Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (1)*

A Naude
BCom LLB LLM
Contracts Manager (Accenture South Africa)

S Papadopoulos
BLC LLB LLM
Senior Lecturer in Mercantile Law, University of Pretoria

OPSOMMING

Databeskerming in Suid Afrika: Die Wet op Beskerming van Persoonlike Inligting 4 van 2013 in die lig van onlangse internasionale verwikkelinge

Die eerste nasionale wetgewing oor dataprivaatheid in die wêreld is in 1973 gepromulgeer. Dit het Suid-Afrika veertig jaar geneem om sy eie plaaslike nasionale wetgewing te promulgeer in die Wet op Beskerming van Persoonlike Inligting. Hierdie twee opvolgende artikels vergelyk die huidige Suid-Afrikaanse databeskermingsregsraamwerk met die benaderings wat gevolg is in internasionale databeskermingsinstrumente wat 'n groot invloed gehad het op die daarstel van die Wet op Beskerming van Persoonlike Inligting. Die bogemelde internasionale databeskermingsinstrumente is ook onlangs gewysig, of is in die proses om gewysig te word. Hierdie opvolgende artikels evalueer ook die nuwe wysigings wat aangebring is, of wat beoog word, in die internasionale databeskermingsinstrumente soverre sodanige wysigings betrekking het op kerndatabeskermingsbeginsels en die regte van datasubjekte. Die artikels ondersoek ook die vraag of daar enige wysigings aan die Wet op Beskerming van Persoonlike Inligting oorweeg moet word ten einde die Wet op dieselfde standaard te bring as die ander internasionale databeskermingsinstrumente wat bespreek word.

1 INTRODUCTION

It took South Africa forty years since the first enactment of national data privacy legislation[1] to enact its own data privacy legislation in the form of the Protection of Personal Information Act (PPI),[2] despite the fact that the South African Law

* This two-part article is an adaptation of an LLM dissertation entitled *Data protection in South Africa: the impact of the Protection of Personal Information Act and recent international developments* submitted by A Naude, University of Pretoria, 2014.

1 Sweden enacted the first Data Act (1973:289) in 1973. Cf Greenleaf "Global data privacy laws: Forty years of acceleration" 2011(112) *Privacy Laws and Business International Report* 11–17, available at http://ssrn.com/abstract=1946700 (accessed on 2 August 2014); Roos "Data protection: Explaining the international backdrop and evaluating the current South African position" 2007 *SALJ* 402.

2 Act 4 of 2013. It was enacted in terms of GN 912 in *GG* 37067 of 26 November 2013.

Reform Commission (SALRC) took the first steps towards enacting data privacy legislation in South Africa fifteen years ago.[3]

In April 2014, the provisions of PPI relating to the office of the Information Regulator and the issuing of the Act's regulations came into effect.[4] Once the remainder of the provisions of PPI become enforceable, parties that process personal information will be required to conform to the provisions of the Act within one year from the commencement of such provisions.[5] To date hereof, the President has not yet announced the commencement of the balance of the provisions of PPI.

This two-part article seeks to compare the current South African data protection legal framework with some of the approaches that have been adopted in other international data protection instruments and to evaluate whether or not South African legislation is still aligned with the most recent international developments in data protection. Whilst acknowledging that there are many exemplary international data privacy instruments, this article limits its focus to the instruments that initially shaped the PPI's existence, such as the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention),[6] the Organisation for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Trans-border Data Flows of Personal Data (OECD Guidelines)[7] 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 (Directive 95/46/EC). All three of these international instruments have recently been affected by amendments or proposed amendments. At the heart of this article 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. In order to complete the comparative study, this article examines the current data protection legal framework applicable in South Africa, followed by an analysis of these three international legal instruments, highlighting the effect of recent amendments or proposed amendments. The article concludes by comparing the current framework in South Africa with that of the amendments in the international instruments to determine if our current legislation is in need of review.

2 THE CURRENT DATA PROTECTION FRAMEWORK IN SOUTH AFRICA

2 1 Introduction

Bygrave states that data privacy laws are those rules that regulate the different stages in the processing of data and accordingly address the way in which data is

3 In 2000, the SALRC approved an investigation into privacy and data protection followed by the appointment of a committee to investigate in 2001. A final report was published in 2009 entitled "Privacy and data protection project 124" Report (2009) (hereafter the SALRC Report).

