Data protection in South Africa: The Protection of Personal Information Act 4 of 2013 in light of recent international developments (2)*

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

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

1 INTRODUCTION

It took South Africa forty years since the first enactment of international 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 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, 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

* See 2016 *THRHR* 51 for Part 1.

1 Sweden enacted the first 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 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.

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

4 S 1 Part A of ch 5, s 112 and s 113 came into operation in accordance with the provisions of Proclamation No R25 in *GG* 37544 of 11 April 2014.

5 S 114 PPI.

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, the 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). These three international instruments also all recently have 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.

Part I of the article explored the regulatory framework for data protection in South Africa and concluded that there was no doubt that the PPI would usher in a comprehensive data protection framework, significantly better than the framework in place prior to its enactment. It therefore remains for the second part of the article to complete the comparative investigation by analysing the international data protection instruments that have recently undergone amendments or proposals for amendments and, in so doing, evaluate whether South Africa remains aligned with the international community as originally envisioned by the PPI.

2 DATA PRIVACY IN INTERNATIONAL INSTRUMENTS

2 1 Introduction

Bygrave[8] maintains 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 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 others process their data.

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[9] or conditions[10]) that should be embodied in data protection legislation.[11] These core data protection principles are contained, in one form or another, in all successful data protection laws and, according to Bygrave, include fair and lawful processing; proportionality,

6 Convention No 108 of 1981, Strasbourg, 28 January 1981.
7 OECD Guidelines available at http://bit.ly/1lWG9Qk, accessed on 2 September 2014.
8 *Data privacy law: An international perspective* (2014) 1.
9 As found in the CoE Convention, OECD Guidelines and Directive 95/46/EC.
10 Ch 3 PPI.
11 Roos "Core principles of data protection law" 2006 *CILSA* 107; Bygrave (2014) 2.

minimality; purpose limitation; data quality; data security; data sensitivity; and data subject influence.[12] Roos adds the principles of openness and transparency,[13] accountability and exemptions.[14]

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 is grouped together in order to form a single principle.[15] The principles also seldom are applied as absolutes.[16]

Although Sweden enacted data privacy legislation as early as 1973, 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 countries of origin, known as trans-border data-flows (hereinafter TBDFs).[17]

Three vital instruments have had a profound effect on data privacy laws across the world, namely, the CoE Convention; the OECD Guidelines; and Directive 95/46/EC (all discussed further below); and, according to Bygrave, these display four general features which are characteristic of successful international instruments:[18]

(a) privacy law is largely statutory;

(b) data privacy legislation normally establishes independent regulatory bodies or 'data protection authorities' (hereinafter DPA) to oversee its implementation;

(c) data privacy laws often take the form of "framework" laws; and

(d) DPAs play a lead role in how data privacy law is understood and applied, even where their views are only advisory.

In line with the comparative aspect of this article, the discussion now turns to these three instruments that have shaped data privacy laws worldwide.

2 2 CoE Convention

2 2 1 Core principles

The CoE Convention contains its core 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 Convention.[19] However, the Convention is not self-executing and no individual rights can be derived from it.[20]

---

12 Bygrave (2014) 1.

13 Roos 2006 *CILSA* 116. Examples of this principle are found in Directive 95/46/EC in the notification procedure (arts 18–19); the DPA must keep a register of data processing operations about which it has been notified (art 21) and the fact that data controllers have a duty to keep the data subject informed (arts 10 and 11(1)).

14 Roos 2006 *CILSA* 127–128.

15 Bygrave (2014) ch 5 paras A–I.

16 *Idem* para A.

