The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'

Anneliese Roos
Professor, Department of Private Law
University of South Africa
roosa1@unisa.ac.za

Abstract

After a lengthy legislative process, South Africa implemented the Protection of Personal Information Act 4 of 2013 (POPI Act) on 1 July 2020. The POPI Act is an omnibus data-protection Act that conforms to the former benchmark for data-protection laws worldwide, namely, the 1995 EU Data Protection Directive. At the time of drafting the proposed Bill that would later become the Act, the South African Law Reform Commission emphasised the importance of a South African data-protection Act that complies with international standards on data protection, especially with the EU's Directive. The Directive, in Article 25, imposed a prohibition on the transfer of personal data to non-member countries that do not ensure an adequate level of protection when personal data of their citizens are processed. South Africa's Act needed to comply with the standard set in the Directive for the protection of personal information if South Africa wanted to remain part of the international information technology market. In 2016, the EU adopted the General Data Protection Regulation (GDPR) that replaced the 1995 Directive with effect from May 2018. The question now arises whether the South African Act still meets the minimum standards for data protection set out by this Regulation and whether amendments to the Act are needed. This article compares certain provisions of the GDPR with similar provisions of the POPI Act in order to establish whether the South African Act meets the standard set in the GDPR.

Keywords: data privacy; data protection; GDPR; POPI Act 4 of 2013; Article 29 Data Protection Working Party; European Data Protection Board

UNISA university of south africa PRESS

Comparative and International Law Journal of Southern Africa
https://upjournals.co.za/index.php/CILSA
Volume 53 | Number 3 | 2020 | #7985 | 37 pages

https://doi.org/10.25159/2522-3062/7985
ISSN 2522-3062 (Online), 0010-4051 (Print)

Introduction

Reason for Adoption of GDPR

On 25 May 2018, the General Data Protection Regulation (GDPR) came into force in the EU.[1] It has been described as 'the most consequential regulatory development in information policy in a generation.'[2] It was adopted in April 2016 after four years of comprehensive deliberations. Enforcement was postponed for two years in order to allow companies to prepare for the implementation of the GDPR. The Regulation replaced the 1995 Data Protection Directive.[3]

The 1995 Data Protection Directive was adopted in order to ensure the free flow of personal data between the member states of the European Community while at the same time ensuring a high level of protection for individuals' right to privacy.[4] Directives are a form of EU legislation used in the harmonisation of public policy throughout the Union.[5] The goals expressed in directives are binding, but member states are granted some leeway in deciding the actual form of implementation and the detailed content of the legislation. In other words, directives have to be transposed into national law by

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (hereafter GDPR).

2 Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Inf & Com Tech L 65, 66.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31 (hereafter Directive 95/46/EC). For a discussion of Directive 95/46/EC, see Anneliese Roos, 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study' (LLD thesis, Unisa 2003) 189 ff; Anneliese Roos, 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 SALJ 400, 406–413; Anneliese Roos, 'Data Privacy Law' in Dana van der Merwe (ed), *Information and Communications Technology Law* (2nd edn, LexisNexis 2016) 382–400.

4 According to the Commission of the EC, 'Directive 95/46 enshrines two of the oldest ambitions of the European integration project: the achievement of an Internal Market (in this case the free movement of personal information) and the protection of fundamental rights and freedoms of individuals. In the Directive, both objectives are equally important.' See Commission of the European Communities, 'First Report on the Implementation of the Data Protection Directive (95/46/EC)' COM (2003) 265 final, 3.

5 There are several types of legislation in the EU: regulations, directives, decisions, recommendations and opinions (see Art 249 of the Consolidated Version of the Treaty establishing the European Community [2002] OJ C325/33). See also Art 288 of the Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1.

means of national legislation. Regulations, on the other hand, have general application and pass into law without further action by the member states.[6]

There were two main reasons why the Data Protection Directive had to be replaced by a regulation on data protection. First, because the Directive had to be transposed into national law by the EU member states by means of national legislation, there was 'legal fragmentation' in the way the different member states implemented it, despite the fact that a minimum level of protection had to be complied with.[7] Since a regulation applies directly in the member states, it would ensure uniform application.[8]

Secondly, owing to globalisation and the rapid development of technology, especially the internet, the Directive no longer provided legal certainty.[9] When the Directive was adopted in 1995, the internet was in its infancy and the drafters of the Directive could not foresee the influence that it, combined with other new technologies, would have on the processing of personal information.[10] As a result, there was 'legal uncertainty and a widespread public perception that there are significant risks associated notably with

6 See further Roos, 'Data (Privacy) Protection' (n 3) 192 fn 211 and the authority referred to there. See also Francoise Gilbert, 'Proposed EU Data Protection Regulation: The Good, the Bad and the Unknown' (2012) 15(10) Journal of Internet Law 1, 22–23.

7 See European Commission, '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) Explanatory Memorandum to the Reform Package' COM(2012) 11 final (European Commission Explanatory Memorandum) 2; Peter Hustinx, 'The Reform of EU Data Protection Law: Towards More Effective and More Consistent Data Protection Across the EU' in Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick, *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014) 64; W Gregory Voss, 'Looking at European Union Data Protection Law Reform through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later' (2014) 17 (9) Journal of Internet Law 1, 3; Anne-Marie Zell, 'Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field' (2014) 15 German LJ 461, 463.

8 According to the Explanatory Memorandum to the Reform Package, '[a] Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU [Treaty on the Functioning of the EU] will reduce legal fragmentation and provide greater legal certainty by introducing a harmonised set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.' See European Commission Explanatory Memorandum (n 7) 5.

9 See European Commission Explanatory Memorandum (n 7) 2.

10 European Commission Explanatory Memorandum (n 7) 3; Viviane Reding, 'The Upcoming Data Protection Reform for the European Union' (2011) 1 International Data Privacy Law (IDPL) 3; Voss (n 7) 13; Zell (n 7) 464.

online activity.'[11] These developments required 'a strong and more coherent data protection framework in the Union, backed by strong enforcement.'[12]

Reason why GDPR affects South Africa

After a lengthy legislative process,[13] South Africa's Protection of Personal Information Act 4 of 2013 (POPI Act) came into force on 1 July 2020.[14] The POPI Act is an omnibus data-protection Act that conforms with the former benchmark for data-protection laws worldwide, namely the 1995 EU Data Protection Directive. When the South African Law Reform Commission brought out its report on data-protection legislation for South Africa, it recommended that South Africa should adopt legislation that met the international standards for data protection.[15] At that stage, the 1995 EU Directive was the gold standard for data protection.[16] As a result, the drafters of the POPI Act followed the Directive closely. Countries outside the EU (third countries) were also affected by the Directive because Article 25 required third countries to provide adequate data protection before personal data might be sent from EU countries to third countries.[17] This meant that countries which wanted to form part of the information market had to adopt measures to comply with the standard of protection provided for personal information in Europe.[18]

---

11 See European Commission Explanatory Memorandum (n 7) 2. Also see Waltraut Kotschy, 'The Proposal for a New General Data Protection Regulation – Problems Solved?' (2014) 4 IDPL 274.

12 See European Commission Explanatory Memorandum (n 7) 2.

13 For a brief discussion of the legislative history of the POPI Act, see Roos, 'Data Privacy Law' (n 3) 434.

14 A Regulator was established in 2016 (see https://www.justice.gov.za/inforeg/) and regulations were drafted in 2018. See GG 42110, RG 10897 (14 December 2018) GN 1383. On 22 June 2020, it was announced that most of the provisions of the POPI Act will commence on 1 July 2020. See Proclamation No R 21 of 2020 in Gazette 11136, Vol 660 No 43461. Sections 110 (amendment of other laws by the POPI Act) and 114(4) (finalisation of the Human Rights Commission's functions in terms of the Promotion of Access to Information Act 2 of 2000) will come into force on 30 June 2021.

15 South African Law Reform Commission, *Privacy and Data Protection: Project 124* (SALRC 2009) para 3.2.7.

16 See Lee A Bygrave, *Data Privacy Law: An International Perspective* (OUP, 2014) 53ff; Paul de Hert and Vagelis Papakonstantinou, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 Comp L & Sec Rev 130, 131.

17 See Roos, 'Data (Privacy) Protection' (n 3) 226–235 for a discussion of Art 25 of Directive 95/46/EC. Also see Douwe Korff, *Data Protection Laws in the European Union* (Federation of European Direct Marketing 2005) 171ff; Roos, SALJ (n 3) 411ff; Anneliese Roos, 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 4 PELJ 62, 63ff.

