committee and enforcement notices

After completing the investigation of a complaint or any other matter related to the *POPI Act* or the PAI Act, the Regulator may refer such complaint or matter to the enforcement committee for consideration and recommendations concerning proposed actions to be taken by the Regulator against the responsible party, information officer or head of a private body.[318]

315 Sec 89, 91 *POPI Act*.
316 Cf par 5.4.3.1 above.
317 Sec 91 *POPI Act*.
318 Sec 92 - 93 id.

Once the Regulator has considered the recommendation of the enforcement committee and it is satisfied that that the responsible party is processing personal information unlawfully,[319] the Regulator may serve such responsible party with an enforcement notice. The enforcement notice may require the responsible party to: [320]

(a) take certain steps within a specified period;
(b) refrain from taking certain steps;
(c) stop processing personal information as specified in the notice;
(d) stop processing personal information for a purpose or in a manner specified in the notice, for the period specified in the notice.

Further provisions relating to content of an enforcement notice,[321] cancellation of enforcement notice[322] and appeals relating to enforcement notices are contained in the Act.[323]

5.5 Civil Remedies

A data subject or the Regulator (at the request of a data subject) may institute civil action, in a court having jurisdiction, against the responsible party for damages as a result of a breach of the conditions, certain other provisions of the Act or of a relevant code of conduct,[324] by a responsible party.[325]

The responsible party may raise any of the following defences:[326]

(a) *vis major;*
(b) the Plaintiff's consented to the breach;
(c) fault on the Plaintiff's part;

319 Cf par 5.4.3.1 above.
320 Sec 95 *POPI Act*.
321 Sec 95(2) id.
322 Sec 96 id.
323 Sec 97-98 id.
324 Cf par 5.4.3.1 above.
325 Sec 99 *POPI Act*.
326 Sec 99(2) id.

(d) compliance was not reasonably practical in the circumstance of the particular case; or

(e) regulatory exemption.[327]

If the Plaintiff is successful with his or her claim, the court may award an amount that is just an equitable in respect of damages as compensation (for patrimonial and non-patrimonial loss), aggravated damages, interest and costs.[328] 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.[329]

5.6 Offences, penalties and administrative fines

5.6.1 Offences

Offences *inter alia* include:[330]

(a) the obstruction or the exercise of unlawfully influencing the Regulator or any person acting on behalf of the Regulator;

(b) the breach of duty to treat as confidential personal information which comes to the knowledge of persons acting on behalf of the Regulator, in the course of the performance of his or her official duties;

(c) obstruction or failure to assist a person in the execution of a warrant of execution that is issued in terms of the Act;

(d) failure, by a responsible party, to comply with an enforcement notice;

(e) failure by a witness that has been summoned in terms of the Act to co-operate;

(f) failure by a responsible party to comply with the conditions of lawful processing where it relates to an account number of a data subject(s);

(g) where a third party, without the consent of the responsible party, knowingly discloses or procures the disclosure of an account number of a data subject to another person; and

327 Sec 37 *POPI Act*.
328 Sec 99(2) id.
329 Sec 99(4) id.
330 Sec 100 - 106 id.

(h) where a third party unlawfully sells or offers to sell the account number of a data subject.

5.6.2 Penalties

Conviction of the following renders one liable to a fine and / or imprisonment not exceeding 10 years:[331]

(a) obstruction or the exercise of unlawfully influencing the Regulator or any person acting on behalf of the Regulator;
(b) failure by a responsible party to comply with an enforcement notice;
(c) where a witness, after having been sworn in, gives false evidence knowing that such evidence is false;
(d) failure by a responsible party to comply with the conditions of lawful processing where it relates to an account number of a data subject(s);
(e) where a third party, without the consent of the responsible party, knowingly discloses or procures the disclosure of an account number of a data subject to another person;
(f) where a third party unlawfully sells or offers to sell the account number of a data subject.