4 S 1 Part A of ch 5, s 112 and s 113 came into operation by virtue of Proc R25 in *GG* 37544 of 11 April 2014.

5 S 114 PPI.

6 Convention No 108 of 1981, Strasbourg, 28 January 1981.

7 OECD Guidelines available at http://bit.ly/1lWG9Qk (accessed on 20 September 2014).

"gathered, registered, stored, exploited and disseminated".[8] Furthermore, data privacy law is aimed at safeguarding the rights and interests of individuals, in their role as data subjects, when others are processing their data.[9]

2 2 Data privacy in South Africa prior to the PPI

2 2 1 Protection of privacy under the common law

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.[10]

Neethling defines privacy as

> "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".[11]

It can accordingly be said that the right to privacy entails an individual's right to control his personal information free from unwanted intrusions.[12] If one 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:[13]

(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.[14]

Although historically, privacy has often been equated with a right to dignity, the common law has developed to give recognition to an independent right to privacy.[15] 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.[16] Remedies for infringement are dealt with under the law of delict.[17]

---

8 Bygrave *Data privacy law an international perspective* (2014) 1.

9 *Ibid*.

10 Roos 2007 *SALJ* 421.

11 Neethling *et al Neethling's Law of personality* (2005) 32. This definition was confirmed in *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271–272. Cf Neethling "The concept of privacy in South African law" 2005 *SALJ* 18 20.

12 SALRC Report 2 para 1.2.1

13 Roos 2007 *SALJ* 403 422.

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

15 Neethling *et al* 217. The *locus classicus* for support of this view is *O' Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C), where, in holding that the unauthorised publication of a person's photograph and name for advertising purposes violated 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*). Cf also *National Media v Jooste* 1996 3 SA 262 (A). Similarly, in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 375 (T) it was held that identity is an independent personality interest worthy of delictual protection, but it was in *Grütter v Lombard* 2007 4 SA 89 (SCA) that it was finally determined that "[t]he 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'".

16 Neethling *et al* 219 273. Cf SALRC Report 24.

17 Neethling *et al* 5 250–251.

Privacy and identity should, however, be distinguished from each other with Neethling defining identity as "a person's uniqueness or individuality that identifies him as a particular person and thus distinguishes him from others".[18] Given the aforesaid, identity entails an individual's right to have control over the accuracy of his or her information.[19]

2 2 2 Common law remedies for infringement of privacy or identity

Delictual actions can generally be classified into one of three categories:[20]

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

(b) the wrongful infringement of interests of personality (referred to as an *iniuria*);[21] and

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

Damages are claimed, in the case of patrimonial loss, with the *actio legis Aquiliae* and, in the case of non-patrimonial loss, with the *actio iniuriarum* for compensation as satisfaction (referred to as *solatium*) for the injury caused to the plaintiff's personality.[22]

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)[23] the aggrieved party can rely on the principles of the law of delict to exercise his or her remedies. Such remedies will be limited to the following:

(a) an interdict to prevent the wrongful processing or the 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; or

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

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, at 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*).[24]

---

18 *Idem* 32; Roos 2004 *PER* 91.
19 Roos 2007 *SALJ* 422.
20 Neethling *et al Law of delict* (2015) 8 267.
21 The unlawful infringement of privacy and identity would fall under this type of delict.
22 Neethling *et al* 267–268 270–271.
23 Roos 2007 *SALJ* 422 fn 172.
24 Neethling *et al* 273.

2 2 3 Protection of privacy under the Constitution

The Constitution of the Republic of South Africa is the supreme law of the country and any conduct or law that is inconsistent with the Constitution is invalid.[25] The Bill of Rights, set out in Chapter 2 of the Constitution, contains the entrenched fundamental rights which are binding on the executive, the legislature, organs of state as well as natural and juristic persons.[26] The entrenchment of these rights in the Constitution fortifies their protection and gives the fundamental rights a higher status in that they apply to all law.[27] Any law or action by the state or a 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 or if it is balanced with another fundamental right contained in the Constitution.

Section 14 of the Constitution entrenches the right of privacy.[28] Identity is not recognised *eo nomine* in the Bill of Rights. However, Neethling 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.[29] The right to identity should therefore be protected under the right to human dignity, which is explicitly mentioned in section 10 of the Constitution.[30]

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.[31] One could also argue that the government has a constitutional responsibility to prioritise the enactment of the remainder of the provisions of PPI because, as will transpire later in this article, the common law is clearly not equipped to deal with data privacy.