18 Paul M Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 Iowa LR 471, 487. The author pointed out, this provision obliged member states to cut

The GDPR has a similar requirement to that of the Directive and, as a result, third countries have to ensure that they provide a level of data protection that meets the GDPR standard. According to Article 44 of the GDPR, a transfer of personal data to a third country,[19] if the data is to undergo processing after the transfer, may take place only if the controller and processor comply with the conditions for processing laid down in the Regulation. These include the conditions for onward transfer of the personal data from the third country to another third country. Any transfer to a third country may be carried out only in full compliance with the Regulation.[20] According to the Regulation, personal data may be transferred to a third country on the basis of an adequacy decision,[21] or subject to appropriate safeguards,[22] which may include binding corporate rules.[23] Irrespective of the basis on which the transfer takes place, the crux of the matter is that the personal data must enjoy adequate protection in the third country.

In the case of an adequacy decision,[24] the Commission of the EU has to decide whether a third country (or a territory or a specific sector in that third country) is ensuring adequate protection.[25] If such a finding has been made, the transfer does not require any further authorisation and data may flow freely.[26] In assessing the adequacy of the protection provided by a third country, the Commission must take certain elements into account, such as the rule of law, respect for human rights and fundamental freedoms, relevant legislation, the existence and effective functioning of one or more independent supervisory authorities and the international commitments the third country or international organisation has entered into. [27]

---

off the flow of personal information to a third country that did not comply with the required standard. See also Roos, SALJ (n 3) 412.

19 Whereas Directive 95/46/EC (n 3) provided only for transfers to third countries, the GDPR (n 1) also provides for transfers to international organisations (see Art 44).

20 This means that the third country must also prohibit the further transfer of the personal data from that country to another third country which does not provide adequate data protection.

21 GDPR (n 1) Art 45.

22 GDPR (n 1) Art 46.

23 GDPR (n 1) Art 47.

24 Adequacy decisions are made in the form of an implementing act—see GDPR (n 1) Art 45(3).

25 GDPR (n 1) Art 45(3): 'The purpose of adequacy decisions by the European Commission is to formally confirm with binding effects on Member States … that the level of data protection in a third country or an international organization is essentially equivalent to the level of data protection in the European Union.' See Art 29 Data Protection Working Party, *Adequacy Referential (Updated)* WP254 28 Nov 2017.

26 Peter Blume, 'EU Adequacy Decisions: The Proposed New Possibilities' (2015) 5 IDPL 34. The Commission must monitor developments in the country that could affect the functioning of an adequacy decision—GDPR (n 1) Art 45(4). If the country no longer assures an adequate level of protection, the Commission may repeal, amend or suspend such a decision—GDPR (n 1) Art 45(5).

27 GDPR (n 1) Art 45(2).

In the absence of an adequacy decision, the transfer of personal data may also take place if the data controller or processor has provided appropriate safeguards and enforceable data subject rights. Effective legal remedies must also be available to data subjects.[28] The safeguards may be provided by legally binding and enforceable instruments between public authorities or bodies,[29] binding corporate rules,[30] standard data-protection clauses approved by the Commission,[31] an approved code of conduct,[32] or an approved certification mechanism.[33]

Scope of Article

The aim of this article is to analyse selected provisions of the Regulation and to compare them with comparable provisions of the POPI Act.[34] This with a view to establishing whether the changes in the EU position will require amendments to the POPI Act so that it meets the minimum standards for data protection set by the EU Regulation. If the Act meets the standards set, the Commission may be approached for a declaration of adequacy. If the Commission makes such a finding, subsequent transfers of personal data from the EU to South Africa are possible without having to employ appropriate safeguards or binding corporate rules.

It is impossible to provide a meaningful discussion of all the provisions of the Regulation and the POPI Act in the limited space of one article.[35] In this article only

---

28 GDPR (n 1) Art 46(1).

29 GDPR (n 1) Art 46(2)*(a)*. An example of this was the Privacy Shield agreement between the EU and the USA. The Privacy Shield replaced the Safe Harbor Agreement after its invalidation by the *Schrems* decision (see *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, 6 October 2015; this case is discussed below in notes 38 and 40). It was adopted on 27 April 2016 and became operational on 1 August 2016. See European Commission, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–US Privacy Shield, C (2016) 4176 final (12 July 2016). However, on 16 July 2020, the CJEU in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* Case C-311/18 (*Schrems II* case) invalidated the Privacy Shield Decision, because the US law assessed by the court does not provide an essentially equivalent level of protection to the EU.

30 In terms of Art 47, a competent supervisory authority may approve binding corporate rules if they are legally binding and apply to an entire group of undertakings, or give the data subject enforceable rights and specify certain prescribed minimum details.

31 GDPR (n 1) Art 46(2)*(c)* and *(d)*.

32 GDPR (n 1) Art 46(2)*(e)*. Also see Art 40.

33 GDPR (n 1) Art 46(2)*(f)*. Also see Art 42.

34 Act 4 of 2013. For a detailed discussion of the POPI Act, see Anneliese Roos, 'Legal Protection of Personal Information' in J Neethling, JM Potgieter and A Roos, *Neethling on Personality Rights* (LexisNexis 2019); Roos, 'Data Privacy Law' (n 3) 434–478; Yvonne Burns and Ahmore Burger-Smidt, *A Commentary on the Protection of Personal Information Act* (LexisNexis 2018).

35 Both the GDPR (n 1) and the POPI Act (n 34) are enormous legislative documents. The GDPR has 99 Articles and the POPI Act 115 sections.

selected provisions are discussed. Since the aim of the article is to determine whether the POPI Act provides 'adequate' data protection, the focus of the discussion will be on some of the provisions that are considered essential to attaining adequacy. In this sense the discussions rely on the guidance provided by the EU's Article 29 Data Protection Working Party[36] on the meaning of 'adequate' data protection.[37] According to the Working Party, a third country's legal framework must contain certain 'core data protection principles' in order to ensure 'essential equivalence' with the EU data-protection framework.[38] Furthermore, 'any meaningful analysis of adequate protection must comprise two basic elements: the content of the rules applicable and the means for ensuring their effective application.'[39] The country must also have essential guarantees for law enforcement and national security access to limit interference with fundamental rights.[40]

---

36 The Working Party was established under Article 29 of the Data Protection Directive 95/46/EC (n 3) and is therefore referred to as the Article 29 Data Protection Working Party. The Article 29 Data Protection Working Party was replaced by the European Data Protection Board (EDPB) as from 25 May 2018. According to its website, '[t]he European Data Protection Board (EDPB) is an independent European body which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities.' See <https://edpb.europa.eu/about-edpb/about-edpb_en>. The EDPB has to provide the Commission with an opinion on the assessment of the adequacy of the level of protection in a third country (GDPR (n 1) Art 70(1)*(s)*).

37 Article 29 Data Protection Working Party (n 25). This document is an updated version of a previous document issued by Article 29 of the Data Protection Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* WP12 (24 July 1998)) and reflects the position under the GDPR.

38 Article 29 Data Protection Working Party (n 25) 3. The CJEU held in the *Schrems* case that the level of protection in the third country need not be identical, but must be 'essentially equivalent'. This means the manner in which the level of protection is accomplished may be different from the means used in the EU. (See *Maximillian Schrems v Data Protection Commissioner* (n 29) para 73). In the *Schrems* case the EUCJ invalidated the decision of the EU declaring that the Safe Harbor agreement provides adequate protection for the transfer of personal data from the EU to the USA. See Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 *OJ* (L 215). For a discussion of the *Schrems* case, see Christopher Kuner, 'Reality and Illusion in EU Data Transfer Regulation Post *Schrems*' (2017) 18 German LJ 881.

39 Article 29 Data Protection Working Party (n 25) 3. These requirements can be traced to the Charter of Fundamental Rights of the European Union [2012] OJ C326, the GDPR (n 1) and other international agreements on data protection, such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS 108 (usually referred to as Convention 108) (see Article 29 Data Protection Working Party (n 25) 3).