Convicted of the undermentioned offences renders one liable to a fine and / or imprisonment not exceeding 12 months:[332]

(a) where the responsible party has failed to obtain prior authorisation from the Regulator;[333]

---

331 Sec 107(a) *POPI Act*.
332 Sec 107(b) id.
333 Sec 57 *POPI Act* requires prior authorisation from the Regulator if the responsible part plans to:
"(a) process any unique identifiers of data subjects-
(i) for a purpose other than the one for which the identifier was specifically intended at collection; and
(ii) with the aim of linking the information together with information processed by other responsible parties;
(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
(c) process information for the purposes of credit reporting; or

(b) The breach of persons', acting on behalf of the Regulator, duty to treat as confidential personal information which comes to his or her knowledge in the course of the performance of his or her official duties;

(c) obstruction or failure to assist a person in the execution of a warrant of execution that is issued in terms of the Act;

(d) where a responsible party, in purported compliance of an enforcement notice recklessly or purposefully makes a false statement; or

(e) where a witness that has been summoned in terms of the Act fails and without sufficient cause fails to attend the hearing, remain in attendance, refuses to be sworn in or make affirmation as a witness, fails to answer fully any question lawfully put to him or produce any book, document or object which he has been summoned to produce

Both the Magistrate's Court and the High Court have jurisdiction to impose any penalties specified in the Act.[334]

5.6.3 Administrative fines

Where it is alleged that a responsible party has committed an offence in terms of the Act the Regulator may cause an infringement notice to be served on the responsible party, the infringer. The infringer may choose to pay or make arrangements to pay the fine or may elect to be tried in court on a charge of having committed an offence in terms of the Act, in which case the Regulator must hand the matter over to the South African Police services.[335] Administrative fines may not exceed R10 million.

Where the responsible party does not comply with the infringement notice, the Regulator may file a statement with a competent court setting forth the amount of the administrative

(d) transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72."

334 Sec 108 *POPI Act*.

335 Sec 109(1)-(3) id.

fine payable by the infringer. Such statement has the effect of a civil judgement given in that court.

The Regulator may not impose an administrative fine where the responsible party has been charged with an offence in terms of the Act and neither may a prosecution be instituted where a responsible party has paid an administrative fine.[336]

Imposition of an administrative fine does not constitute a previous conviction in terms of the Criminal Procedure Act.[337]

5.7 Transitional Arrangements

The *POPI Act* requires that the processing of personal information must conform to the provisions of the Act within one year of the commencement of the Act.[338] To date hereof the President of South Africa has not yet announced the commencement of the remainder of the provisions of the Act.

6. How does the *POPI Act* compare with other international instruments?

6.1 Core Data Privacy Principles

6.1.1 A comparison between the *POPI Act* and other international instruments

At the end of this study is a detailed comparison between the core data privacy principles contained in the *POPI Act* and the conditions contained in *OECD* Guidelines, the *CoE*

336 Sec 109(6) - (7) *POPI Act*.
337 Act 51 of 1977.
338 Sec 114 *POPI Act*.

Convention and the *EU Directive*.[339] On the whole, it is evident that the *EU Directive* and the *POPI Act* offer better protection than the *OECD Guidelines* and *CoE Convention*.

When it comes to data sensitivity, the *POPI Act* offers superior protection to data subjects as opposed to the *CoE Convention*, *OECD Guidelines* and *EU Directive*.[340] The *POPI Act* also offers better protection to children as there is general prohibition against the processing of personal information relating to children, whereas similar provisions are absent in the *CoE Convention*, *OECD Guidelines* and *EU Directive*.[341] However, once the *EU Regulation* becomes operational it will address both of these limitations.[342]

Another aspect that bears mentioning is that once the *EU Regulation* becomes operational the *POPI Act* will still offer children superior protection due to the fact that the *POPI Act* defines a child as a "natural person under the age of 18 years,"[343] whereas the *EU Regulation's* prohibition on the processing of personal data of a child, only relates to children below the age of 13.[344]

Given the fact that the SALRC produced its *SALRC PDP Report* in 2009, it is some feat that the *POPI Act* has addressed aspects of the core data privacy principles that are only now being considered in the international arena.