17 Roos 2007 *SALJ* 403; SALRC Report para 1.2.12.

18 Bygrave (2014) 1 and Roos 2007 *SALJ* 404.

19 Art 4 CoE Convention.

20 SALRC Report 143.

Chapter two sets out the core principles under the following titles:

(a) duties of the parties;[21]

(b) quality of the data which includes provisions relating to the fair and lawful processing, purpose limitation and minimality;[22]

(c) special categories of data;[23]

(d) data security;[24]

(e) safeguards for the data subject;[25]

(f) sanctions and remedies;[26] and

(g) extended protection.[27]

Chapter three states that member states shall not prohibit TBDFs to the territory of another member state unless they 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.[28]

In May 2001, the CoE Committee of Ministers adopted an additional Protocol which made provision for member states to establish DPAs; and to allow for TBDFs to recipients who are not a party to the CoE Convention by requiring that the recipient ensures an adequate level of protection for the intended data transfer.[29]

---

21 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.

22 Art 5 provides 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".

23 Art 6 provides 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".

24 Art 7 provides that appropriate security measures must be taken for the protection of personal data stored in automated data files.

25 Art 8 contains additional safeguard provisions relating to automated personal data files such as rights of access, rectification and erasure.

26 Art 10 provides for each party to establish appropriate sanctions and remedies for violations of provisions of domestic law.

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

28 Art 12.

29 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows, ETS 181, Strasbourg, 8 November 2001, available at http://bit.ly/1K8ZMPW, accessed on 18 October 2014.

2 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.[30] 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 Modernisation Proposal).[31]

The Modernisation Proposal seeks to build on the current data protection principles, but only material changes proposed to the current CoE Convention as introduced by the Modernisation Proposal are highlighted below.

2 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 for personal data.[32] Firstly, that such processing must be proportionate in relation to the legitimate purpose pursued, i.e. 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 foundation laid down by law.

In respect of data quality provisions, the proposed change requires that data quality principles should apply to all personal data processed and not just personal data undergoing automatic processing, as was stipulated in the original provisions of the CoE Convention.

2 2 2 2 Processing of sensitive data

It was further proposed that genetic data, identifying biometric data and trade union membership be added as categories of sensitive data, with the accompanying appropriate safeguards, to prevent the risk of discrimination against the data subject on these grounds.[33]

2 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.[34] Data controllers are further required to notify the relevant DPA of any data breaches that may seriously interfere with the rights of data subjects.[35] Interestingly, the Modernisation

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

31 The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS no 108], Strasbourg, 18 December 2013, available at http://bit.ly/1Hat00r, accessed on 18 October 2014. 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://bit.ly/1SFnDYV, accessed on 18 October 2014; Greenleaf "Modernising Data Protection Convention 108: A safe basis for a global privacy treaty?" 2013 *Computer Law & Security Review (CLSR)* 430, available at http://bit.ly/1BIFSc6, accessed on 16 September 2014.

32 Art 5 Modernisation Proposal.

33 Art 6.

34 Art 12*bis*.

35 Art 7.

Proposal does not require the data subject to be notified of such breach.[36] The remainder of the data security provisions are similar to the original provisions contained in the CoE Convention.

2 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 parties, except where the processing is prescribed by law or it proves to be impossible or involves disproportionate efforts.[37]

2 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. These are similar to those contained in Directive 95/46/EC and the EU Regulation,[38] as discussed in more detail below.

Another provision that was not included in the original CoE Convention is the requirement that member states should ensure that data controllers and/or data processors are required to:[39]

(a) take, at all stages of the processing process, all appropriate measures, which give effect to the data privacy principles and be able to demonstrate compliance to the relevant DPA;[40]

(b) 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; and

(c) take into account the rights of data subjects in respect of products and services, intended for data processing, from the stage of their design.[41]

An interesting provision which has been included in order to reduce the cost of compliance allows 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.[42]

36 Although the Draft Explanatory Report to the Modernisation Proposal encourages notification to data subjects where a data breach has occurred (para 66).

37 Art 7*bis*.

38 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 (hereafter EU Regulation) available at http://bit.ly/1mRrHn6, accessed on 20 September 2014.

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

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

41 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.