40 Article 29 Data Protection Working Party (n 25) 7. The *Schrems* decision (n 29) declared the Safe Harbor Agreement invalid in part because US public authorities were not themselves subject to it and the national-security, public-interest and law-enforcement requirements of the US prevailed

In evaluating whether the POPI Act meets the standard set by the GDPR, it is essential to compare the content of certain provisions, and the rules for enforcing the provisions. Following the example of the Article 29 Data Protection Working Party's guidance document, the provisions dealing with the definitions of certain concepts, the legal bases for lawful data processing, the data-protection principles, the data subject rights, restrictions on onward transfers and the enforcement mechanisms in the Act should be compared.[41] However, owing to the aforementioned limitation for this article, the discussion is confined to the so-called content principles as they relate to the content of concepts and the legal bases for lawful processing. The data-protection principles, data subject rights, restrictions on onward transfer and the procedural and enforcement mechanisms will not be dealt with in this article.[42]

Concepts

A requirement for a finding of adequate data protection is that certain basic data-protection concepts and principles, such as 'personal data', 'processing of personal data', 'data controller', 'data processor', 'recipient' and 'sensitive data' should exist in the third country's legal system. These concepts do not have to mirror the European data-protection law, but must be consistent with it.[43] The meaning of these concepts in the GDPR and the POPI Act will therefore be compared.

Personal Data/Information[44]

The GDPR defines personal data as information that relates to a natural person who is identified or can be identified (either directly or indirectly).[45] The definition also gives examples of information that can serve as an identifier, namely, a name, an identification number, location data or an online identifier. A person can also be identified by one or more factors 'specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'[46]

---

over the Safe Harbor scheme—the scheme therefore enabled interference, by US public authorities, with the fundamental rights of persons (see Roos, 'Data Privacy Law' (n 3) 409).

41 Article 29 Data Protection Working Party (n 25).

42 The essential guarantees for law-enforcement and national-security access to limit interference with fundamental rights will have to be found in other legislation (not in the POPI Act). Therefore they do not form part of the discussion of the POPI Act.

43 Article 29 Data Protection Working Party (n 25) 5.

44 The GDPR uses the term 'data' whereas POPI uses 'information'. In the present context, the two terms can be used interchangeably. See Roos, 'Data (Privacy) Protection' (n 3) 18.

45 The regulation does not apply to the personal data of deceased persons. See GDPR (n 1) recital 27.

46 GDPR (n 1) Art 4(1) provides:
'"personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly,

The POPI Act defines personal information as information that relates to an identifiable, living person.[47] The POPI Act applies not only to natural persons but also to juristic persons 'where it is applicable'.[48] The Act gives a long list of examples of personal information. The list is not closed, and other information may be regarded as personal information if it relates to a person who is identifiable from that information. The list includes information that can be considered specific to the 'physical, physiological, genetic, mental, economic, cultural or social identity' of that person, as mentioned in the GDPR.[49]

It is opined that, the definition of personal information in POPI is adequate. The fact that South African law recognises that juristic persons may in certain circumstances be entitled to personality rights—specifically the right to a good name and privacy[50]—explains why juristic persons are included in the definition in POPI. It does not,

---

in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' The CJEU has considered the meaning of 'personal data' in several cases. For a list of which data have been considered to be personal data, see Denis Kelleher and Karen Murray, *EU Data Protection Law* (Bloomsbury Professional 2018) 82–88.

47 As with the GDPR, the POPI Act excludes deceased persons.

48 In terms of s 8(4) of the South African Constitution, 1996, juristic persons are also entitled to fundamental rights 'to the extent required by the nature of the rights and the nature of that juristic person.' The South African courts apply the common-law principles developed for the protection of the privacy of natural persons also to juristic persons (see, among other cases, *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 (2) SA 451 (A); *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) (Ltd) v Smit NO* 2001 (1) SA 545 (CC)).

49 POPI Act 4 of 2013 s 1. Also see GDPR (n 46). The list includes:

(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.

50 See J Neethling, J Potgieter and JC Knobel, *Neethling-Potgieter-Visser Law of Delict* (7th edn, LexisNexis 2014) 342–345; SALRC (n 15) 72.

however, detract from the minimum standard set by the GDPR. In fact, its scope is wider than that of the GDPR.

Processing

Processing is defined in the GDPR as the operation (or set of operations) performed on personal data (or sets of personal data). This could be, but is not necessarily, by automatic means. It includes 'the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' of data.[51]

POPI has a very similar provision. Processing means any operation (or set of operations) but also any activity concerning personal information. It may also be done by automated or non-automated means.[52] It includes: '*(a)* the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; *(b)* dissemination by means of transmission, distribution or making available in any other form; or *(c)* merging, linking, as well as restriction, degradation, erasure or destruction of information.'[53]

The POPI Act's definition is certainly more than adequate. It appears to be even wider than that of the GDPR, since it includes not only operations performed on data, but also any activity concerning data. However, 'any activity concerning personal information' and 'any operation performed on personal information' arguably amounts to the same thing. The bottom line is that both the POPI Act and the GDPR define processing in broad terms and processing essentially includes anything that can be done with personal information.[54]

Data Controller, Data Processor, and Recipient

The GDPR defines a controller as a natural or legal (ie juristic) person, public authority, agency or other body which has a certain function, namely to determine both the purposes and the means of processing personal data. The controller may do the determination alone or in conjunction with someone else.[55] A processor, on the other hand, is the person (who could again be a natural or a legal person), public authority,

---

51 GDPR (n 1) Art 4(2). For examples of actions that were considered to be the processing of personal data in the European Union, see Burns and Burger-Smidt (n 34) 26.

52 If processing is done manually, the recorded personal information must form part of a filing system or be intended to form part of it before the Act will be applicable to such processing. See POPI Act s 3(1) *(a)*; see further Roos (n 34) 375.

53 POPI Act 4 of 2013 s 1.

54 See Roos, 'Data (Privacy) Protection' (n 3) 198; Kelleher and Murray (n 46) 94.

55 GDPR (n 1) Art 4(7).

agency or other body which does the actual processing of the personal data on behalf of the controller.[56] The processor serves the interests of the controller in carrying out a specific task and must follow the instructions of the controller.[57]

A recipient is defined by the GDPR as a person (natural or legal person), public authority, agency or another body to whom or which the personal data are disclosed. A recipient may or may not be a third party.[58] A third party is a person who processes personal data under the direct authority of the processor.[59]

In the POPI Act, a data controller is called a 'responsible party'[60] and a processor the 'operator'. Both of these concepts are defined in the Act. Although the Act also refers to third parties and recipients, these two terms are not explicitly defined.

The POPI Act defines a responsible party in almost exactly the same terms as those in which a controller is defined in the GDPR.[61] The definition of an operator in POPI is also similar to that of a processor in the GDPR. However, the POPI definition stipulates that the processing must be done in terms of a mandate or other contract with the responsible party, without the operator coming under the direct authority of the responsible party. As previously mentioned, the concepts of recipient and third party are not explicitly defined, but they are used in the Act. In the context of the Act, a third party appears to be someone to whom the personal information is supplied (in other words, very similar to a recipient). For example, in the section that concerns the transfer of personal information outside the Republic, the Act refers to 'the third party who is the recipient of the information.'[62] In other sections, however, a distinction is drawn between the two concepts. In the section referred to above, the Act later refers to 'the transfer of personal information from the recipient to third parties who are in a foreign country.'[63]

In summary, a 'responsible party' (ie a data controller) and an 'operator' (ie a data processor) are clearly defined in the POPI Act, despite the fact that the Act uses different terminology from the GDPR. Although the POPI Act does not clearly define the terms third party or recipient, it does use these two terms in the Act and, despite the somewhat

56 GDPR (n 1) Art 4(8).

57 European Data Protection Supervisor, *Guidelines on the Concepts of Controller, Processor and Joint Controllership under Regulation (EU) 2018/1725* (7 November 2018) 16.

58 GDPR (n 1) Art 4(9).

59 GDPR (n 1) Art 4(10).

60 The term 'responsible party' was borrowed from the Dutch Personal Data Protection Act of 2000 (Wet Bescherming Persoonsgegevens). See Roos, 'Data (Privacy) Protection' (n 3) 403.

61 POPI Act 4 of 2013 s 1.

62 POPI Act 4 of 2013 s 72(1)*(a)*.

63 POPI Act 4 of 2013 s 72(1)*(a)*(ii).

confusing use of the terms, it is evident that their meaning is fairly similar to the meaning ascribed to them in the GDPR.