In respect of the cost of compliance, The *EU Regulation* has a similar provision as contained in the *Modernisation* Proposal (which allows for member states to take the measures needed

339 See appendix 1 below.

340 The *POPI Act* includes "biometric information" under special information, whereas the EU Directive does not make provision for "biometric information" (Sec 26 *POPI Act*). The *POPI Act* further contains specific provisions which contain the exclusions for each category of special data, to the general prohibition on the processing special information (Sec 27 – 33 *POPI Act*), whereas the *EU Directive* only sets out general exclusions to the processing of special categories of data (Art 8(2) – (7) *EU Directive*).

341 Sec 34 *POPI Act*. Exceptions to the general prohibition are contained in sec 35 of the *POPI Act*.

342 Art 8 EU Regulation. Cf par 4.5.1.2; 4.5.1.3 above.

343 Sec 1 *POPI Act*.

344 Art 8 *EU Regulation*.

in order to adapt the application of the core data privacy principles, by taking into account the size of the data controller and / or the data processor, the volume or nature of data processed and the risks posed to the privacy rights of data subjects)[345] by allowing for micro, small and medium-sized enterprises to be exempt from certain of the provisions of the *EU Regulation*.[346] No such similar provision is contained in the *POPI Act*. It is submitted that the Regulator may not decide to exempt micro, small and medium-sized enterprises in terms of the provisions of section 37 of the *POPI Act*,[347] due to the fact that the Regulator when exercising his or her discretion to exempt a responsible party from the conditions for lawful processing of personal information, on the grounds that it is in the public interest to do so, may only do so in respect of a public body when taking into account the important economic and financial interests of such a public body.

6.2 Data subjects' rights

On the whole, the rights of a data subject, as specified in the *EU Directive,* are comparative with the data subject's rights specified in section 5 of the *POPI Act*.[348]

6.2.1 Modernisation Proposal

The *Modernisation Proposal* requires the data controller to perform a risk analysis of the potential impact on the privacy rights of a data subject, prior to the proposed processing of personal data. This provision is unique to the *Modernisation Proposal*.[349] The *EU Regulation* also has a similar provision; however, only once it has been determined that the processing

345 See par 4.2.2.5 above.

346 E.g. Art 8 (re: processing of personal data of a child), 12 (re procedures and mechanisms for exercising the rights of the data subject), 14 (re: information to be provided to the data subject, 22 (re: the responsibilities of the controller) and art 33 (re: the data protection impact assessment which is to be conducted by a data controller) of the EU Regulation.

347 See par 5.2.3.3 above.

348 Cf par 0 above. Examples include: direct marketing (art 14(b) *EU Directive* and sec 69 *POPI Act*), access to one's own data, and rectification (art 12 *EU Directive* and sec 23 - 24 *POPI ACT*), automated decision making (art 15 *EU Directive* and sec 71 *POPI Act*), etc.

349 Cf par 4.2.2.5 above. This is not to be confused with the risk assessment contained in sec 19(2)(1) of the *POPI Act*, which relates to security measures on integrity and confidentiality of personal information.

operations pose a specific risk.[350] The *POPI Act* does not have a similar proactive provision which requires the data controller to perform the risk assessment prior to the processing of personal information. However, as previously mentioned,[351] it must be borne in mind that the Regulator may *mero moto* (or at the request of any party) make an assessment of whether an instance of processing complies with the Act. Thereafter the Regulator may make recommendation to the responsible party in respect of action or proposed action that is to be taken in order to implement the recommendations contained in the Regulator's assessment. Clearly this provision is not as advanced as the provisions of the *Modernisation Proposal* and the *EU Regulation* which offer more protection as they are proactive. Nevertheless the *POPI Act* does offer some protection in this regard.

