Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part I: The Territorial Scope Provision

J Coetzee*

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed, open access online law publications

Author

Juana Coetzee

Affiliation

Stellenbosch University, South Africa

Email

jcoet@sun.ac.za

Date Submitted

25 November 2022

Date Revised

31 May 2024

Date Accepted

31 May 2024

Date Published

7 November 2024

Editor

Prof W Erlank

Journal Editor

Prof C Rautenbach

How to cite this contribution

Coetzee J "Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part I: The Territorial Scope Provision" *PER / PELJ* 2024(27) - DOI http://dx.doi.org/10.17159/1727-3781/2024/v27i0a15233

DOI
http://dx.doi.org/10.17159/1727-3781/2024/v27i0a15233

Abstract

The *Protection of Personal Information Act* 4 of 2013 (POPIA) was introduced to protect the right to privacy of the South African data subject. The Act prescribes obligations that a responsible party must fulfil to achieve this purpose. However, for the Act to be enforced against a responsible party who has transgressed any of its provisions, the responsible party needs to be brought under its jurisdiction. To that end, POPIA makes provision for a territorial scope provision (section 3) based on the notion of *domicilium* and the use of automated and non-automated means for processing personal information situated in the Republic. This article makes use of comparative analysis to interpret the content of these provisions with reference to the European Union (EU)'s 1995 *Data Protection Directive* (DPD), on which they were modelled, and its successor, the 2016 *General Data Protection Regulation* (GDPR). The article demonstrates that section 3 can give rise to interpretative uncertainties which could result therein that personal information processed by responsible parties who are outside the Republic would not be regulated by the Act, or that these parties could move their processing activities out of the country to escape liability. An expansive interpretation of these provisions by the courts is needed to plug these gaps; alternatively, legislative revision must be undertaken in line with developments in the EU, where the GDPR endeavoured to address some of these aspects.

Keywords

POPI/POPIA; personal information; territorial scope; section 3 POPIA.

.....

1 Introduction

Using the Internet for commercial exchange has led to an increase in international trade in goods and services. This stimulates the global economy and, in turn, creates an opportunity for economic growth, which can assist in alleviating poverty.[1] However, standing central to the development of the digital economy is the free flow of data. A report of the Organisation for Economic Cooperation and Development (OECD) published in 2018 noted that the free flow of data facilitates trade in goods and services.[2] Moreover, the free flow of information is a basic human right that is protected constitutionally.[3]

The impact of Covid 19 has emphasised the value of the free flow of information on different levels. Thus, data sharing assisted in researching the virus and ultimately in developing a vaccine. Furthermore, the free flow of data facilitates online shopping, which provided many with the opportunity to continue doing business, and for the consumer the possibility of obtaining household necessities without having to expose themselves to the virus. When lockdowns and other social distancing measures prevented contact in person, your house suddenly became your home, office, classroom, and movie theatre. Many could continue working from home; education resumed online when face-to-face teaching was no longer possible; online platforms enabled social connection with family and friends; and digital service networks provided entertainment.[4]

However, the free flow of data often entails the collection and distribution of personal information. In some instances the processing of personal information is necessary to complete a transaction and its performance; for example, in connection with the payment and delivery aspects thereof. In this context the transfer of personal data to another country is often unavoidable for the completion of a cross-border transaction; for example, when a consumer purchases goods online via a non-domestic website or

* Juana Coetzee. BA, LLB, LLM, LLD (Stellenbosch University). Associate Professor (Emeritus) and Research Fellow, Department of Mercantile Law, Stellenbosch University, South Africa. Email: jcoet@sun.ac.za. ORCiD: https://orcid.org/0000-0003-1388-4792.

1 This explains why the digital economy is listed as one of the United Nations 2030 Sustainable Development Goals. UN General Assembly *Transforming our World: The 2030 Agenda for Sustainable Development* UN Doc A/RES/70/1 (2015) Goal 9c.

2 OECD 2018 https://one.oecd.org/document/TAD/TC/WP(2018)19/FINAL/En/pdf.

3 Section 14 of the *Constitution of the Republic of South Africa*, 1996 (the Constitution). Even internationally, it is protected by the *Universal Declaration of Human Rights* (1948) and numerous other conventions.

4 This contribution recognises the consequences of the digital divide between the rich and the poor, which affects access to digital information. However, it is not the purpose of this article to discuss these aspects in any detail.

when registering with a digital service provider. Information that is processed in South Africa can also leave the country to be further processed in another country or stored on servers, or in the cloud, located in another legal jurisdiction. Data processing connected to social media or cross-border data sharing by public authorities are common examples of the export of personal information to other countries. Processing can even take place without the knowledge or consent of the data subject. Cookies, scanners, sensors, radio frequency identification tags on consumer goods and other technological interventions that support Big Data are a few examples that fall into the latter category. To make our lives easier the Internet of Things connects household appliances and other smart goods to the Internet, and to make us feel safer they watch our houses and our children. In the process they follow our daily movements and collect information on our likes and dislikes, record our voices, store images of our loved ones and ourselves, and much more. Once collected, do we know where our personal data is going and what is done with that information? Even if technology can help to keep us safe by monitoring who enters our properties and neighbourhoods, is our personal data safe?