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) when in *Bernstein v Bester*[32] it limited privacy to the "inner sanctum" of a person's life when the court held that "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".[33]

---

25 S 2 Constitution.
26 S 8(1) and (4) Constitution.
27 SALRC Report 20 para 2.1.11.
28 "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."
29 Neethling *et al* 18 fn 147.
30 Roos 2007 *SALJ* 422.
31 *Idem* 423.
32 *Bernstein v Bester* 1996 2 SA 751 (CC) 788C.
33 789A.

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.[34] In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*,[35] the informational right to privacy was interpreted as coming 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.

When it comes to interpreting fundamental rights and their limitation, the court warned that caution must be exercised.[36] It 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, at common law there is a single enquiry as to whether or not an unlawful infringement has taken place.[37]

2 2 4 Limitations to the protection of data privacy under the common law and the Constitution

The 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. Traditional delictual principles do not give active control to the individual because they do not cater for instances where the data subject is unaware that his or her personal information is being processed, that the personal information is accessible or that incorrectly held personal information may be corrected or removed.[38]

Neethling proposes that in order for the individual to exercise active control over his or her personal information, an individual must be aware of the existence of the data record containing that information; aware of the purposes for which the data is being processed; be legally entitled to have access to such data records; be legally entitled to know who has access to those records and legally entitled to procure a correction or deletion of the data.[39]

Only once an individual has active control over his or her own personal data do the traditional common law protections play a more meaningful role.[40]

2 3 Data protection under existing South African legislation

Prior to the promulgation of PPI, South African law did not have omnibus data privacy legislation.[41] Currently, there are predominantly four statutes, discussed below, that contain data protection provisions albeit in a limited capacity. These are the Promotion of Access to Information Act (PAIA),[42] the Electronic

34 Neethling 2005 *SALJ* 20.
35 *In Re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 1 SA 545 (CC) 557.
36 *Bernstein v Bester* 790D–E; Burchell *Personality rights and freedom of expression: The modern actio injuriarum* (1998) 388; SALRC Report 21 para 2.1.14.
37 Cf SALRC Report 34 para 2.3.5.
38 Roos 2007 *SALJ* 423.
39 Neethling *et al* 278.
40 *Idem* 280.
41 Roos 2007 *SALJ* 424. Not all the sections of PPI have as yet been enacted and therefore the position regarding data privacy under the common law and under legislation, as discussed above, still applies.
42 Act 2 of 2000.

Communications and Transactions Act (ECTA),[43] the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[44] and the National Credit Act (NCA).[45]

2 3 1 PAIA

PAIA is essentially a law that has been enacted to give effect to an individual's constitutional right of access to information[46] held by the State or any another person and when this information is required for the exercise or protection of any rights.[47] This Act 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;[48]

(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;[49] and

(c) prohibiting the disclosure of a record if it would involve the unreasonable disclosure of personal information relating to a third party.[50]

2 3 2 ECTA

ECTA was enacted to regulate electronic transactions.[51] Sections 50 and 51 contain provisions that relate to the protection of the personal information of an individual that has been obtained through an electronic transaction.[52] 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.[53] 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.[54] The rights and obligations of the parties, in the event of a breach of the said voluntary data privacy principles, are to be regulated by the agreement between the parties.[55] These two sections will be repealed once PPI becomes fully enforceable.[56]

---

43 Act 25 of 2002.
44 Act 70 of 2002.
45 Act 32 of 2005.
46 S 32 the Constitution.
47 Preamble to PAIA.
48 S 11 (re public body) and s 50 (private body) PAIA.
49 For a discussion on the reason why PAIA does not contain specific provisions for individuals to correct incorrect data, see Currie and Klaaren *The Promotion of Access to Information Act commentary* (2002) 18.
50 S 34 (public body) and s 63 (private body) PAIA.
51 Preamble to ECTA.
52 S 50(1). S 1 defines a "transaction" as being either of "a commercial or non-commercial nature, including the provision of information and e-government services".
53 S 50(2) ECTA.
54 S 50(3).
55 S 50(4).
56 Schedule to PPI.