42 Art 8*bis*(4) Modernisation Proposal.

2 3 OECD Guidelines

2 3 1 Core principles

The OECD Guidelines similarly contain a set of eight data-protection principles that apply to the processing of personal data. However, the 1980 version did not contain requirements as to how these principles were to be enforced by member nations. The eight data-protection principles contained in the Guidelines include the limitation of collection;[43] data quality;[44] purpose specification;[45] use limitation;[46] security safeguards;[47] openness;[48] individual participation;[49] and accountability.[50]

On TBDFs the Guidelines require member countries to take all reasonable and appropriate steps to ensure that TBDFs of personal data remain secure and uninterrupted,[51] save for three instances where the member country should prevent a data flow such as if the receiving country does not have acceptable data-protection rules, only acting as a transit country for another country which has not implemented the OECD Guidelines and the member country has imposed restrictions on special categories of personal data, and if the receiving jurisdiction does not have similar protections enabled.[52]

According to Roos, members of the OECD include the most important countries in the information-communications arena, such as the USA, most European countries, Canada, Japan, Australia and New Zealand and, through its affiliations with 70 non-member countries, the OECD has global reach, making it instrumental in data-protection. However, because the Guidelines are not legally binding, and because they allow for considerable variation in implementation amongst member states, they are not adequate to ensure the proper functioning of a global market.[53]

---

43 Para 7 OECD Guidelines provides 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.

44 Para 8 provides that personal data should be relevant to the purpose for which it is collected, accurate and kept up-to-date.

45 Para 9 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.

46 Para 10 states that personal data should not be disclosed for any other purpose than the purpose specified, unless the data subject has consented or it is required by law.

47 Para 11 requires personal data to be protected by reasonable security safeguards against loss, unauthorised access, modification, use or disclosure.

48 Para 12 requires a general policy of openness regarding policies and practices relating to personal data.

49 Para 13 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.

50 Para 14 provides that a data controller should be accountable to comply with the other seven principles.

51 Para 16.

52 Para 17.

53 Roos in Van der Merwe *et al Information and communication technology law* (2008) 324.

2 3 2 Revised OECD Privacy Guidelines 2013

The OECD Guidelines were revised in 2013 and are referred to as the updated/ revised OECD Privacy Guidelines.[54] This revision was required due to changing technologies, markets, user behaviour and the greater importance of digital identities. It was highlighted that compared with the situation 30 years ago, there has been a profound change of scale in terms of the role of personal data in our economies, societies and daily lives. The environment in which the traditional privacy principles now are implemented has undergone significant changes, for example, in the volume of personal data being collected, used and stored; the range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities; the value of the societal and economic benefits enabled by new technologies and responsible uses of personal data; the extent of threats to privacy; the number and variety of actors capable of either putting privacy at risk or protecting privacy; the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate; and, finally, the global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.[55]

Two themes run through the revised Privacy Guidelines of 2013. First, is a focus on the practical implementation of privacy protection through an approach grounded in risk-management. Second, is the need for greater efforts to address the global dimension of privacy through improved interoperability;[56] however, once again only material changes adopted are highlighted below.

2 3 2 1 Accountability and privacy management programmes

The importance of the principle of accountability (placing the onus of compliance on the data controller) cannot be underestimated as a means to promote and define organisational responsibility for privacy protection.

The revised Privacy Guidelines 2013 introduce the concept of a privacy management programme and articulate its essential elements.[57] The requirement is that these programmes be integrated into the governance structure of a data controller and that there should be appropriate internal oversight mechanisms and provision for audits.[58]

---

54 Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data as adopted July 2013 and contained in The OECD Privacy Framework (2013) 1, available at http://bit.ly/1eFAf3Y, accessed on 30 March 2015).

55 *OECD Privacy Framework* (2013) 3–4.

56 *Idem* 4.

57 Para 15(a)(i) of the revised Privacy Guidelines 2013 specifies that a data controller's privacy management programme should give effect to the Guidelines for all personal data under its control and therefore should not only address the data controllers own operations but also all operations for which it may be accountable.