6.2.2 EU Regulation

If one has regard to the *EU Regulation* it would seem as if the *EU Regulation* offers more protection than the *POPI Act*, when it comes to the rights of the data subject. The *POPI Act* does not have a similar provision as set out in article 11 of the *EU Regulation* where information and communications in respect of the processing of personal data addressed to the data subject must be in an intelligible form, using clear and plain language and adapted to the data subject (especially where the data subject is a child).[352] Although, in instances where the data subject is also a consumer, as defined in the *Consumer Protection Act* (hereinafter "*CPA*"),[353] the data subject will be able to rely on his or her right to information in plain and understandable language as provided for in section 22 of the *CPA*.

In respect to the rights of rectification and erasure, [354] it is submitted that the *POPI Act* also provides for the "right to be forgotten," although this right is not explicitly specified as

350 Art 33 *EU Regulation* states that: "where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

351 See par 0 above.

352 Cf par 0 above.

353 68 of 2008.

354 Cf par 4.5.2.3 above; n 224; n 225 above.

provided for in article 17 of the *EU Regulation*. It must be borne in mind that the EU Court of Justice in the *Google Spain* case,[355] came to its decision based upon the provisions of article 6(1)((c)-(e) and Art 12(b) of the *EU Directive*.[356] The *POPI Act* has similar provisions in sections 10, 16 and 24,[357] which are comparative to article 6(1)((c)-(e) and Art 12(b) of the *EU Directive*.[358] It is therefore submitted that the same reasoning as applied by the EU Court of Justice could apply in South Africa.

The *EU Regulation* also provides for the right to portability of data,[359] which is not provided for in the *POPI Act*. However, the regulations[360] under the Electronic Communications Act[361] provide for mobile number portability[362] and as such the principle of data portability is recognised in the South African legal framework, albeit to a limited extent.

6.3 Data protection by design and by default

The EU Regulation introduces the two concepts of data privacy by design and data privacy by default.[363] The former means that data protection safeguards should be built into products and services from the earliest stage of development of such products and the latter means

355 Cf n 224 above.

356 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* par 93 – 94: "It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed. Therefore, if it is found, following a request by the data subject pursuant to Article 12(b) of Directive 95/46, that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with Article 6(1)(c) to (e) of the directive because that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased."

357 Cf par 5.3.2.8 above.

358 Cf appendix 1 below.

359 Cf par 4.5.2.3; n 226 above.

360 GN 889 in *GG* 30089 of 13 July 2007.

361 36 of 2005.

362 The definition of "**person information**" in sec 1 of the *POPI Act* includes a telephone number.

363 Art 23 *EU Regulation*; Cf n 161 above.

that privacy-friendly default settings should be the norm (e.g. on social networks).[364] The *Modernisation* Proposal has a similar provision to the data protection by design principle in article 8bis which requires the data controller to "… design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms". The *POPI Act* does not contain any provisions that are similar to the data protection by design and by default principles.

6.4 Trans-border data Flows

As with the other international instruments that have been discussed the *POPI Act* also contains a general prohibition on transfers of personal information to Third Countries that do not provide adequate levels of protection.[365] Both the *POPI Act* and the EU Regulation[366] also make provision for "binding corporate rules," where the responsible party within a group of undertakings transfers personal data within the same group of undertakings in a foreign country. However, the provisions as provided for in the EU Regulation are more onerous than those provided for in the *POPI Act*.

7. Conclusion

When one compares the *POPI Act* with some of the approaches that have been adopted within the international data protection instruments that have been discussed herein, it is quite surprising that the gap between the international instruments discussed and the *POPI Act* is not that large. Furthermore, in many instances the *POPI Act* provides better protection.[367]

364 Memo/14/186 4
365 Sec 72 *POPI Act*.
366 Chapter V of the *EU Regulation* deals with transfer of personal data to third countries or international organisations.
367 See par 6 above.