Glaring deficiencies in the data protection provision of ECTA include the fact that the data privacy principles are voluntary (and only binding if agreed to by both parties) with the result that there is very little uptake of these provisions, very low awareness among data subjects and very low compliance with these voluntary provisions.[57]

2 3 3 RICA

RICA prohibits the interception[58] and monitoring of any communication in the course of its occurrence or transmission within South Africa.[59] There are, however, certain statutory exemptions such as when the intercepting party is also a party to the intercepted communication, when a party to the communication has given prior written consent to the interception, where the interception is to prevent serious bodily harm and to locate a person in case of an emergency.[60] The definitions are seemingly wide enough to prohibit the collecting of personal information but it is limited to collecting via interception.

2 3 4 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).[61]

In respect to the right to confidentiality, the NCA states that any person, who receives, compiles, retains or reports any confidential information relating to a consumer or prospective consumer must protect the confidentiality of that

57 Unauthorised access to data is also dealt with in ECTA as an offence and, in particular, s 86(1) prohibits a person from intentionally accessing or intercepting any data without authority or permission to do so.

58 "Intercept" is defined as "an aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication and includes: (a) the monitoring of any such communication by means of a monitoring device; (b) viewing or examining or inspecting the contents of any indirect communication; and (c) the diversion of any indirect communication from its intended destination to any other destination and 'interception' has a corresponding meaning": s 1 RICA

59 S 2 RICA. In s 1 a distinction is drawn between direct and indirect communications. A "direct communication" is an oral communication other than an indirect communication, between two or more person in the immediate presence of all other persons participating in the communication; or it is an utterance by a person participating in an indirect communication if the utterance is audible to another person, who at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. An "indirect communication" is the transfer of information, including a message or part thereof either in the form of speech, music, sound, data, text, visual imagery, signals, radio frequency spectrum or in any other form or combination of form that is transmitted in whole or in part by means of the postal service or telecommunication system.

60 Ss 4–5 7–8 and cf ss 6 9–11 for further exemptions and ss 16–25 for the process and requirements to obtain an interception order, decryption direction or entry warrant.

61 Preamble to NCA.

information.[62] Furthermore; 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 a compliance notice, issued by the National Credit Regulator[63] in respect of the right to confidentiality provisions is an offence in terms of the NCA.[64]

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. Such information includes the name, address, and identifying number of the consumer as well as information about the credit provided such as the credit limit and principal debt involved.[65]

In respect of consumer credit information[66] 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 providing a report to any person containing inaccurate information.[67]

The NCA also gives individuals the right to access and challenge credit records and information.[68]

If one has regard to the discussion above concerning data privacy and the common law, 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, but the South African statutory framework remains inadequate when it comes to the processing of personal information, that is, until the PPI becomes fully fledged law.

2 4 The Protection of Personal Information Act

2 4 1 Introduction

The shortcomings as described above demonstrate that a massive overhaul of the statutory framework was necessary in order to ensure that legislation provided an adequate level of data protection.[69] For this reason, PPI was enacted.

Data protection refers to the legal protection afforded to a person (a data subject) in respect of the processing[70] of personal data concerning the data subject

62 S 68 NCA. "Confidential information" is defined in s 1 as "personal information that belongs to a person and is not generally available to or known by others".
63 Established under s 12 NCA.
64 S 70(6).
65 Established under s 69 NCA.
66 "Consumer credit information" as defined in s 70 includes a person's credit history, financial history, education, employment career, business history or identity.
67 S 70(2).
68 S 72.
69 SALRC Report ix.
70 S 1 PPI 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,

continued on next page

by another person, institution or organisation (data controller). A third party processing personal data on behalf of the data controller is referred to as a "data processor".[71]

The PPI uses the terms "personal information"[72] instead of personal data, "responsible party"[73] instead of data controller, "operator"[74] instead of data processor and "conditions" for lawful processing instead of data privacy "principles".[75] However, in essence these terms bear similar meanings and are interchangeable.

2 4 2 Application

One of the PPI's stated aims is to regulate the manner in which personal information may be processed, subject to certain conditions for lawful processing, which accord with international standards.[76]

The PPI applies to the processing of personal information entered into a record by or for a responsible party by making use of automated or non-automated means; provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.[77] It also applies to both private and public bodies.

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 PPI.[78]

---

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".

71 Neethling *et al* 276. Cf Roos "Core principles of data protection law" 2006 *CILSA* 104.

72 S 1 PPI 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".

73 S 1 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".

74 S 1 defines an "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".

75 Ch 3.

76 S 2(a)–(d).

77 Ss 1 and 3 for definitions.

78 S 2(a)–(b).

The PPI does not however apply where the processing of personal information:[79]

(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 processed by the Cabinet; or

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

Section 7 contains exclusions for the processing of personal information for journalistic, literary or artistic purposes and where the responsible party is subject to a code of ethics that provides adequate safeguards for the protection of personal information.