The concept "personal information" is hard to define exhaustively.[5] To illustrate, it includes not only regular personal and contact details such as your name, address, telephone number or ID number,[6] but also other demographic information such as your gender, marital status, language, nationality and race.[7] It can further include identifiers such as images of a person, voice recordings, location data[8] and biometric information;[9] financial information;[10] and behavioural information such as your personal preferences, beliefs and opinions,[11] or sexual orientation;[12] and other background information such as your physical and mental health,[13] education, religion, or criminal and employment history.[14] It even includes other people's opinions on a data subject,[15] or a data subject's private correspondence.[16] The definition of personal information as set out in section 1 of the *Protection of Personal Information Act* 4 of 2013 (hereafter

5 See De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.1.1.

6 Para (c) of the definition of "personal information" in s 1 of the *Protection of Personal Information Act* 4 of 2013 (POPIA).

7 Paragraph (a) of the definition of "personal information" in s 1 of POPIA.

8 Paragraph (c) of the definition of "personal information" in s 1 of POPIA.

9 Paragraph (d) of the definition of "personal information" in s 1 of POPIA.

10 Paragraph (b) of the definition of "personal information" in s 1 of POPIA.

11 Paragraph (e) of the definition of "personal information" in s 1 of POPIA.

12 Paragraph (a) of the definition of "personal information" in s 1 of POPIA.

13 Paragraph (a) of the definition of "personal information" in s 1 of POPIA.

14 Paragraph (b) of the definition of "personal information" in s 1 of POPIA.

15 Paragraph (g) of the definition of "personal information" in s 1 of POPIA.

16 Paragraph (f) of the definition of "personal information" in s 1 of POPIA.

POPIA or the Act) therefore does not constitute a *numerus clausus* of types of information covered by the Act but takes account of all "information relating to an identifiable, living, natural person, and … an identifiable, existing juristic person".[17] Certain types of personal information such as that of children, information on gender, race, medical condition, religion, philosophical beliefs or biometric information are furthermore classified as so-called sensitive or special personal information.[18] POPIA prohibits the processing of these types of personal information unless the information falls under the limited grounds for exceptions.[19]

The protection of personal information does not prohibit the processing of all personal information but ensures the lawful processing of personal data by imposing legal conditions on such processing. As the processing of personal information can infringe on a data subject's right to privacy, data protection laws must balance the right to the free flow of information with the rights to privacy and identity.[20] To that effect, international organisations have formulated instruments, guidelines and principles on data privacy that form the basis for data privacy laws. Where countries make use of these principles, they harmonise and bring greater equivalence between the standards and rules in these countries' domestic privacy laws.[21] As the processing of personal information is mostly facilitated by the Internet, personal data can move across geographical and jurisdictional borders in a matter of seconds. Legal harmonisation of and legal certainty on data protection laws are important to ensure that the data subject's rights are protected, irrespective of where the data is processed.[22] Moreover, the processing of personal information can be complex and can involve chains

17 Section 1 of POPIA.

18 Section 26 of POPIA.

19 Sections 26-35 of POPIA. The Information Regulator can also provide exemptions: ss 36-38 of POPIA.

20 Section 14 of the Constitution.

21 One example of such international standards or guidelines is the *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (adopted on Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, Paris, 23 September 1980, revised 11 July 2013) (OECD 2013 https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonal data.htm). The *OECD Guidelines* make provision for so-called data privacy principles. They are not legally binding but they can be adopted by states in the form of legislation or by companies in the form of codes of conduct. These guidelines have played an important role in the formulation of the major data protection. Also see the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108/1981* (1981); *Directive 95/46/EC of the European Parliament and of the Council enacted 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 L 281/31, which served as a model for the drafting of national data protection laws, specifically so in the case of POPIA.

22 Roos "Data Privacy Law" 395-396.

of processors situated in different countries, which might entail that the data subject's personal information is transferred to another country and later transferred onwards to yet another country for further processing. Whether the information would be protected adequately in third party countries is often not clear. This can leave data subjects vulnerable to further processing of their personal information for purposes other than those for which they were collected originally.