When comparing the *POPI Act* to the other international instruments discussed in this study, it can comfortably be said that the recommendations of the *SALRC PDP Report* have largely been achieved and that "… the protection of information privacy in South Africa …[is] in line with international requirements and developments",[368] especially insofar as it relates to the core data privacy principles and data subject's rights. This is no small feat when one considers that the SALRC issued its *SALRC PDP Report* in 2009 and that the European Commission only proposed its major reform of the EU legal framework on the protection of personal data, which lead to the proposed *EU Regulation*, in 2012.[369] Public consultation on the *Modernisation Proposal* commenced in 2011.[370] It is remarkable that the *POPI Act* has set such a high standard, by for example providing for biometric information as a special data category and allowing additional protection for children where the *CoE Convention*, *OECD Guidelines* and *EU Directive* initially failed to do so.[371]

When one looks at possible improvements to the *POPI Act* insofar as the rights of data subjects are concerned, the right of data protection by design, the right to data protection by default as well as the right to portability of data are possible considerations which should be considered for incorporation in any future amendments to the *POPI Act*. Another improvement to be considered for incorporation in any future amendments to the *POPI Act* is the cost of compliance by allowing for micro, small and medium-sized enterprises to be exempt from certain of the provisions of the *POPI Act*, which tend to drive up the costs of compliance.

What is strikingly apparent is that the South African legal framework, as the time of writing this study, when dealing with the processing of personal information and the protection of

368 Cf *SALRC PDP Report* ix.

369 European Commission press release "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" Brussels, 25 January 2012. Available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (accessed 2014-11-30).

370 The consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data, ETS 108, Strasbourg, 18 January 2012. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf (accessed 2014-11-30).

371 Cf par 6.1.1 above.

the rights of data subjects, in terms of the common law, other material pieces of legislation (that have been discussed herein) and the Constitution, is wholly inadequate.[372] This despite the fact that section 14 of the Constitution guarantees individuals the entrenched right to privacy.[373] Accordingly until such time as that the *POPI Act* becomes fully operational South Africa cannot be seen as a serious contender in the arena of data privacy.

Until such time as the remainder of the provisions of the *POPI Act* are enacted individuals will not be in a position to exercise active control over personal data in the hands of unscrupulous data controllers and neither will they be in a position to exercise any of the rights or remedies that have been incorporated in the *POPI Act*. One can only hope that the government of South Africa will prioritise this important piece of legislation that seeks to bring South Africa in line with the international community.

Word Count: 22 741

372 See par 2.2.3; 2.2.4 above.
373 See par 2.2.2 above.

Appendix 1:

A comparison between the *POPI Act*, the *OECD Guidelines,* the *CoE Convention* and the *EU Directive*

	POPI Act[374]	***OECD Guidelines***[375]	***CoE Convention***[376]	***EU Directive***[377]
Fair & Lawful processing	Sec 9(a) – (b)	Par 7	Art 5(a)	Art 6 (1)(a)
	Personal data must be processed lawfully and in a reasonable manner.	Personal data must be processed lawfully with knowledge or consent of the data subject, where applicable.	Personal data must be processed fairly and lawfully.	Personal data must be processed fairly and lawfully.
Purpose Limitation	Sec 13, S18 & S15	Par 9	Art 5(b)	Art 6(1)(b)
	Personal data must be complete must be collected for a specific, explicitly defined purpose of which the data subject is aware. Further processing must be compatible with original purpose.	The purpose should be specified at time of collection of personal data. Subsequent use limited to original purpose.	Personal data must be stored for specified and legitimate purposes and not used in a way incompatible with those purposes.	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
Data Quality (Minimality) * Relevant	Sec 10	Par 8	Article 5 (c)	Art 6(1)(c)
	Personal data must be complete adequate, relevant and not excessive.	Personal data must be complete relevant, accurate, complete and kept up-to-date.	Personal data must be complete adequate, relevant and not excessive.	Personal data must be complete adequate, relevant and not excessive.
* Accurate	Sec 10, S16 and S24	Par 8	Art 5(d) & 8(c) - (d)	Art 6(1)(d) & 12(b)-(c)