Other exclusions included relate to situations where the regulator may grant an exemption to the responsible party for the processing of personal information provided it is in the public interest;[80] where there is a clear benefit for the data subject or a third party that outweighs any interference with the privacy of the data subject or third party[81] or the personal information is processed for the purpose of discharging a relevant function.[82]

Accordingly, the processing of personal information by the responsible party, falling within the ambit of the PPI, must comply with the conditions specified in the Act.

2 4 3 Conditions for the lawful processing of information

The conditions do not stand in isolation and often interact and overlap with one another and therefore need to be viewed holistically.[83]

2 4 3 1 Condition 1: Accountability

In terms of section 8 the responsible party must ensure that the conditions set out in the Act, and all the measures that give effect to such conditions, are complied with.

---

79 S 6(1)(a)–(e).

80 S 37(2) considers "public interest" to include 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.

81 S 37.

82 S 38(1). S 38(2) provides that a "relevant function" means "any function – (a) of a public body; or (b) conferred on any person in terms of the law, 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".

83 Heyink "Protection of personal information for South African Law firms" 2011 *LSSA Guidelines* 10; SALRC Report 161.

This means that the responsible party is the party who is ultimately held responsible for compliance, regardless of whether or not the personal information has been handed to an operator to process for or on behalf of the responsible party.[84]

2 4 3 2 Condition 2: Processing limitation

The processing limitation entails that the responsible party needs to process in a lawful and reasonable manner so as not to infringe the privacy of the data subject;[85] limit the processing to levels that are adequate, relevant and not excessive;[86] with the data subject's consent[87] (although numerous exceptions apply);[88] and the data must be collected directly from the data subject (although numerous exceptions apply).[89]

2 4 3 3 Condition 3: Purpose specification

This condition is the critical core condition because the purpose specification underpins all other aspects of processing under the Act, that is, it defines the scope of processing.

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.[90] The PPI compels the responsible party to take reasonable steps[91] to ensure that the data subject is aware of the purpose of the collection of personal information, unless the responsible party is exempt.[92]

---

84 Heyink (2011) 11.

85 S 9 PPI.

86 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.

87 Referring to ss 13 and 18 PPI, it is clear that blanket consent will not be in compliance with the Act and a responsible party carries the burden of proof to show that consent was properly given.

88 S 11(1).

89 The exceptions include instances where the information is contained in a public record, is 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 conducting 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 reasonably practicable in the circumstances of a particular case (s 12).

90 S 13.

91 S 18(1)(a)–(h) 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 and any other relevant information.

92 S 18(4).

As part of the purpose specification requirements, personal information may not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed.[93]

2 4 3 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).[94] In order to assess whether or not further processing is compatible with the initial purpose for which it was collected, the PPI lists factors to be taken into account, as well as specific instances where further processing, by the responsible party, is considered to be compatible with the initial purpose for which it was collected.[95]

2 4 3 5 Condition 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.[96]

2 4 3 6 Condition 6: Openness

This condition requires the responsible party to take reasonable steps to ensure that the data subject is aware of the information being collected, the source from which it is collected, the name and address of the responsible party; the purpose for which the information is being collected; whether or not the supply of information is mandatory or voluntary; the consequences of failure to provide the information; if applicable, the law authorising collection of the information; and 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.[97]

2 4 3 7 Condition 7: Security safeguards

A responsible party is required to secure the integrity and confidentiality of personal information, having regard to generally accepted information security practices and procedures[98] and by taking appropriate reasonable technical and organisation measures to prevent loss of, unauthorised destruction of, unlawful access to or processing of personal information.[99]

---

93 S 14(2)–(3). Exceptions are contained in s 14(1)(a)–(d) and s 14(2)–(3).
94 S 15.
95 S 15(2)–(3). These instances of further processing, contained in s 15(3)(a)–(f), are similar to the grounds upon which information may be processed as specified in s 9(1)(a)–(f).
96 S 16.
97 S 18(1)(a)–(h). Certain exceptions are listed in s 18(4)(a)–(f).
98 S 19(3).
99 S 19(1).

Accordingly, the responsible party must take reasonable measures to[100]

(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.