58 Para 15(a)(iv) specifies that a data controllers privacy management programme should give effect to the Guidelines for all personal data under its control and therefore should not only address the data controller's own operations but also all operations for which it may be accountable. Cf para 15(a)–(b).

2 3 2 2 Data security breach notification

This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data. The new provision that has been added to the Guidelines (paragraph 15(c)) reflects a risk-based approach to notification. Notice to an authority is called for where there is a 'significant security breach affecting personal data', a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well. To determine whether individuals are likely to be adversely affected by a breach, the term 'adverse effect will be interpreted broadly to include factors other than just financial loss.[59]

2 3 2 3 Privacy enforcement authorities and trans-border data-flows

The revised Privacy Guidelines 2013 explicitly make provision for the establishment of DPAs,[60] and they contain three additional principles relating to TBDFs; i.e., that the data controller remains accountable for personal data despite the location of the data;[61] that 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;[62] and restrictions to TBDFs should be proportionate to the risk, taking into account the sensitivity of the data, the purpose and context of processing.[63]

2 4 Directive 95/46/EC

2 4 1 Core principles

Directive 95/46/EC evolved from the original OECD Guidelines, but sought to set a higher level of protection for data subjects.[64] Member states, therefore, were obliged to adopt national legislation that conformed to the standards set out in Directive 95/46/EC.[65] Once this had been achieved, member states were not permitted to restrict TBDFs to other member states for reasons relating to the protection of the rights of an individual. However, member states are required to prohibit TBDFs to non-EU member countries that do not provide an adequate level of data protection. As a result, as with the OECD Guidelines, Directive 95/46/EC also has an influence in respect of the transfer of personal data on non-member states outside the EU.[66]

Directive 95/46/EC additionally contains a set of data-protection principles that require that personal data be processed fairly and lawfully; collected for a specified, explicit and legitimate purpose; that further processing may not be incompatible with the initial purpose for collection; that collection be adequate, relevant and not excessive in relation to the purposes for which it was collected; be accurate and kept up to date; and, therefore, data that is incomplete or

59 *OECD privacy framework* (2013) 27.
60 Para 19(c) revised Privacy Guidelines 2013.
61 Para 16.
62 Para 17.
63 Para 18.
64 Roos 2007 *SALJ* 405.
65 Preamble para 8 and art 32.
66 Art 25.

inaccurate should either be erased or rectified or not kept in a form that allows for the identification of the data subject for a period longer than is necessary.[67]

There are further principles to ensure that the processing of data is legitimate, by providing for, e.g., that personal data may only be processed where the data subject has given consent; it is necessary in terms of a contract or at the request of the data subject prior to such contract; the processing is necessary in order for the data controller to comply with a legal obligation or such processing is necessary to protect the vital interests of the data subject; and so on.[68]

When it comes to the processing of special categories of data, there is a general prohibition on the processing of such data,[69] except where the data subject has given explicit consent for the processing of such data; where the data controller processes such data to carry out its obligations or rights in accordance within the field of employment law; 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; 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 where the processing of such data is necessary for the establishment, exercise or defence of legal claims; or the data is made public by the data subject.[70]

Rights afforded by Directive 95/46/EC include[71] that personal data must be processed according to the data quality principles contained in the Directive;[72] the right to be informed of the identity of the data controller, the purpose for collection as well as any other relevant information;[73] the rights of access to one's own personal data, which includes the right to rectification, erasure 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);[74] the right to object to the processing of personal information 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[75] on compelling legitimate grounds;[76] and for the purposes of direct marketing;[77] 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

67 Art 6(1)(a)–(e).
68 Art 7(a)–(f).
69 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)).
70 Art 8(2).
71 These rights are not absolute and must be enforced by member states. Cf art 13 Directive 95/46/EC.
72 Cf art 6(1) Directive 95/46/EC.
73 Arts 10(1) and 11(1).
74 Art 12.
75 Art 7((e)–(f).
76 Art 14(a).
77 Art 14(b).