Personal data has become the commodity of our times,[23] which means that processors, operators or their employees often sell personal data to be used for market research, targeted advertising or profiling. However, the processing of personal information can take place without a lawful purpose. Alternatively, data can be obtained through illegal access to databases and used for illegal purposes such as extortion, or to commit crimes involving identity theft.[24] Furthermore, in some countries governments are allowed for security purposes to access the personal data of data subjects stored or hosted on databases or servers located in that country, which actions may go far beyond what is necessary or proportionate in a democratic society. The facts giving rise to the European Court of Justice (ECJ)'s decisions in *Maximillian Schrems v Data Protection Commissioner* (hereafter *Schrems I*) and *Data Protection Commissioner v Facebook Ireland, Maximillian Schrems* (hereafter *Schrems II*) that involved the transfer of personal data by Facebook from its servers in Ireland to the United States of America (USA) are a typical example here.[25] In these cases the main concern was that the personal data of European Union (EU) citizens transferred to the USA were subjected to surveillance by their intelligence agencies. Although these aspects do not form the main focus of this article, they can become relevant when it comes to the transfer of information outside the borders of a country.[26]

It is clear that there is a need for legal regulation that protects the data subject against unlawful processing but at the same time supports the free and lawful flow of data to facilitate commerce, innovation, and technological and economic development. In South Africa POPIA finally came into

---

23 Data has become a major commodity of the twenty-first century and has been called the "new oil". See Hayward 2021 *UNSW Law Journal* 888.

24 This article will not focus on these scenarios although they are covered by POPIA and more specifically by the *Cybercrimes Act* 19 of 2020.

25 *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14) [2015] ECLI:EU:C:2015:650 (*Schrems I*); *Data Protection Commissioner v Facebook Ireland, Maximillian Schrems* Case C-311/18 [2020] ECLI:EU:C2020:559 (*Schrems II*).

26 Data transfers are discussed in more detail in part II of this article. In *Schrems II*, the ECJ invalidated the Privacy Shield agreement between the EU and the USA. The process of negotiating a new adequacy agreement is currently under way. See EDPB 2022 https://edpb_statement_202201_new-trans-atlantic_data-privacy_framework.pdf.

operation on 1 July 2020 after it had already been promulgated in 2013.[27] For many this was a long-awaited day as the purpose of the Act is to regulate the processing of personal information of both natural and juristic persons. The preamble to POPIA makes it clear that the Act is aimed at the protection of personal information when processed by public as well as private bodies. It therefore covers the processing of the information of natural and juristic persons by the state and its organs, but also processing in the private sphere, such as that associated with commercial transactions.

According to its Preamble and section 2,[28] POPIA is to give effect to the fine balance between the constitutional right to privacy in section 14 of the *Constitution of the Republic of South Africa*, 1996, which includes "a right to protection against the unlawful collection, retention, dissemination and use of personal information",[29] and the need to remove unnecessary impediments to the free flow of information in order to promote "constitutional values of democracy and openness, the need for economic and social progress, within the information society".[30] This balance is to be achieved in the context of international standards aimed at the processing of personal information. POPIA provides minimum threshold requirements for the lawful processing of personal information, which translate into duties for the responsible party but also corresponding rights for the data subject.[31] These rights and duties can be enforced with the assistance of the Information Regulator and by way of the criminal, administrative and civil remedies provided for in the Act.[32]

Where responsible parties collect personal information from data subjects in South Africa such information can be processed inside the country but it can also leave the country to be processed abroad.[33] For example, a South African responsible party can make use of call centres abroad, or the data can be stored on servers or in cloud-based depositories located in another country. Data can also be collected from South African data subjects by a non-South African responsible party, such as an internet service or social network providers, and then processed in another country. These are typical examples where personal data end up outside the borders and the jurisdiction of the Republic of South Africa (RSA).

---

27 Most sections of the Act came into operation on 1 July 2020 but responsible parties were given a grace period of one year to make sure that they meet the requirements of the Act.

28 Sections 2(a)(i) and (ii) of POPIA.

29 Preamble to POPIA.

30 Preamble to POPIA.

31 Sections 2(b), 5, 8-25, 69-71 of POPIA.

32 Sections 2(b)-(d), 73-109 of POPIA.

33 See s 72 of POPIA.

Worldwide the main measures used to protect data flows to destinations outside the borders of a country are territorial scope provisions and data transfer provisions. Both aim to prevent the circumvention of the data protection laws of a country by exporting the data to another country. Territorial scope rules determine when the provisions of a data protection law will apply to parties located outside the borders of the country where the law would normally apply. This therefore extends the scope of the data protection law beyond the borders of a particular country. Data transfer rules, on the other hand, restrict the transfer of personal data to a third country by placing restrictions on and adding conditions to the processing of such information. Although both find application to parties located in other countries, the purpose and function of these rules are different. POPIA, like many other data protection laws, uses both measures. Section 3(1) states that the Act will apply in instances where the responsible party is domiciled in the RSA or where it makes use of equipment located in the Republic for its processing purposes. Section 72, on the other hand, explicitly regulates the cross-border transfer of data by a responsible party from the RSA to another country by setting certain conditions for such transfer.