Special categories of personal data/information

The GDPR prohibits the processing of 'special categories of personal data', namely data that reveal 'racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.' Such data include 'genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'[64]

The POPI Act, in similar vein, prohibits the processing of 'special personal information'. Special personal information is personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life of a data subject or biometric information on a data subject. It includes information concerning the criminal behaviour of a data subject to the extent that it relates to the alleged commission of any offence, or any proceedings in respect of an alleged offence committed by a data subject or the disposal of such proceedings.[65]

The categories of special personal data/information in the GDPR and in the POPI Act are similar, except that the POPI Act includes personal information relating to criminal behaviour or criminal proceedings as a special category of personal information. Although the GDPR does not include criminal data under special categories of data, it has separate provisions containing safeguards for the processing of personal data relating to criminal convictions and offences.[66] It is submitted that the meaning of special personal information in the POPI Act is similar to that of special categories of personal data in the GDPR.

Conclusion

Based on the above analysis the provisions of the POPI Act are essentially equivalent to those in the GDPR.[67]

---

64 GDPR (n 1) Art 9(1). Particular categories of personal information are treated as 'sensitive' information because it is assumed that the misuse of these types of information could have more severe consequences for a data subject's fundamental rights. See Anneliese Roos, 'Core Principles of Data Protection Law' (2006) 39 CILSA 102, 121 and GDPR (n 1) recital (51).

65 POPI Act 4 of 2013 s 26.

66 GDPR (n 1) Art 10.

67 As required by the *Schrems* decision (n 29).

Next, the grounds for the lawful processing of personal data or information are compared.

Grounds for Lawful and Fair Processing

GDPR

It is a basic requirement of an adequate data protection regime that data must be processed in a 'lawful, fair and legitimate manner'. The legitimate grounds (or 'legitimate bases') on which personal data may be lawfully, fairly and legitimately processed should be set out clearly.[68]

The GDPR requires that all personal data should be processed fairly and lawfully and in a transparent manner.[69] Processing is lawful only if at least one of six possible grounds for processing is applicable.[70] These grounds fall into two broad categories: the consent of the data subject or the necessity to process personal information to accomplish certain objectives. In other words, personal data may be processed if the data subject has *consented* to it and/or if it is *necessary* to process personal data for specific purposes. These purposes are:

- performance in terms of a contract to which the data subject is a party or taking steps at the request of the data subject before entering into the contract;
- compliance with a legal obligation;
- protection of a *vital* interest of the data subject or another natural person;
- performance of a task in the public interest or in the exercise of official authority; and
- pursuant to the legitimate interests of the controller or a third party, provided that these interests are not overridden by the fundamental rights and freedoms of the data subject, especially if the data subject is a child.

Public authorities cannot rely on the ground that processing of personal information is in their interests—they must have another legal basis provided by the legislator for

---

68 According to the Article 29 Data Protection Working Party (n 25) 5, the principle of fair and lawful processing underlies all the other principles: 'if all the other data processing principles are applied, the result will be that processing is done fairly and lawfully.' Also see Roos (n 64) 108.

69 GDPR (n 1) Art 5(1)*(a)*. The GDPR groups this provision under the data processing principles.

70 GDPR (n 1) Art 6(1). Processing may have more than one lawful basis—see Kelleher and Murray (n 46) 153.

processing personal information.[71] Where processing is based on the ground that it is necessary for compliance with a legal obligation,[72] or to perform a task in the public interest or in the exercise of official authority vested in the controller,[73] member states are given leeway to introduce more specific requirements for the processing.[74]

Consent as a basis for processing is carefully described. The GDPR defines consent as

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[75]

In analysing the definition, certain key aspects should be emphasised. First of all, consent must be freely given. Consent is not freely given if the data subject has no choice but to consent or if it would be detrimental for the data subject to refuse consent.[76] Consent is not freely given either if the performance of a contract or the provision of a service is made conditional on the data subject's consent to the processing of personal data where this is not necessary for the performance of the contract.[77]

Another requirement is that the consent must be informed. The information that the data subject must be made aware of for their consent to be informed is the identity of the controller, the purposes of the processing, the type of data that will be collected, the existence of the right to withdraw consent, information about the use of the data for automated decision-making (if relevant) and the possible risks of data transfers due to the absence of an adequacy decision and of appropriate safeguards.[78]

Furthermore, the consent must be unambiguous and the data controller must be able to show that the data subject has consented.[79] When the consent is given in the context of a written declaration concerning another matter, the data subject must be made aware of the fact that consent is being given for the processing of personal data, by clearly distinguishing the consent for processing personal data from the other matters. The request for consent must be in an intelligible and easily accessible form and should be in clear and plain language. The declaration itself must not infringe the provisions of the GDPR. Any part of such declaration which constitutes an infringement will not be

71 GDPR (n 1) Art 6(1)*(a)–(f)*.
72 GDPR (n 1) Art 6(1)*(c)*.
73 GDPR (n 1) Art 6(1)*(e)*.
74 GDPR (n 1) Art 6(2); also see Art 6(3).
75 GDPR (n 1) Art 4(11).
76 GDPR (n 1) recital (42).
77 GDPR (n 1) Art 7(4).
78 GDPR (n 1) recital (42); Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* WP259 rev.01 (10 April 2018) 13.
79 GDPR (n 1) Art 7(1).

binding.[80] The consent must be given 'by a statement or by a clear affirmative action, [by which he or she] signifies agreement to the processing of personal data relating to him or her.'[81] In other words, the data subject must have taken deliberate action signifying their consent to the processing.[82]

The consent must also be specific; in other words, it must be obvious that the data subject has consented to the specific type of processing. A blanket acceptance of general terms and conditions is not considered to be valid consent to the processing of personal data. The use of pre-ticked opt-in boxes is therefore invalid under the GDPR.[83]

Consent may be withdrawn at any time. Processing that took place before consent was withdrawn will remain valid. It must be as easy to withdraw consent as it was to give it.[84]

The controller must decide in advance, before the processing takes place, on which lawful basis the processing will take place. The data subject must be notified of any change in the lawful basis for processing.[85]

POPI Act

Next, the grounds for lawful processing in the POPI Act are considered. The POPI Act requires that personal information should be processed lawfully and in a reasonable

80 GDPR (n 1) Art 7(2).

81 GDPR (n 1) Art 4(11).

82 Article 29 Data Protection Working Party, WP259 rev.01 (n 78) 14–15.

83 Article 29 Data Protection Working Party, WP259 rev.01 (n 78) 16. The GDPR states in recital 32:
'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.'

84 GDPR (n 1) Art 7(3).

85 This is in accordance with the information requirements of Arts 13 and 14 and the general principle of transparency. See Article 29 Data Protection Working Party (n 78) 23.

manner that does not infringe the privacy of the data subject.[86] It lists six grounds on which processing may be done lawfully, namely if:

- the data subject has consented;
- the processing of personal information is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
- processing complies with an obligation imposed by law on the responsible party;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public-law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.[87]

The POPI Act also describes consent in more detail, although not in as much detail as the GDPR. It defines 'consent' as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.'[88] The Act does not stipulate what information the data subject must be made aware of in order for the consent to be considered to be informed, at a minimum, the data subject must be made aware of the identity of the responsible party, which third parties will have access to the personal information, what information will be processed, the purpose of the processing and the rights to which the data subject is entitled.[89]

---

86 POPI Act 4 of 2013 s 9.

87 POPI Act 4 of 2013 s 11. The lawful bases for processing are listed under the second condition for processing, namely, processing limitation. The subhead is 'Consent, justification and objection'. It is a pity that these bases are not clearly indicated as grounds for lawful processing, as was done in the GDPR in Art 6 under 'Lawfulness of processing'.

88 POPI Act 4 of 2013 s 1.

89 See also POPI Act 4 of 2013 s 18, which lists the information that a data controller must supply to a data subject when their personal information is collected in order to meet the openness requirement of the POPI Act. This list of information also informs our understanding of the information that is needed to ensure that consent is 'informed'. This includes the information that is collected and its source, the contact details of the responsible party, the purpose for which the collection takes place, whether or not the supply of the information by the data subject is voluntary or mandatory; the consequences of failure to provide the information; any particular law authorising or requiring the collection of the information; the fact that the responsible party intends to transfer the information to a third country and the level of protection afforded to the information by that third country, and any further information which is necessary, having regard to the specific circumstances, to ensure that the processing in respect of the data subject is

The POPI Act places the burden of proof that the data subject has consented on the responsible party.[90] It also provides that consent may be withdrawn at any time. Such withdrawal will not affect the lawfulness of the processing of personal information before such withdrawal.[91]

In the POPI Act the age of consent is 18 years. In the case of a child under the age of 18, the person who is legally competent to consent to any action or decision being taken in respect of any matter concerning the child (referred to as the 'competent person') must consent on behalf of the child.[92]

Comparison

When comparing the grounds for lawful processing under the GDPR and the POPI Act, it becomes clear that the POPI Act deals with most of the important aspects. Processing must be done lawfully and must be based on a legitimate ground. Although the GDPR requires the processing to be done 'lawfully, fairly and legitimately' and the POPI Act states that it should be done 'lawfully and in a reasonable manner', the end result is the same when considering the context of data privacy (or data protection) laws.[93]

Considering the specific grounds on which processing is allowed, certain differences become apparent. Both the POPI Act and the GDPR list six grounds for the lawful processing of personal information that is not considered to be special personal information. In the main, these grounds are similar. However, on closer inspection, there are a few subtle differences that influence the level of protection provided to data subjects in certain circumstances.