374 Cf par 5.3 above.
375 Cf par 4.3 above.
376 Cf par 4.2.1 above.
377 Cf par 4.4.1 above.

	Personal data may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive. (S10). A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary (S16). A data subject may request a responsible party to correct or delete personal information about the data subject l that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or to destroy or delete a record that the responsible party is no longer authorised to retain. S24	same as above	Personal data must be complete accurate and kept up-to-date. A data subject may to obtain, rectification or erasure of personal data if it has been processed contrary to the provisions of domestic law or the basic principles set out in Art 5 and 6 of the CoE Convention (Art 8(c)) and to have an additional remedy if the above request is not complied with (Art 8(d)).	Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it was further processed, is erased or rectified. A data subject may request the rectification, erasure or blocking of data if the processing of which does not comply with the provisions of the EU Directive, in particular because of the incomplete or inaccurate nature of the data (Art 12(b)) A data subject may request notification to third parties to whom the data has been disclosed of any rectification, erasure or blocking carried out in compliance with the above, unless this proves impossible or involves a disproportionate effort (Art 12(c))
* Limited retention	Sec 14		Art 5(e)	Art 6(1)(e)
	Personal data must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed		Personal data must be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored	Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed
Data Security	Sec 19 - 22	Par 11	Art 7 & Art 8	Art 17 & 18

	Deals with the responsible party's obligation 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 loss of, damage to or unauthorised destruction or unlawful access to personal information Additional provisions are provided for in respect of the data operator and notification to DPA.	data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data	Appropriate security measures shall be taken for the protection of data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. (Art 7) Additional safeguards for the data subject. (Art8)	Deals with the controller's obligation to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing Additional provisions are provided for in respect of the data operator and notification to DPA.
Data Sensitivity * General	Sec 26 – 33 & S27(2)		Art 6	Art 8 (1) and 8(2) - (7)
	General prohibition relating to the processing of personal information relating to the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject as well as criminal behaviour of a data subject. (Sec 26 - 33) Specific sections dealing with authorisations when processing special information in each		Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.	General prohibition relating to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. (Art 8(1)) Contains general exemptions to the prohibition in Art 8(1) (Art 8(2) - 8(7)). The only specific exemption for a specific category of data is for "criminal convictions" in Art 8(5).

	category will be permitted. (Sec 27(2))			
* Child	Sec 34 - 35			
	General prohibition relating to the processing personal information concerning a child			
Data subject influence	Sec 11; Sec 23 - 25	Par 10, and 13	Art 8(a) - (d)	Art 7(a), 8(2)(a) and 10 - 12.
	Data subjects are required to give consent for their personal data to be processed (Sec 11) A data subject has a right to: access his/her own personal information (Sec 23); and correction of personal information (Sec 24).	Personal data should not be disclosed, made available or otherwise used for purposes other than those for which the data was originally collected without the consent of the data subject (Par 10). Individuals have the right: to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them (Par 13).	These sections have been listed elsewhere in this table.	Data subjects are required to give consent for their personal data to be processed (Art 7(a) & 8(2)(a)) Data subject have a right to access their personal data (Art 12)
Openness	Sec 17 - 18; 22	Par 12	Art 8(a) - (b)	Art 18 – 19, 10 – 11 & 21

	A responsible party must maintain documentation of all processing operations. (Sec 17) Detailed list of information that must be provided to a data subject when collecting personal data from a data subject (Sec 18) Deals with notification of security compromises to the data subject as well as the DPA (Sec 22)	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	A data subject may: establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file (Art 8(a)); and obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form (Art 8(b))	Specifies the required information in cases of collection of data from the data subject is specified (Art 10). Specifies the required information in cases where the data has not been obtained from the data subject (Art11). Deals with obligation to notify DPA (Art 18 -19). Deals with publication of processing operations by the responsible party (Art 21)
Accountability	Sec 8	Par 14		Art 6(2)
	The responsible party must ensure that the conditions 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.	A data controller should be accountable for complying with measures which give effect to the principles in the OECD Guidelines		It is the data controller's responsibility to ensure that the conditions are complied with.