This article restricts itself to a critical interpretation of the territorial scope provision. This is not the first time that section 3 of POPIA has been discussed and analysed in the context of academic scholarship;[34] however, this article focusses on the uncertainties created by section 3 and seeks to provide guidance regarding possible interpretations that would protect South African data subjects if their personal information is processed by a non-South African responsible party. As South Africa does not yet have a body of case law or extensive scholarship on the application of POPIA, guidance will be sought in other jurisdictions, especially in the EU. The wording of sections 3 and 72 of POPIA is primarily a verbatim repetition of similar provisions in the *EU Data Protection Directive*[35] (hereafter DPD), which preceded the current GDPR. Both the DPD and GDPR are based on the same international privacy conditions that also underpin POPIA. Existing scholarship and guidelines on these matters in the context of the DPD and GDPR can therefore provide valuable insights in interpreting and understanding the South African Act.[36]

To follow the discussion it is essential to note that the terminology in the EU regulations differs from that used in POPIA. Both the DPD and the GDPR

34 See, for example, Baumann and Ismail 2021 *CILSA* 30 *et seq*.

35 *Directive 95/46/EC of the European Parliament and of the Council enacted 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 L 281/31 (DPD).

36 Baumann and Ismail 2021 *TSAR* 720-721, 723; Baumann and Ismail 2021 *CILSA* 30; Roos 2020 *CILSA* 4.

use "controller" for what we call a responsible party and "processor" where we refer to an operator.

2 Territorial scope provisions

2.1 Rationale for extra-territorial application

The main reason for extending the scope of data protection rules to outside the borders of a country is to protect the rights of its data subjects. There is not much sense in protecting the personal information of data subjects if these protective measures can be circumvented by transferring the data to a third party that is not subject to that law or if personal information is collected and processed by a responsible party that falls outside the scope of the data protection law in a country where the protection of personal information is either weak or non-existent. Where service providers in other countries process the personal information of South African data subjects, they deserve that their human rights to privacy and identity enjoy protection similar to that in their own country.

2.2 Section 3: General

Section 3(1) states:

> (1) This Act applies to the processing of personal information-
>
> (a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and
>
> (b) where the responsible party is-
>
> (i) domiciled in the Republic; or
>
> (ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

It must be noted that POPIA applies only where personal data are entered into a record. It is also necessary to point out that "processing";[37] "personal

37 "Processing", as used in the context of the Act, is a broad concept that is defined in s 1 as: "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including- (*a*) the collection, receipt, recording, organization, 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".

information"[38] and "record"[39] are defined very widely and non-exhaustively in section 1 to ensure that a data subject's constitutional right to privacy is best protected.

Paragraph (b) of section 3(1) deserves closer analysis as this paragraph requires a territorial connection for the Act to apply.

2.3 Section 3(1)(b)(i)

POPIA's point of departure is that the responsible party (or data controller) must be domiciled in the Republic. A responsible party is "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[40] This means that any responsible party who is in the Republic with the intention of being here indefinitely will fall within the scope of the Act. Apart from natural persons who are resident in the Republic for an indefinite period of time, it includes companies registered or incorporated in the Republic, business entities established or formed in South Africa, and those who have their central management and control in South Africa.[41]

As against the EU data protection regulation, the DPD and the current GDPR do not require *domicilium* or residency *per se* but that "the activities of an establishment of the controller" must take place in the territory of an EU Member State.[42] According to the ECJ, this involves the actual pursuit of an activity through a fixed establishment for an indefinite time.[43] This is

---

38 Section 1 of POPIA lists eight different types of information which are to be included in the definition but does not purport to serve as a *numerus clausus*. De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.1.1 categorises personal information as identifiers, biometric information, demographic information, contact details and location, financial information, background information, behavioural information, correspondence, opinions about data subjects, and "what is in a name".

39 Section 1 of POPIA states that "record" includes writing on any material, information produced recorded or stored by means of tape-recorder, computer equipment or other devices, labels, marking or writing that identify or describe anything that it is a part of books, maps, plans, graphs or drawings, or devices that can embody or reproduce images such as photographs, films, negatives or tapes.

40 Section 1 of POPIA.

41 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.4.1.

42 Article 4(1)(a) of the DPD; Art 3(1) of *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)* OJ L 119/1 (GDPR). Art 3(1) of the GDPR also extends this requirement to processors.

43 *R v Secretary of State for Transport (Ex parte Factortame)* (Case C-221/89) [1991] ECR I-3905 para 20. The GDPR does not define "establishment" but Recital 22 refers to the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect. This is identical to Recital 19 of the DPD.

not the place where the technology used to support the website of a company is situated or the place at which the website is accessible, but the place where the controller pursues its activity.[44] In other words, there must be a territorial link between the activities of the establishment of a controller and a Member State.