Consent is a valid ground for processing in both legislative instruments. However, the GDPR spells out the requirements for valid consent in more detail and these requirements are arguably at a higher level than those of the POPI Act. In both the GDPR and the POPI Act, consent must be voluntary or freely given, specific and

reasonable. Such further information includes the recipients; the nature of the information; the existence of the right of access to and the right to rectify the information collected; the existence of the right to object to the processing of personal information; and the right to lodge a complaint to the Information Regulator. Also see Burns and Burger-Smidt (n 34) 52.

90 POPI Act 4 of 2013 s 11(2)*(a)*.

91 POPI Act 4 of 2013 s 11(2)*(b)*.

92 POPI Act 4 of 2013 s 11(1)*(a)* read with s 1.

93 See Roos, 'Data (Privacy) Protection' (n 3) 483.

informed. However, the GDPR also requires consent to be given 'by a clear affirmative action'.[94] This element is absent from the definition in the POPI Act.[95]

Another difference is that the GDPR requires that processing must be *necessary* to comply with a legal obligation, to protect vital interests, to perform public tasks or exercise official authority, and to pursue the legitimate interests of the controller or a third party.[96] The POPI Act does not always require the processing to be *necessary* for a specific purpose.[97] Processing that complies with an obligation imposed by law on the responsible party or processing that protects a legitimate interest of the data subject need not be necessary to fulfil that purpose. This might be considered a flaw, because the requirement that the processing must be necessary introduces a higher level of protection of the interests of the data subject.

Both the GDPR and the POPI Act allow personal information to be processed in order to protect an interest of the data subject, but the GDPR requires that the interest that is to be protected must be *vital*, whereas the POPI Act requires that it must only be a *legitimate* interest. This is another important distinction between the GDPR and the POPI Act. A vital interest implies a higher level of protection before the processing of personal information is allowed on this basis. An interest is vital if 'it is essential for the life of the data subject or that of another person.'[98] The POPI Act does not spell out when an interest would be considered legitimate, but presumably it would have to be an interest that legally justifies protection.

It is submitted that the POPI Act should be amended to include the stricter requirements set out by the GDPR in order to ensure an adequacy finding. Alternatively, the South African courts could play a role when interpreting these provisions by requiring that the data subject's consent should be clearly indicated and by requiring that the interest that is protected by the processing should be a 'vital' interest. Although it would be prudent to amend the POPI Act, the differences pointed out are not so significant that one cannot state that the POPI Act is 'essentially equivalent' to the GDPR in this respect.

94 GDPR (n 1) Art 4(11).

95 Burns and Burger-Smidt (n 34) 52 are of the view that 'since the requirement of consent is essential, it should ideally be explicit.'

96 GDPR (n 1) Art 6(1)*(b)–(f)*.

97 See eg POPI Act s 11(1)*(c)* and *(d)*.

98 According to the GDPR, this basis for lawfully processing personal information should be used only where the processing cannot have another legal basis. See GDPR (n 1) recital (46).

Grounds for Lawful Processing of Special Categories of Data

GDPR

The GDPR prohibits the processing of special categories of personal data,[99] unless a specific basis exists that allows such processing.[100] It is important to recognise that in addition to the specific requirements for such processing, the general principles and other rules of the GDPR still apply—for example, the conditions for lawful processing.[101]

In general, all special categories of data may be processed if the data subject has given their consent; but in this instance the consent must be 'explicit'. [102] This refers to the way the consent is expressed—for example, by means of a written agreement, filling out an electronic form or sending an email.[103] Member states may provide in their laws that the data subject may not consent to a particular form of processing. [104]

Such processing may also take place if the processing is necessary to protect the vital interests of the data subject, or of another natural person in a situation where the data subject is physically or legally incapable of giving consent.[105]

If a data subject has made personal data that belong to a special category 'manifestly public', then such data may be processed.[106] In other words, if sensitive personal data relating to the data subject become manifest from the data subject's conduct.[107]

---

99 For the definition of special categories of data, see the text to (n 64) above.

100 GDPR (n 1) recital (51) states that:
'[p]ersonal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. … Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation … Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.'

101 GDPR (n 1) recital 51.

102 GDPR (n 1) Art 9(2)*(a).*

103 See Article 29 Data Protection Working Party (n 78) 18.

104 GDPR (n 1) Art 9(2)*(a).*

105 GDPR (n 1) Art 9(2)*(c).* For example, the data subject is unconscious after an accident and cannot consent to someone accessing their medical records.

106 GDPR (n 1) Art 9(2)*(e).*

107 An example would be if persons made their preference for a political party known in a newspaper or published information about their health.

Special categories of personal data may, furthermore, be processed if processing is necessary for establishing, exercising or defending legal claims or whenever courts are acting in their judicial capacity.[108]

Such processing is also allowed if it is in the public interest. The public interest must be 'substantial'[109] and the processing must then take place on the basis of a law which must be proportionate to the aim pursued,[110] respect the essence of the right to data protection[111] and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[112]

Derogations to the prohibition on the processing of special categories of data are also allowed in the fields of employment and medicine, or by non-profit bodies.[113] For example, processing is allowed if its place to carry out the obligations of a data controller or to exercise the rights of the data subject in the field of employment[114] and social security and social protection law. In these situations, the processing must be authorised by a law or a collective agreement and appropriate safeguards must be in place to protect the fundamental rights and the interests of the data subject.[115]

A foundation, association or another not-for-profit body with a political, philosophical, religious or trade union aim may also process special personal data relating to its members or former members or persons who have regular contact with it in connection

---

108 GDPR (n 1) Art 9(2)*(f)*.

109 The UK Data Protection Act 2018 Schedule 1 para 6-28 identifies public interests that are substantial. These include statutory and government purposes; administration of justice and parliamentary purposes; equality of opportunity or treatment; preventing or detecting unlawful acts; journalism, academia, art and literature; and preventing fraud.

110 In other words, the law must not go further than is necessary to achieve the aim pursued.

111 What is the essence of the right to data protection? According to Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88, 97: 'In essence, the "hard core" of data protection would be what needs to be protected, so that the final values that data protection pursues such as individual autonomy, dignity, and personal identity are safeguarded.' See further Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-terrorism Surveillance* (Hart 2017) 43. Also see Maria Grazia Porcedda, 'On Boundaries – Finding the Essence of the Right to the Protection of Personal Data' in Ronald Leenes, Rosamunde Van Brakel, Serge Gutwirth and Paul de Hert (eds), *Data Protection and Privacy: The Internet of Bodies* (Hart 2018) 277f. Tzanou identifies the following attributes of the right to personal data protection: legitimate processing, oversight, supervisory authority, human intervention, data subject rights, security and minimisation.

112 GDPR (n 1) Art 9(2)*(g)*.

113 GDPR art 9(2)*(b)*, *(d)*, *(h)* and *(i)*.

114 Also see GDPR (n 1) Art 88, which provides that member states may provide for more specific rules to protect employees when their personal data are processed.

115 GDPR (n 1) Art 9(2)*(b)*.

with its purposes. The processing must be done in the course of its legitimate activities with appropriate safeguards in place and the personal data may not be disclosed outside that body without the consent of the data subjects.[116]

The processing of special personal information is also allowed in the medical field in the following situations: if it is necessary for the purposes of preventive or occupational medicine; for assessing the working capacity of the employee; for a medical diagnosis; for the provision of health or social care or treatment; or for managing health or social care systems and services.[117] Processing must be done on the basis of a law, or in terms of a contract with a health professional and subject to specific conditions and safeguards,[118] namely that the processing must be done under the responsibility of a person who is subject to an obligation of professional secrecy.[119]

Processing may also take place to protect the public interest in the area of public health. This would include protecting against serious cross-border threats to health such as the prevention and control of communicable diseases,[120] or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices. Processing must be done on the basis of a law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.[121]

Finally, special categories of personal data may be processed if processing is necessary for archiving purposes—which must be in the public interest—or for scientific or historical research purposes, or statistical purposes.[122] It must be based on a law that is proportionate to the aim pursued which respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[123]

---

116 GDPR (n 1) Art 9(2)*(d)*.

117 GDPR (n 1) Art 9(2)*(h)*.

118 GDPR (n 1) Art 9(2)*(h)*.

119 GDPR (n 1) Art 9(3).

120 For instance, Covid-19. Although this exception allows for sensitive medical information to be processed without the consent of the patient, it should be remembered that the other requirements of the law still apply, such as the need for confidentiality, data minimisation, purpose limitation and data security.