relating to the data subject (eg, the data subject's performance at work, creditworthiness, reliability, conduct, etc.);[78] and the right of every person to a judicial remedy for any breach of the rights guaranteed by the national laws enacted by member states.[79]

Member states are required to appoint their own DPAs who have relatively wide powers to monitor the application of the provisions of Directive 95/46/EC.[80]

Pitfalls to Directive 95/46/EC 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 leading to legal uncertainty.[81] The cost of compliance for small and medium-sized bodies may be excessive 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 Directive. As a result, the European Commission 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 EU Regulation),[82] that will "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".[83]

2 4 2 EU Regulation

A press release of the EC states that:[84]

> "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 is yet to be passed into law by the European Parliament, it would seem that progress on EU data protection reform is now irreversible.[85] Material changes or improvement brought about by the EU Regulation insofar as they relate to the core data principles will be mentioned briefly below.

78 Art 15; exceptions to this are listed in art 15(2).

79 Art 22.

80 Art 28.

81 EU Regulation Explanatory Memorandum 2.

82 On 25 January 2012, the European Commission proposed a comprehensive reform of Directive 95/46/EC. 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://bit.ly/1mRrHn6, accessed on 13 February 2014.

83 EU Regulation Explanatory Memorandum 2.

84 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://bit.ly/1cSL4YF, accessed on 22 September 2014.

85 Following a European Parliament vote in favour of the EU Regulation on 12 March 2014. Cf Memo/14/186.

2 4 2 1 Data quality

On the principle relating to data quality, the EU Regulation introduces additional elements in respect of the requirements of transparency,[86] minimality[87] and accountability.[88]

2 4 2 2 Lawful processing

When processing in terms of the lawful processing principle, the EU Regulation clarifies the balance of interest criterion where it is specifically stated 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.[89] The conditions for valid consent,[90] as well as verifiable consent (where consent is given on behalf of a child under 13 years old),[91] as a valid legal ground for lawful processing are likewise amplified in the EU Regulation.

2 4 2 3 Special categories of data

The general prohibition on processing special categories of personal data has been expanded in the EU Regulation. Genetic data, criminal convictions and related security measures have been added to the definition of special categories of data.[92] Exceptions to the general prohibition to the processing of special categories of personal data have also been expanded.[93]

2 4 2 4 Data subject's rights in terms of the EU Regulation

Chapter 3 of the EU Regulation deals with the rights of a data subject. In this chapter, data-controllers are required to have transparent and easily-accessible policies relating to the processing of personal data;[94] 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;[95] and provide procedures and mechanisms to enable data subjects to exercise their rights, including means for electronic requests, responding to a data subject's request within a defined period (generally one month) and the motivations for a refusal to action a request by a data subject.[96]

86 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.
87 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 it is processed and that such purposes could not be fulfilled by processing information that does not contain personal data.
88 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.
89 Exceptions include where processing is carried out by public authorities in the performance of their tasks (art 7).
90 Art 7 EU Regulation.
91 Art 8.
92 Art 9.
93 Art 9(a)–(j).
94 Art 11(1).
95 Art 11(2).
96 Art 12 EU Regulation.

The EU Regulation further builds on Directive 95/46/EC 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, unless this involves disproportionate effort.[97]

2 4 2 5 Information and access to data

The EU Regulation expands on the data subject's right to be informed about his or her personal data that is being processed as well as the data subject's right to access personal information, by providing for additional information that must be provided to the data subject (such as the right to lodge a complaint; storage period of data; etc).[98]

2 4 2 6 Rectification and erasure

A recent decision of the EU Court of Justice[99] based on the current provisions of Directive 95/46/EC, found that a data subject has the 'right to be forgotten' where a data subject's personal information is inaccurate, inadequate, irrelevant or excessive.[100] In line with the court's ruling, 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.[101] 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 any copies of that data.