In *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*[45] (hereafter *Google Spain*) the Court had to construe the rules concerning the territorial scope of the DPD in the context of processing carried out by Google in the territory of a Member State. It held that in this case the processing of personal information had been undertaken by a search engine operated by an undertaking established outside the EU but that it had another establishment in an EU Member State which provided a territorial link with the EU as required by Article 4(1)(a) of the DPD (now Article 3(1) of the GDPR). The Court stated that the activities of the establishment in Spain in the form of selling and promoting advertising and marketing space were inextricably linked to those of the operator of the search engine in the USA as the activities in Spain allowed the search engine to be economically viable. In *Google LLC v Commission nationale d' l'informatique et de libertés (CNIL)*[46] (hereafter *Google LLC*), the Court also held that the operation of a search engine in a third country that was inextricably linked with an establishment in the EU meant that the DPD and GDPR would be applicable. The ECJ furthermore ruled that an establishment extends to any effective activities exercised through stable arrangements for an indefinite period which is to be determined on a case-by-case basis, especially in the case of online activity.[47] The European Data Protection Board (EDPB) Guidelines,[48]

---

44 Recital 19 of *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce)* [2000] OJ L 178/1; Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 8; Baumann and Ismail 2021 *CILSA* 11.

45 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12) [2014] ECLI:EU:C:2014:317 (*Google Spain*).

46 *Google LLC v Commission nationale d' l'informatique et de libertés (CNIL)* Case C-507/17 [2019] ECLI:EU:C:2019:722 para 51.

47 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabaság Hatóság (NAIH)* (Case C-230/14) [2015] ECLI:EU:C:2015:639 (*Weltimmo*) para 28 *et seq.* The ability to access a website from a particular place will not suffice, see *Verein für Konsumenteninformation v Amazon EU Sàrl* (Case C-191/15) [2016] ECLI:EU:C:2016:612 para 75 *et seq*. Recital 19 of the DPD also excludes the place where a server that supports the website is located. Also see Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 8.

48 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 6-8. See also Baumann and Ismail 2021 *CILSA* 12.

therefore, note that the case law departs from a more formalistic approach that would otherwise restrict the interpretation of the term establishment to a place of registration or incorporation.[49]

This raises the question whether the scope of the EU territorial rule is broader than that of section 3(1)(b)(i) of POPIA. Is the South African rule restricted to the principles of incorporation, management or control, or can it include a place of business? Can businesses or companies that conduct business operations in the Republic by having a physical presence in the RSA or in the online environment by making use of an address in the RSA on their website fall under the territorial scope of section 3(1)(b)(i) if they are not incorporated or controlled from the Republic? There is no real clarity on this aspect. Although most sources do not deal with this question at all, some scholars seem to suggest that this would be possible,[50] while others argue that it is unlikely that the courts would expand the established meaning of domicile.[51] Section 3(3) requires that the Act be interpreted in line with its purpose as set out in section 2, namely to regulate the processing of personal information by protecting the rights of the data subject on the one hand and the right to the free flow of information on the other hand. The intention, therefore, is to make sure that responsible parties do not escape their duties by moving their processing activities abroad. Where domicile is used in connection with natural persons, the focus is on the intention of such a person to reside in a particular place indefinitely; it does not, for example, require citizenship. By analogy one could therefore argue that engaging in continuous business activities in the Republic with the intention of doing so for an indefinite time should be sufficient to establish a territorial link and that it should not be restricted to a place of registration, management or control. It is therefore submitted that similar to the position in the GDPR, having a branch office, an employee or a representative in the Republic could be regarded as having a stable arrangement if that is inextricably linked to the processing of personal data outside the Republic, and that this would suffice for the purposes of section

49 For example, *Google Spain* para 53; *Weltimmo* para 25.

50 De Stadler and Esselaar *Guide to the Protection of Personal Information Act* 6.

51 Baumann and Ismail 2021 *CILSA* 31-32 argue that the express wording of the Act suggests otherwise. Their argument is that the Constitutional Court does not support the use of ECJ case law when such an interpretation would deviate from the express meaning of the words used in the statute. They derive authority for their opinion from the judgment in *Competition Commission of South Africa v Media 24 (Pty) Ltd* 2019 5 SA 598 (CC) 655 para 185. However, it is not a foreign concept to use international law to interpret uncertainties and gaps in our law. The Constitution provides for international law to be used to interpret South African law (s 233 of the Constitution). Moreover, the Preamble to POPIA states that the Act seeks to regulate the processing of personal information "in harmony with international standards". It is therefore submitted that an extended interpretation would not deviate from the express meaning of s 3(1)(b)(i) and would therefore not fall into the category of cases against which Theron J warned in the *Media 24* judgment.