121 GDPR (n 1) Art 9(2)*(i)*.

122 GDPR (n 1) Art 89(1) spells out the safeguards that must be in place. The safeguards relate to technical and organisational measures to protect the rights and freedoms of the data subject. In particular, the principle of data minimisation must be respected.

123 GDPR (n 1) Art 9(2)*(j)*.

POPI Act

Turning to the POPI Act, we see that the processing of special personal information is also prohibited, unless an 'authorisation' (that is, an exemption to the prohibition) is applicable.[124] There are general authorisations that apply to the processing of all types of sensitive information and specific authorisations that are applicable to certain types of sensitive information only.

Special personal information may in general be processed when:

- processing is carried out with the consent of the data subject;
- processing is necessary for establishing, exercising or defending a right or an obligation in law;
- processing is necessary to comply with an obligation under international public law;
- processing is done for historical, statistical or research purposes (to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible to ask for consent or asking for consent would involve a disproportionate effort);
- the information has deliberately been made public by the data subject; or
- one of the specific grounds for processing special information is present.[125]

The responsible party may also apply to the Regulator for permission to process special information in the public interest. The Regulator may then authorise the responsible party, by means of a publication in the Government Gazette, to do the processing. The Regulator may impose reasonable conditions under which the processing must take place.[126]

The Act furthermore contains exemptions specific to every type of special information. For example, personal information concerning a person's religious or philosophical beliefs may be processed by a spiritual or religious organisation to which the data subject belongs if the processing is necessary to achieve its aims and principles.[127] They may also process personal information of the member's family if the organisation has

124 POPI Act 4 of 2013 s 26*(a)*.
125 POPI Act 4 of 2013 s 27(1).
126 POPI Act 4 of 2013 s 27(2) and (3).
127 POPI Act 4 of 2013 s 28(1).

regular contact with the family members in connection with its aims and they have not objected in writing to the processing.[128]

Institutions other than spiritual or religious organisations may also process personal information concerning a person's religious or philosophical beliefs if it is necessary to protect the spiritual welfare of the data subject, unless the data subject has objected to this.[129] This personal information may never be supplied to third parties without the consent of the data subject.[130]

Personal information concerning race or ethnic origin may be processed to identify data subjects when processing information on the race of a person is essential to identify the person, or to comply with laws or measures designed to protect persons disadvantaged by unfair discrimination.[131]

Trade unions or trade federations may process the personal information of their members if this is necessary to achieve the aims of the trade union.[132] Once again, this personal information may never be supplied to third parties without the consent of the data subject.[133]

A political institution to which the data subject belongs may process the personal information of the data subject if the processing is necessary to achieve the aims of the institution.[134] It may also process the personal information of a data subject if it is necessary for the purposes of forming a political party, participating in the activities of the party, canvassing for the party in an election or campaigning for its cause.[135] This personal information may not be supplied to a third party without the data subject's consent.[136]

A number of persons or institutions—such as medical professionals and healthcare facilities, insurance companies, medical schemes, schools, institutions managing the care of children, pension funds and prison authorities—may process personal information concerning the health or sex life of a data subject.[137] In each case, the

128 POPI Act 4 of 2013 s 28(2).
129 POPI Act 4 of 2013 s 28(1)*(c)*.
130 POPI Act 4 of 2013 s 28(3).
131 POPI Act 4 of 2013 s 29.
132 POPI Act 4 of 2013 s 30(1).
133 POPI Act 4 of 2013 s 30(2).
134 POPI Act 4 of 2013 s 31(1)*(a)*.
135 POPI Act 4 of 2013 s 31(1)*(b)*.
136 POPI Act 4 of 2013 s 31(2).
137 POPI Act 4 of 2013 s 32(1) provides:
'The prohibition on processing personal information concerning a data subject's health or sex life, as referred to in section 26, does not apply to the processing by –

processing must be necessary to enable the institutions to provide care to the data subject, to properly administer the particular institution or to perform their lawful duties and obligations.[138] The persons processing the information must be subject to an obligation of confidentiality[139] or must treat the information as confidential.[140] If it is necessary for the proper treatment or care of the data subject, any type of special information (race, gender, etc) may be processed.[141]

Bodies charged with applying criminal law may process personal information concerning criminal behaviour or biometric information.[142] So, too, may responsible parties who have obtained personal information concerning criminal behaviour or biometric information in accordance with the law.[143] Any type of special information may be processed if such processing is necessary to supplement the processing of information on criminal behaviour or biometric information.[144] In the case of processing

---

medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;
insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations, if such processing is necessary for—
assessing the risk to be insured by the insurance company or covered by the medical scheme and the data subject has not objected to the processing;
the performance of an insurance or medical scheme agreement; or
the enforcement of any contractual rights and obligations;
schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sex life;
any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;
any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or
administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for –

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sex life of the data subject; or
(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.'

138 POPI Act 4 of 2013 s 32(1).
139 POPI Act 4 of 2013 s 32(2).
140 POPI Act 4 of 2013 s 32(3).
141 POPI Act 4 of 2013 s 32(4).
142 POPI Act 4 of 2013 s 1 defines 'biometrics' as 'a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.'
143 POPI Act 4 of 2013 s 33(1).
144 POPI Act 4 of 2013 s 33(3).

the personal information of personnel in the service of a responsible party, processing must comply with labour law rules.[145]

Comparison

Both the GDPR and the POPI Act introduce a higher level of protection when sensitive personal information is processed. It is somewhat problematic to compare the grounds for processing in the case of special personal information, since the POPI Act spells out the authorisations for each type of special personal information separately, whereas the GDPR groups them together.

Both allow sensitive data to be processed based on the consent of the data subject, but the consent that is required by the GDPR must be 'explicit'. It appears that the data controller must make an extra effort to obtain the consent of the data subject in order to process special categories of personal information. POPI has only one level of consent, irrespective of whether the information being processed is sensitive personal information or not. POPI therefore does not afford the same level of protection as the GDPR in this regard. The GDPR also allows member states to provide that a data subject may not give consent in certain situations, whereas the POPI Act does not contain a similar provision.

The GDPR specifically allows for special personal information to be processed in the field of employment and social security and social protection law. The POPI Act makes an exception for administrative bodies, pension funds, employers or institutions working for them to process special personal information, but only when the information concerns a data subject's health or sex life.[146]

An important provision in the GDPR in the light of the Covid-19 pandemic is that sensitive personal information may be processed if it is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices.[147]

A scrutiny of the POPI Act's provisions dealing with the processing of medical information[148] shows that the Act does not specifically provide that the government may process sensitive personal information in the form of medical information for public health purposes. There is a general provision that general, non-sensitive personal information may be processed in the public interest; however, personal information

145 POPI Act 4 of 2013 s 33(2).
146 POPI Act 4 of 2013 s 32(1).
147 GDPR (n 1) Art 9(2)*(i)*.
148 See (n 137) for more detail.

relating to a data subject's health is a special category of data and the grounds for processing personal information in general do not apply. The Regulator may have to authorise the government to process medical health information for reasons of public interest in the area of public health, such as combating a pandemic, by means of a publication in the Government Gazette.[149] The other exceptions allowing medical information to be processed are all narrowly circumscribed and do not seem to be applicable.

An important difference which should be pointed out is that the GDPR requires that in certain situations where processing of special personal information is allowed, the processing must be authorised by a law, a contract and/or a collective agreement and appropriate safeguards must be in place to protect the fundamental rights and interests of the data subject. Examples of these situations are where processing is allowed in order to carry out the obligations of the data controller or to exercise the rights of the data subject in the field of employment and social security and social protection law;[150] where a foundation, association or another not-for-profit body with a political, philosophical, religious or trade union aim is allowed to process the special personal information of its members;[151] where the processing of special personal information is allowed in the medical field;[152] and permissible processing for archiving purposes, scientific or historical research purposes, or statistical purposes.[153] The POPI Act does not require the processing in similar situations to be authorised by a law, an agreement or a contract. The question arises whether this places the protection provided by the POPI Act at a lower level or whether the GDPR merely allows for national laws to determine the level of protection. Whether these differences are material for the purposes of an adequacy decision is uncertain at this stage, but in my opinion they are not material.