2 4 2 7 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 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.[102]

2 4 2 8 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 Directive 95/46/EC with some minor additional safeguards.[103]

---

97 Art 13.

98 Art 14–15.

99 C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* [2014] (*Google Spain* case), available at http://bit.ly/1K8Y4Ox, accessed on 11 October 2014.

100 In this case, a Spanish citizen lodged a complaint against a Spanish newspaper with the national Data Protection Agency 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.

101 Arts 16–17 EU Regulation.

102 Art 18.

103 Arts 19–20.

2 4 2 9 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.[104]

2 4 2 10 Restrictions

As with Directive 95/46/EC, the EU Regulation empowers member states to restrict the application of the core data privacy principles,[105] as well as certain data subject rights, when such a restriction constitutes a necessary and proportionate measure in a democratic society.[106]

In light of the discussion above, it is submitted that when finalised, the EU Regulation will be a comprehensive data protection instrument insofar as it relates to the core data privacy principles as well as the rights afforded to data subjects.

3 HOW DOES PPI COMPARE?

3 1 Core conditions

On the whole, it is evident that Directive 95/46/EC and PPI offer better protection than the OECD Guidelines and the CoE Convention.[107]

When it comes to data sensitivity, PPI offers superior protection to data subjects as opposed to the CoE Convention, OECD Guidelines and Directive 95/46/EC.[108] PPI also offers better protection to children as there is a general prohibition against the processing of personal information relating to children, whereas similar provisions are absent in the CoE Convention, OECD Guidelines and Directive 95/46/EC.[109] However, once the EU Regulation becomes operational, it will address both of these limitations.[110] Despite this improvement to Directive 95/46/EC, PPI will still offer children superior protection due to the fact that PPI defines a child as a "… natural person under the age of 18 years",[111] whereas the EU Regulation's prohibition on the processing of personal data of a child only relates to children below the age of 13.[112]

104 Cf art 32.

105 Cf art 5.

106 Art 21 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.

107 At the end of the original LLM study that formed the basis of this article is a detailed comparison between the core data privacy principles contained in PPI, the OECD Guidelines, the CoE Convention and Directive 95/46/EC.

108 PPI includes "biometric information" under special information, whereas Directive 95/46/EC does not make provision for biometric information (s 26 PPI). PPI further contains specific provisions which contain the exclusions for each category of special data, to the general prohibition on the processing special information (s 27–33 PPI), whereas Directive 95/46/EC only sets out general exclusions to the processing of special categories of data (art 8(2)–(7)).

109 S 34 PPI. Exceptions to the general prohibition are contained in s 35 PPI.

110 Art 8 EU Regulation.

111 S 1 PPI.

112 Art 8 EU Regulation.

In respect of the cost of compliance, the EU Regulation has a similar provision to the Modernisation Proposal which allows for member states to take the measures needed 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, thereby allowing for micro, small and medium-sized enterprises to be exempt from certain of the provisions of the EU Regulation.[113] No such provision is contained in PPI. It is further submitted that the Regulator may not decide to exempt micro-, small- and medium-sized enterprises in terms of the provisions of section 37 of PPI, due to the fact that when exercising his or her discretion, the Regulator may only do so on the grounds that it is in the public interest or 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.

3 2 Data subjects' rights

On the whole, the rights of a data subject, as specified in Directive 95/46/EC, are comparable with the data subject's rights specified in section 5 of PPI.[114]

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.[115] The EU Regulation has a similar provision; however, only once it has been determined that the processing operations pose a specific risk.[116] PPI 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, it must be borne in mind that the regulator may *mero motu* (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 recommendations 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, PPI does offer some protection in this regard.

If one has regard to the EU Regulation it would seem as if the EU Regulation offers greater protection than PPI when it comes to the rights of the data subject.