3(1)(b)(i). A local address on a website or the ability to access a website from the Republic, on the other hand, might not be enough unless it is the address of a local branch, or if another stable arrangement and effective activity in the Republic can be established, even if that is in relation to a mere online activity. In the latter case, that will be determined in the light of the nature of the economic activities and the services offered in the Republic, especially if that is an exclusively online service. For example, a local office of a non-South African company operating an e-commerce website processes personal information for marketing purposes in South Africa. The processing of personal information can serve to make the e-commerce website profitable and could therefore be considered as a processing activity that will be subject to POPIA by virtue of section 3(1)(b)(i).[52] The EDPB Guidelines suggest adopting a balanced approach that cautions against a too restrictive interpretation but at the same time also against a too broad interpretation.[53]

This highlights a further shortcoming in POPIA, namely that it does not provide for instances where non-South African parties market or sell products in South Africa. Article 3(2) was introduced into the GDPR because of concerns that the DPD failed to provide sufficient protection where data is processed or stored outside the EU. This section applies to processing activities by data controllers or processors who do not have an establishment in the EU but where goods or services are offered to data subjects in the EU (Article 3(2)(a)),[54] or where they monitor the behaviour of data subjects in the EU (Article 3(2)(b)). Despite the introduction of this provision, it seems that the courts rather apply the approach taken in the *Google Spain* case based on the requirement in Article 3(1), namely the location of the activities of a controller or processor, before relying on Article 3(2) and that the latter article is mostly added as an afterthought.[55] POPIA does not contain a provision similar to Article 3(2) of the GDPR, and by extending the interpretation of section 3(1)(b)(i) of POPIA to cover these

52 Example derived from EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 8-9.

53 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 7. An inextricable link between the data processing activities of the responsible party outside the EU and the activities of a local establishment in the EU as well as revenue raising in the EU by a local establishment that is inextricably linked to the processing activity are factors that can be considered to determine whether the processing is carried out in the context of a responsible party's establishment in the Union.

54 According to Recital 23 of the GDPR, in order to determine whether a controller is offering goods or services to data subjects in the Union, it must be established whether "it is apparent that the controller envisages offering services to data subjects in one or more Member States in the Union". Obviously, that is not easy to determine and it would depend on the circumstances; factors such as language and currency can play a role here.

55 Kuner 2021 https://ssrn.com/abstract=3827850 13.

instances one would be able to fill this gap. However, from a South African perspective, it is important to take note of Article 3(2) of the GDPR as it brings all South Africans who offer goods or services in the EU under the scope of the GDPR when they process or monitor the personal data of EU data subjects. For the most part, compliance with POPIA will suffice as the provisions of the Act and the GDPR largely overlap, but it is important to note that the GDPR contains provisions where the duties of a responsible party exceed those required by POPIA.[56] Moreover, Article 3(1) of the GDPR extends the establishment criterion to processors (or operators as they are called in POPIA), which casts the net wider than is presently the case in South Africa.[57] This might be an additional shortcoming of our section 3(1)(b) as formulated currently.

POPIA does not require that the processor or operator must be physically present in South Africa at the time of processing but only that there must be a territorial connection established with the Republic, based on the concept of the *domicilium* of the responsible party. Therefore, if the personal information of a South African data subject is processed outside the borders of the Republic, the question would be whether that person is acting on behalf of a responsible party who is domiciled in the Republic. An employee of a business or company is not a responsible party as the business or company for whom it works determines the purpose and means of processing.[58] However, if the business or company is domiciled in South Africa, an employee can process the data remotely and the act of processing will be regulated by POPIA.

Moreover, once the territorial condition is met, the location of the means of processing is not important. For example, if personal information is stored on a server or other storage medium outside the Republic but the responsible party who determined the means for the processing is domiciled in the Republic, the processing of such information still must take place in accordance with the conditions set out in POPIA. This is due to the territorial link between the responsible party and the Republic. The same would apply if a responsible party domiciled in South Africa were to make use of an operator or processor situated outside South Africa.[59]

---

56 See, in general, Roos 2020 *CILSA* 1-37.

57 POPIA regulates the position of operators in ss 20 and 21. This is largely based on the contract between the responsible party and the operator.

58 The employee does not act as an operator either. See s 1 of POPIA for the definition of "operator", which clarifies that an operator also acts on behalf of the responsible party but, unlike an employee, does not act under the direct authority of the responsible party but in terms of a contract or mandate.

59 In these circumstances the responsible party must comply with s 72 of POPIA regulating data transfers out of the country. This section will be discussed in part II of this article. As storage is also a form of processing, the server could also be a third-party operator for the purposes of s 72.