Processing of Personal Data Relating to Criminal Convictions and Offences

GDPR

The GDPR does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal

149 POPI Act 4 of 2013 s 27(2) and (3).

150 GDPR (n 1) Art 9(2)*(b)*.

151 GDPR (n 1) Art 9(2)*(b)*. In this instance, the GDPR also requires that the personal data may not be disclosed outside that body without the consent of the data subjects. The POPI Act does not contain such a provision.

152 GDPR (n 1) Art 9(2)*(i)*.

153 GDPR (n 1) Art 89(1) spells out the safeguards that must be in place. The safeguards relate to technical and organisational measures to protect the rights and freedoms of the data subject. In particular, the principle of data minimisation must be respected.

offences or the execution of criminal penalties.[154] These activities are subject to another Union law.[155] However, in certain instances the GDPR may be applicable to these authorities, namely, when member states entrust other tasks, which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to these authorities. The processing of personal data for those other purposes falls within the scope of the GDPR.[156] Private entities, such as employers, may also process personal information that relates to possible criminal convictions of data subjects, such as when they do background screening of job applicants. In those instances, the GDPR is also applicable.

The processing of personal data concerning criminal offences committed by a data subject is not treated as a special category of personal data by the GDPR. Processing this type of data may therefore be done lawfully based on any one of the general grounds for processing personal data found in Article 6(1).[157] However, it is further required that such processing must be done 'only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.' Furthermore, 'a comprehensive register of criminal convictions must also be kept under the control of official authority.'[158]

POPI Act

The POPI Act, on the other hand, considers personal information relating to criminal offences committed by the data subject as a special category of personal information.[159] In order to compare the provisions of the POPI Act with those of the GDPR, the provisions are briefly repeated here.

In terms of the POPI Act a responsible party may, subject to exceptions, not process personal information concerning '*(a)* the criminal behaviour of a data subject to the extent that such information relates to – (i) the alleged commission by a data subject of

154 GDPR (n 1) Art 2(2)*(d).*

155 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA Official Journal L119/89.

156 GDPR recital (19).

157 GDPR (n 1) Art 10.

158 GDPR (n 1) Art 10.

159 POPI Act s 26.

any offence; (ii) or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.'[160]

The general exceptions to the prohibition on the processing of special personal information, including information concerning criminal behaviour or biometric information, were discussed previously.[161] In short, special personal information may be processed if the data subject consented to this, if the processing is necessary to establish, exercise or defend a right or an obligation in law or to comply with an obligation of public international law, if the processing is done for historical, statistical or research purposes, or if the information has deliberately been made public by the data subject.

The Act also authorises the processing of a data subject's criminal behaviour and biometric information in specific circumstances. First of all, bodies charged with applying criminal law may process such data; so, too, may responsible parties who have obtained this information in accordance with the law.[162] If the responsible party processes this type of personal information about its employees, the processing must comply with labour legislation.[163] Other types of special personal information may also be processed if this is necessary to supplement the processing of information on criminal behaviour or biometric information as permitted by the Act. [164]

The responsible party may also apply to the Regulator to be allowed to process special information in the public interest. The Regulator may then authorise the responsible party, by publication in the Government Gazette, to do the processing. The Regulator may impose reasonable conditions under which the processing must take place.[165]

Comparison

When comparing the GDPR and the POPI Act in respect of the processing of personal data relating to criminal convictions and offences, it is evident that they both allow processing about the criminal convictions of a data subject by an official authority, or by another party when the processing is authorised by a specific law. The GDPR provides that only an official authority may keep a comprehensive register of criminal convictions. The POPI Act does not contain a similar rule.

160 POPI Act 4 of 2013 s 26*(b)*.
161 See the paragraph 'Grounds for Lawful Processing of Special Categories of Data' above.
162 POPI Act 4 of 2013 s 33(1).
163 POPI Act 4 of 2013 s 33(2).
164 POPI Act 4 of 2013 s 33(3).
165 POPI Act 4 of 2013 s 27(2) and (3).

Since the GDPR does not consider personal information regarding criminal convictions and offences to be a special category of personal information, all of the general grounds for processing are applicable. In contrast, the POPI Act considers this to be a special category of personal information and allows it to be processed only in specific limited circumstances. Arguably, this places the protection provided by the POPI Act at a higher level than that required by the GDPR.

Processing Personal Information of Children

GDPR

The GDPR states that

> children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[166]

Only persons over the age limit set for consent may consent to the processing of their personal data. In the case of a child under the age of consent, the person holding parental responsibility for the child must consent. The GDPR states that the age of consent is sixteen years, but a member state may provide for a lower age provided it is not lower than thirteen years.[167]

The GDPR does not provide for a separate set of lawful bases for the processing of personal information of children.

POPI Act

Under the POPI Act, the personal information of children (as defined in the Act) may not be processed, unless the processing is specifically authorised in the Act.[168] The Act defines a child as 'a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.'[169]

The grounds on which processing the personal information of a child is allowed are the same as the general exemptions for special information which were discussed above,

166 GDPR recital (38).

167 GDPR (n 1) Art 8(1).

168 POPI Act 4 of 2013 s 34.

169 POPI Act 4 of 2013 s 1. If a child under the age of 18 is competent to act without the assistance of a competent person, then it would appear that the provisions of s 34 of the Act do not apply. See Hanneretha Kruger, 'Protection of a Child's Right to Privacy in South African Law' in J Potgieter, J Knobel and R Jansen (eds), *Essays in Honour of/Huldigingsbundel vir Johann Neethling* (LexisNexis 2015) 277; Roos (n 34) 393.

apart from the fact that a competent person has to act on behalf of the child. A competent person is a person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child[170]—in other words, the guardian of the child[171] or a person appointed by the courts.[172]

The grounds for processing can briefly be summarised as the prior consent of a competent person, where processing is necessary for establishing, exercising or defending legal rights or obligations or to comply with an international public-law obligation; or processing that is done for historical, statistical or research purposes (subject to the provisos explained); or where the information processed has deliberately been made public by the child with the consent of the competent person.[173]

As is the case when processing special information, the Regulator may authorise processing of personal information of a child if it is in the public interest.[174] Here again, the Regulator may impose reasonable conditions in respect of this authorisation, but in this instance, the Act provides a more detailed explanation of the conditions.[175]

Comparison

When comparing the GDPR and the POPI Act as they relate to the processing of the personal information of a child, we see that both allow the processing of the personal information of children on the general grounds for processing, apart from the fact that the child may not consent on its own but requires the assistance of a person who has parental responsibility over the child (termed a competent person in the POPI Act.)

The main difference between the GDPR and the POPI Act is the fact that under the GDPR children who are sixteen years of age or older are considered capable of consenting on their own to the processing of personal information. Under the POPI Act, any child below the age of eighteen years needs the assistance of a competent person,

170 POPI Act 4 of 2013 s 1.

171 See Children's Act 38 of 2005 s 18(3).

172 Burns and Burger-Smidt, (n 34) 97.

173 POPI Act 35(1)*(a)–(e)*.

174 POPI Act 4 of 2013 s 35(2).

175 POPI Act 4 of 2013 s 35(3)*(a)–(d)*. The Regulator may impose conditions regarding how the responsible party should allow the competent person to review the personal information or refuse to permit further processing. The conditions may also require the responsible party to give notice about the nature of the information, how the information is being processed and what further processing will take place. The conditions may also instruct the responsible party not to encourage or persuade a child to disclose more personal information about themself than is reasonably necessary, given the purpose for which it is intended. Finally, the conditions may provide that the responsible party should have reasonable procedures in place to protect the integrity and confidentiality of the personal information.

unless the child is legally competent to consent to any action or decision being taken in respect of that child.[176] The provisions of the POPI Act are therefore arguably substantially similar to those of the GDPR and actually afford protection to a wider group of subjects.