8. Bibliography

8.1 Books

I Currie & J KLaaren (2002) *The Promotion of Access to Information Act Commentary* Claremont: SiberInk

European Union Agency for Fundamental Rights (2014) *Handbook on European data protection law* Luxembourg: Publications Office of the European Union

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

J Neethling, JM Potgieter & JC Knobel (2006) *Law of Delict* Durban: Butterworths

J Burchell (1998) *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum* Cape Town: Juta

L A Bygrave (2014) *Data Privacy Law an International Perspective* New York: Oxford University Press[378]

[378] References to this authority are quoted by chapter and not by page number due to the fact that an eBook was used due to the unavailability of the hard copy.

8.2 Articles and Journals

K Allan & I Currie "Enforcing Access to Information and Privacy Rights: evaluating proposals for an information protection regulator for South Africa: current developments" (2007) 23 *South African Journal on Human Rights: Sexuality and the law: Special Issue* 570.

G Greenleaf "Global Data Privacy Laws: Forty Years of Acceleration" (2011) 112 *Privacy Laws and Business International Report* 11 – 17.

G Greenleaf "Global Data Privacy Laws 2013: 99 Countries and Counting" (2013) 123 *Privacy Laws and Business International Report* 10 – 13.

G Greenleaf "Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?" (2013) *Computer Law & Security Review* 430 – 436.

J Neethling "The Concept of Privacy in South African Law" (2005) 122 *South African Law Journal* 18

A Roos "Core Principles of Data Protection Law" (2006) *Comparative and International Law Journal of South Africa* 102

A Roos "Data Protection: explaining the international backdrop and evaluating the current South African position" (2007) *South African Law Journal* 402

A Roos "Personal Data Protection in New Zealand: Lessons for South Africa" (2004) *Potchefstroom Electronic Law Journal* 89

8.3 Legislation, Conventions and Directives

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, ETS 181, Strasbourg 8 November 2001.

APEC Privacy Framework (2005)

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data No 108 Strasbourg 1981

Electronic Communications and Transactions Act 25 of 2002

Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 on 15 December 1989, and contained in a document E/CN.4/1990/72

National Credit Act 34 of 2005

Organisation for Economic Cooperation and Development 2013 Privacy Framework

Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Paris, 23 September 1981

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

8.4 Other

European Commission (2014) "Factsheet on the "Right to be Forgotten" ruling (C-131/12)"

The King Code on Corporate Governance for South Africa (The Institute of Directors in Southern Africa) September 2009.

South African Law Reform Commission Project 124: "Privacy and Data Protection" Report 2009

M Heyink "Protection of Personal Information for South African Law Firms" (2011) *LSSA Guidelines*

M Heyink "Protection of Personal Information for South African Law Firms" (2012) *LSSA Guidelines*

8.5 Press release

European Commission (2012) "Commission to Renegotiate Council of Europe Data Protection Convention on behalf of EU" 19 November 2012 (Memo/12/877)

European Commission (2014) "Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote" 12 March 2014 (Memo/14/186)

8.6 Cases

Berstein & Others v Bester & Others NNO 1996 (2) SA 751

C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González [2014]

Grutter v Lombaard 2007 4 SA 89 (SCA)

Investigating Directorate: Serious Economic Offences and others v Hyundai Motor Distributors (Pty) ltd and others: In re Hyundai Motor Distributors (Pty) Ltd and others v Smit No and others 2001 (1) SA 545 (CC)

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

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

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 (T)

Universiteit Van Pretoria v Tommie Meyer Films (Edms) Bpk 1979 (1) SA 441 (A)