Furthermore, the Act does not require that the data subject must be a South African citizen or be physically present or resident in the Republic as the Act focusses on bringing the party who is responsible for determining the purpose and means of the processing under its scope of application. Similar to the South African act, its European counterparts do not require that the data subjects must be EU citizens or physically present or resident in the EU.[60]

2.4 Section 3(1)(b)(ii)

Section 3(1)(b)(ii) provides for cases where the responsible party is not domiciled in the Republic but there is still a connection with the Republic in that the responsible party makes use of a means of processing that is located in South Africa. Therefore, unless the processing falls within one of the exceptions set out in sections 6 or 7, POPIA will apply to a non-South African responsible party if it makes use of an automated or non-automated means of processing in South Africa.

It is necessary to first define the notion "automated or non-automated means of processing". Section 3(4) defines automated means of processing as "any equipment capable of operating automatically in response to instructions given for the purpose of processing information". This indicates that a "means of processing" refers to equipment used to conduct the processing of personal information, which can operate automatically. The Act fails to define it any closer, probably because no definition would be able to keep up with the technological development and would become unnecessarily restricted. It does not define non-automated means either, but the Act requires that information so collected must be recorded in a filing system,[61] which is not the case for automated processing. Non-automated means therefore refers to the manual processing of personal information.[62] The only exception, as indicated by section 3(1)(b)(ii), is a means of which the sole purpose is to act as a mere conduit to transfer or forward information through the Republic. Physical equipment used for transferring information such as telephone lines, cables and other connections used to convey or forward information, therefore, would not be included.[63] Servers situated in South Africa through which information moves when passing

60 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 10.

61 Section 3(1)(a) of POPIA.

62 Baumann and Ismail 2021 *CILSA* 33; Papadopoulos and Snail ka Mtuse *Cyberlaw@SA IV* para 10.3.6.3.2.

63 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9.

from one country to another country are excluded as well.[64] A South African textbook on information and communications technology law, however, opines that "the Internet will fall within the definition of fully automated processing".[65] Although the Internet is a means of processing, its intangible nature can complicate the issue as section 3(1)(b)(ii) requires that the means of processing must be located in the Republic to establish the territorial connection needed for POPIA to apply.

The online environment creates specific challenges. Where a data subject concludes an online transaction via a website that they access in the RSA, it is not always possible to ascertain where the website is located. Domain names do not always contain geographical elements, and even if they do, that does not automatically mean that the website is hosted on a server in that country. When one considers this example from the viewpoint of POPIA, it is clear that if the responsible party is domiciled outside the Republic, such as where the vendor is registered in another country, and there are insufficient activities of an establishment in the Republic, section 3(1)(b)(i) will not apply. However, jurisdiction could perhaps be found based on section 3(1)(b)(ii). Again, guidance can be sought in the EU privacy regulations which have informed the POPIA, more specifically Article 4(1)(c) of the DPD.[66] A working document by the Article 29 Data Protection Working Party, the predecessor of the current EDPB,[67] deals with the requirement relating to "equipment automated or otherwise situated on the territory of a Member State to process personal data".[68] Previous drafts of Article 4, and non-English versions of the Directive, used the word "means" instead of the word "equipment". For interpretative purposes, one can therefore replace the word "means" in the counterpart section 3(1)(b)(ii) of POPIA with automated or non-automated "equipment". The working document mentions personal computers, terminals or servers as examples of equipment that can be used for processing operations.[69] Similar to the view

64 SALRC 2009 https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf 403; De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.1.2.

65 Roos "Data Privacy Law" 478.

66 Article 4 of the DPD delineated its territorial scope under the heading "national law applicable". This provision was to prevent data processors and data controllers evading their responsibilities by relocating their establishments outside the EU.

67 The EDPB is a group of European data protection authorities (DPAs).

68 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf.

69 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9. Note that the servers referred to here are those used for hosting or storage (processing) purposes and should be distinguished from servers merely functioning as conduits for the passing of information.

of South African scholars,[70] it excludes telecommunications networks, as these are equipment merely used for the transportation of Internet communications.[71] The working document clarifies that the controller (the responsible party) must determine the way the equipment works and must make the decisions concerning the purpose, nature and substance of the data to be processed, and how the processing is to take place. This involves an activity undertaken by the controller with the intention of processing personal information and not merely any use of equipment in that location.[72] Local commentators confirm this requirement for the purposes of section 3(1)(b)(ii).[73] Therefore, if a responsible party uses a server located in South Africa to store or host information, irrespective of where the data was collected, this could qualify as a means of processing[74] as envisaged by section 3(1)(b)(ii). Similarly, if a non-South African responsible party collects information through an automated means located in the Republic, POPIA will apply to the processing of such information irrespective of whether the data is processed inside or outside the country.[75] The EU working document, furthermore, states that where the website installs cookies[76] on a data subject's device, the location of the device can determine a territorial link with an EU Member State (or in our case, the Republic).[77] JavaScript, ad banners and other comparable technology are further examples mentioned.[78] Whether the use of an operator in the Republic can constitute the necessary territorial link as a means of processing is questionable.[79]

Although the ECJ was asked to opine on the applicability of Article 4(1)(c) of the DPD to instances where a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in

---

70 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.1.2.