---

113 Eg, art 8 (processing of personal data of a child); art 12 (procedures and mechanisms for exercising the rights of the data subject); art 14 (information to be provided to the data subject); art 22 (the responsibilities of the controller); and art 33 (the data protection impact assessment which is to be conducted by a data controller).

114 Examples include direct marketing (art 14(b) Directive 95/46/EC and s 69 PPI); access to one's own data and rectification (art 12 Directive 95/46/EC and ss 23–24 PPI); automated decision making (art 15 Directive 95/46/EC and s 7 1 PPI).

115 This is not to be confused with the risk assessment contained in s 19(2)(1) PPI, which relates to security measures on integrity and confidentiality of personal information.

116 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".

PPI 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). Although, in instances where the data subject is also a consumer as defined in the CPA, 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, it is submitted that PPI also provides for the "right to be forgotten", although this right is not explicitly specified as provided for in article 17 of the EU Regulation. It must be borne in mind that, in the *Google Spain* case, the EU Court of Justice came to its decision based on the provisions of article 6(1)((c)–(e) and Art 12(b) of the EU Directive.[117] PPI has similar provisions in sections 10, 16 and 24, which are comparable to article 6(1)((c)–(e) and Article 12(b) of Directive 95/46/EC. Therefore, it is 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, which is not provided for in PPI. However, the regulations[118] under the Electronic Communications Act[119] provide for mobile number portability[120] and, as such, the principle of data portability is recognised in the South African legal framework, albeit to a limited extent.

3 3 Data protection by design and by default

The EU Regulation introduces two concepts: that of data privacy by design and data privacy by default.[121] 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 that privacy-friendly default settings should be the norm (e.g. on social networks).[122] The Modernisation Proposal has

117 The *Google Spain* case paras 93–94 states: "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."

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

119 36 of 2005.

120 The definition of personal information in s 1 PPI includes a telephone number.

121 Art 23 EU Regulation.

122 Memo/14/186 4.

a similar provision to the data protection by design principle in article 8*bis*, 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". PPI does not contain any provisions that are similar to the data protection by design and by default principles.

3 4 Trans-border data flows

As with the other international instruments that have been discussed, PPI also contains a general prohibition on the transfers of personal information to countries that do not provide adequate levels of protection.[123] Both PPI and the EU Regulation[124] 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 PPI.

4 CONCLUSION

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

When comparing PPI to the other international instruments discussed in this study, it can comfortably be said that the recommendations of the SALRC Report largely have been achieved and that "… the protection of information privacy in South Africa is in line with international requirements and developments",[125] 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 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.[126] Public consultation on the Modernisation Proposal commenced in 2011.[127] It is remarkable that PPI has set such a high standard by, for example, providing for biometric information as a special data category and allowing additional protections for children where the CoE Convention, OECD Guidelines and EU Directive initially failed to do so.

When one looks at possible improvements to PPI insofar as the rights of data subjects are concerned, the right of data protection by design, the right to data

123 S 72 PPI.

124 Ch V of the EU Regulation deals with transfer of personal data to third countries or international organisations.

125 SALRC Report ix.

126 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://bit.ly/1GwHK39, accessed on 30 November 2014.

127 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://bit.ly/1H9PL2u, accessed on 30 November 2014.

protection by default, as well as the right to portability of data are possible aspects which should be considered for incorporation in any future amendments to PPI. Another improvement to be considered for incorporation in any future amendments to PPI is the cost of compliance by allowing for micro-, small- and medium-sized enterprises to be exempt from certain of the provisions of PPI, which tend to drive up the costs of compliance.

What is strikingly apparent is that at the time of writing this article, the South African legal framework regarding the processing of personal information and the protection of the rights of data subjects in terms of the common law, legislation (that have been discussed herein) and the Constitution, is wholly inadequate. This is despite the fact that section 14 of the Constitution guarantees individuals the right to privacy. Accordingly, until the time that PPI 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 PPI 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 into PPI. One can only hope that the government will prioritise this important piece of legislation that seeks to bring South Africa in line with the international community.