Where there are reasonable grounds to believe 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.[101]

2 4 3 8 Condition 8: Data subject participation

This condition allows a data subject to access, view and correct information held by a responsible party and therefore they can request the responsible party to confirm, at no charge to the data subject, whether or not the responsible party holds personal information relating to the data subject;[102] and 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.[103] 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 PAIA.[104]

A responsible party is also required to advise the data subject of his or her right to request a correction of information,[105] and where the responsible party is no longer authorised to retain the personal information, the data subject may request the destruction or deletion of the information.[106] The responsible party must comply with such a 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.[107] 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.[108]

---

100 S 19(2).

101 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 (s 22).

102 S 23(1)(a).

103 S 23(1)(b).

104 Ch 4 (Part 2) and ch 4 (Part 3) PAIA, which relate to grounds for refusal of access to records held by public and private bodies respectively.

105 Ss 5(c) and 24 PPI.

106 S 24(1).

107 S 24(2).

108 S 24(3).

2 4 4 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.[109]

The PPI 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;

(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.[110]

In addition to the aforesaid exceptions, the Act 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.[111]

2 4 5 Processing of personal information relating to children

There is also a general prohibition on the processing of personal information relating to children,[112] 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;

---

109 S 26.
110 S 27.
111 S 28–33.
112 S 34. A child is defined as a natural person under the age of 18 years (who is not legally competent) (s 1).

(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.[113]

2 4 6 Enforcement of data privacy provisions

PPI makes provision for the establishment of an information regulator that 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.[114]

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.[115] Upon receipt of the complaint the regulator may:[116]

(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;[117] or

(g) take any other action as allowed for in terms of Chapter 10 of PPI relating to enforcement.

The regulator also has the right, *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 PPI. The regulator is obliged to conduct the assessment, if it seems appropriate.[118]

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, 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 PPI.[119]

---

113 S 35.

114 S 39. The information regulators' powers and duties are set out in s 40 and, in particular, they are empowered to handle complaints by receiving and investigating complaints about alleged violations of PPI and reporting to complainants about the complaints (s 40(1)).

115 S 74.

116 S 76.

117 S 78.

118 Ss 89 and 91.

119 S 90.

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.[120]

Once the regulator has considered the recommendation of the enforcement committee and it is satisfied that the responsible party is processing personal information unlawfully, the regulator may serve such responsible party with an enforcement notice. The enforcement notice may require the responsible party to take or refrain from taking certain steps within a specified period or stop processing personal information as specified in the notice.[121]

2 4 7 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 PPI or of a relevant code of conduct, by a responsible party.[122]

The responsible party may raise any of the following defences:[123]

(a) *vis major*;
(b) the plaintiff's consent to the breach;
(c) fault on the plaintiff's part;
(d) compliance was not reasonably practical in the circumstance of the particular case; or
(e) regulatory exemption.[124]

If the plaintiff is successful with his or her claim, the court may award an amount that is just and equitable in respect of damages as compensation (for patrimonial and non-patrimonial loss), aggravated damages, interest and costs.[125] 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.[126]

2 4 8 Offences, penalties and administrative fines

Offences under the PPI are dealt with in sections 100 to 106 and include the breach of the 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; failure, by a responsible party, to comply with an enforcement notice; 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); 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 where a third party unlawfully sells or offers to sell the account number of a data subject. Conviction of any of these renders one

120 S 91.
121 S 95.
122 S 99.
123 S 99(2).
124 S 37.
125 S 99(2).
126 S 99(4).

liable to a fine and/or imprisonment not exceeding 10 years.[127] Both the Magistrate's Court and the High Court have jurisdiction to impose any penalties specified in the Act.[128]

Where it is alleged that a responsible party has committed an offence in terms of PPI, 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 which case the regulator must hand the matter over to the South African Police Services.[129] Administrative fines may not exceed R10 million.

3 CONCLUSION

There is no doubt that the PPI will usher in a comprehensive data protection framework, significantly better than the framework in place prior to its enactment. However, this two-part article seeks to compare this new framework with some of the approaches that have been adopted in other international data protection instruments that have recently undergone amendments or proposals for amendments and in so doing, evaluate whether or not South Africa remains aligned with the international community in respect of data privacy legislation.

(to be continued)

127 S 107(a). S 107(b) sets out offences for which the penalty is a fine and/or imprisonment not exceeding 12 months.

128 S 108.

129 S 109(1)–(3).