Conclusion

In this article, the GDPR and the POPI Act were compared with regard to the content of specific concepts and the legal bases for lawful processing. It is indicated that the content of concepts such as personal data or information, the processing of personal information, data controller, data processor, recipient, and special categories of personal data found in the POPI Act is equivalent to the content of those concepts in the GDPR. Regarding the grounds for lawful processing of personal information, differences were pointed out and it was suggested that the POPI Act should be amended to comply with the standard set in the GDPR. One could argue that these differences are not substantial enough to derail an adequacy finding. However, in my opinion, it would be prudent for the legislature to bolster the provisions that do not reach the standard set by the GDPR before approaching the EU for such a declaration.

It is recommended that the following amendments be made:

(1) In the case of consent as a ground for processing personal information in general, it should be required that the data subject gives consent by means of a *clear affirmative action*.

(2) In the case of consent as a ground for processing special categories of personal information, it should be required that the data subject *explicitly* gives such consent.

(3) In the case of processing that complies with an obligation imposed by law on the responsible party or processing that protects a legitimate interest of the data subject, it should be required that the processing is *necessary* to fulfil those purposes.

(4) In the case of processing personal information to protect the interests of the data subject, it should be required that the interests that are to be protected are *vital* and it must be provided that public authorities may not use this ground as a basis for processing personal information, but must instead have another legal basis provided by the legislator.

[176] POPI Act 4 of 2013 s 1. The POPI Act defines a child as 'a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.'

(5) Where processing of personal information is allowed in order to carry out the obligations of the data controller or to exercise the rights of the data subject in the field of employment, and social security and social protection law; or where a foundation, association or another not-for-profit body with a political, philosophical, religious or trade union aim is allowed to process the special personal information of its members; or where processing of special personal information is allowed in the medical field; and where processing for archiving, scientific or historical research purposes, or statistical purposes is allowed, such processing should be authorised by a law, an agreement or a contract.

(6) Regarding the processing of information relating to criminal convictions, it would be advisable to follow the example set by the GDPR and to spell out that only an official authority may keep a comprehensive register of criminal convictions.

(7) Where the processing of special categories of personal information is allowed on the basis that it is in the public interest, it should be a requirement that the public interest is *substantial* and that the processing takes place on the basis of a *law*. Such a law should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The legislature should also consider introducing the following provisions found in the GDPR:

- The processing of special categories of information should be allowed in order to protect the public interest in the area of public health, especially where protection is required against serious cross-border threats to health such as communicable diseases, which must be prevented and controlled, or high standards of quality and safety of healthcare and of medicinal products or medical devices must be ensured. Processing must be done on the basis of a law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- The legislature should consider whether there are situations in which data subjects should not be allowed to give consent to the processing of special personal information.

There are, of course, other provisions relating to the data-protection principles, data subject rights, restrictions on onward transfer and the procedural and enforcement mechanisms which should also be evaluated before a definitive answer can be given to the question whether the POPI Act meets the benchmark set by the GDPR. As indicated earlier, these provisions will be dealt with in future articles.

References

Blume P, 'EU Adequacy Decisions: The Proposed New Possibilities' (2015) 5 International Data Privacy Law <https://doi.org/10.1093/idpl/ipu026>

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

Bygrave LA, *Data Privacy Law: An International Perspective* (OUP 2014) <https://doi.org/10.1093/acprof:oso/9780199675555.001.0001>

De Hert P and Papakonstantinou V, 'The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals' (2012) 28 The Computer Law and Security Review <https://doi.org/10.1016/j.clsr.2012.01.011>

Gilbert F, 'Proposed EU Data Protection Regulation: The Good, the Bad and the Unknown' (2012) 15 (10) Journal of Internet Law.

Hoofnagle CJ, Van der Sloot B and Zuiderveen Borgesius FJ, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law <https://doi.org/10.2139/ssrn.3254511>

Hustinx P, 'The Reform of EU Data Protection Law: Towards More Effective and More Consistent Data Protection Across the EU' in Witzleb N, Lindsay D, Paterson M and Rodrick S, *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press 2014).

Kelleher D and Murray K, *EU Data Protection Law* (Bloomsbury Professional 2018).

Korff D, *Data Protection Laws in the European Union* (Federation of European Direct Marketing 2005).

Kotschy W, 'The Proposal for a New General Data Protection Regulation – Problems Solved?' (2014) 4 International Data Privacy Law <https://doi.org/10.1093/idpl/ipu022>

Kruger H, 'Protection of a Child's Right to Privacy in South African Law' in Potgieter J, Knobel J and Jansen R (eds), *Essays in Honour of / Huldigingsbundel vir Johann Neethling* (LexisNexis 2015).

Kuner C, 'Reality and Illusion in EU Data Transfer Regulation Post Schrems' (2017) 18 German Law Journal <https://doi.org/10.2139/ssrn.2732346>

Neethling J and Potgieter JM, *Neethling-Potgieter-Visser Law of Delict* (7th edn, LexisNexis 2014).

Neethling J, *Neethling-Potgieter-Visser Law of Delict* Potgieter JM and Knobel JC, (7th edn, LexisNexis 2014).

Porcedda MG, 'On Boundaries – Finding the Essence of the Right to the Protection of Personal Data' in Leenes R, Van Brakel R, Gutwirth S and De Hert P, *Data Protection and Privacy: The Internet of Bodies* (Hart Publishing 2018).

Reding V, 'The Upcoming Data Protection Reform for the European Union' (2011) 1 International Data Privacy Law <https://doi.org/10.1093/idpl/ipq007>

Roos A, 'Core Principles of Data Protection Law' (2006) 39 Comparative and International Law Journal of Southern Africa.

Roos A, 'Data Privacy Law' in Van der Merwe DP (ed), *Information and Communications Technology Law* (2nd edn, LexisNexis 2016).

Roos A, 'Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position' (2007) 124 South African Law Journal.

Roos A, 'Legal Protection of Personal Information' in Neethling J, Potgieter JM and Roos A, *Neethling on Personality Rights* (LexisNexis 2019).

Roos A, 'Personal Data Protection in New Zealand: Lessons for South Africa?' (2008) 4 Potchefstroom Electronic Law Journal <https://doi.org/10.4314/pelj.v11i4.42243>

Roos A, 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study' (LLD thesis, Unisa 2003).

Schwartz PM, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 Iowa Law Review.

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law <https://doi.org/10.1093/idpl/ipt004>

Tzanou M, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-terrorism Surveillance* (Hart 2017).

Voss WG, 'Looking at European Union Data Protection Law Reform through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later' (2014) 17 (9) Journal of Internet Law.

Zell A, 'Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field' (2014) 15 German Law Journal <https://doi.org/10.1017/S207183220001899X>

Cases

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Case C-311/18 (*Schrems II* case).

Financial Mail (Pty) Ltd v Sage Holdings Ltd 1993 (2) SA 451 (A).

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; *In re Hyundai Motor Distributors (Pty) (Ltd) v Smit NO* 2001 (1) SA 545 (CC).

Maximillian Schrems v Data Protection Commissioner, Case C‑362/14, 6 October 2015.

Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C326.

Children's Act 38 of 2005.

Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 OJ (L 215).

Data Protection Act 2018.

European Commission, Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU–U.S. Privacy Shield, C (2016) 4176 final (12 July 2016).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31.

Personal Data Protection Act of 2000 (Wet Bescherming Persoonsgegevens).

Protection of Personal Information Act 4 of 2013.

Promotion of Access to Information Act 2 of 2000.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Government Publications

Commission of the European Communities, 'First Report on the Implementation of the Data Protection Directive (95/46/EC)' COM (2003) 265 final.

Commission 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) Explanatory Memorandum to the Reform Package COM(2012) 11 final.

European Commission, '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) Explanatory Memorandum to the Reform Package' COM(2012) 11 final (European Commission Explanatory Memorandum).

GG 42110, RG 10897 (14 December 2018) GN 1383.

Proclamation No R 21 of 2020 in Gazette 11136, Vol 660 No 43461.

South African Law Reform Commission, *Privacy and Data Protection: Project 124* (SALRC 2009).

EU Data Protection Working Party Documents / European Data Protection Supervisor Documents

Article 29 Data Protection Working Party, Adequacy Referential (Updated) WP254 28 Nov 2017.

Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 WP259 rev.01 (10 April 2018).

Article 29 Data Protection Working Party, Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive WP12 (24 July 1998)).

European Data Protection Supervisor, *Guidelines on the Concepts of Controller, Processor and Joint Controllership under Regulation (EU) 2018/1725* (7 November 2018).

Treaties and Conventions

Consolidated Version of the Treaty establishing the European Community [2002] OJ C325/33).

Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS 108.