71 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9.

72 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9.

73 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.4.2.

74 The definition of "processing" includes the storage of information.

75 Where data so collected are transferred out of the country, it is questionable whether the data transfer rule of s 72 of POPIA will apply. The application of this section would depend on interpreting both s 3(1)(b)(ii) and s 72's requirement of "a responsible party in the Republic" extensively. See part II of this article for a discussion of this matter.

76 A text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country.

77 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 10-11.

78 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 11-12.

79 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.4.2 is uncertain on whether an operator in the Republic will fall under s 3(1)(b)(ii).

a Member State, and where a website, using a domain name pertaining to a Member State, arranges for searches and the results thereof to be based on the language of the Member State, the Court failed to address these matters.[80] There is therefore still no clarity on these examples. However, it is safe to assume that where a data subject uses a device such as a personal computer or smart phone located in the Republic, that would normally provide the necessary territorial link. This would furthermore include devices, apparatus, sensors or software located in the Republic that support the Internet of Things. Personal data that is collected through these devices, with or without the knowledge of the data subject, could therefore be covered by this interpretation of section 3(1)(b)(ii).

Ownership is not a prerequisite for the operation of this provision; neither the responsible party nor the data subject must be the owner of the equipment being used to process the personal data. The guiding principle here is the ability to exercise control over the equipment – it does not have to be full control but the equipment must be at the disposal of the responsible party.[81] Moreover, where personal information is available in records that are publicly available on the Internet, POPIA will not find application as no control is exercised by a responsible party over the equipment because the records are publicly available.[82]

Therefore, if a data subject in South Africa accesses a non-South African website on a smart phone, and a cookie is installed on the device,[83] the automatic means of processing is located in the Republic as the device on which the cookie is installed is situated here. Consequently, the responsible party will fall under the territorial scope of the POPIA as it exercises some form of control over the means of processing via the cookie (text-file). The connecting factor is dependent on the location of the device and not on ownership thereof. However, on a literal reading, if a South African data subject accesses the same website on his smart phone while he is outside the Republic on holiday or on a business trip, there is no territorial link with the Republic. This reading could of course give rise to anomalies. For example, what if the data subject now returns to the Republic and the means of processing that was installed outside the country continues to process the personal information of the data subject after she has returned to the country? Similarly, what if the data subject previously accessed a website while in the Republic and a cookie was installed at that time that continues

80 See *Google Spain* para 20.

81 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9; De Stadler *et al Over-thinking the Protection of Personal Information Act* para 3.2.4.2.

82 Also see s 12(2)(a) of POPIA, which states that publicly available data is to be treated as an exception to the conditions of lawful processing.

83 Section 18 of POPIA requires that the data subject is to be informed of the cookie.

to process data when the data subject is outside the country? Furthermore, non-South African data subjects may access the website of a non-South African data controller during their stay in South Africa, and in this way, their personal data may be processed by an automatic means of processing located in the Republic.

The EU Working Party's working document notes that one has to be cautious when interpreting territorial provisions and only apply them if necessary and where there is a reasonable degree of enforceability.[84] POPIA is primarily aimed at protecting the rights of South African data subjects but it is not limited to South Africans. Furthermore, the Act reaches further than processing activities undertaken on South African soil. The extra-territorial reach of POPIA is not completely foreign to South African law as the *Electronic Communications and Transactions Act*[85] and the *Consumer Protection Act*[86] both provide for the protection of South Africans beyond the country's borders by extending the scope of the application of these statutes outside the Republic. Naturally, if these matters are not heard in a South African court, it will not be that easy or straightforward to enforce these laws.[87] The GDPR tries to address this issue by requiring the appointment of a representative in the EU in cases where Article 3(2) applies.[88] Article 3(2)(b) of the GDPR was specifically introduced into EU law to address the shortcomings in the DPD in cases where a non-EU controller or processor monitors the behaviour of a data subject in the Union, which previously necessitated an extensive interpretation of Article 4(1)(c) of the DPD. According to scholarly opinion, this has not proven so far to have any real effect as the courts mostly try to make the connection on the basis of Article 3(1) of the GDPR to find jurisdiction at the place of the establishment.[89]

3 Conclusion

If read in conjunction with the purposes of POPIA set out in section 2, it is clear that the Act aims to protect the rights of the data subject as far as is

84 Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf 9.

85 Section 47 of the *Electronic Communications and Transactions Act* 25 of 2002.

86 Section 5 of the *Consumer Protection Act* 68 of 2008.

87 Forum selection and choice of law clauses can complicate these matters even further.

88 Article 27(1) of the GDPR. The closest to this in POPIA is an information officer who is to maintain documentation of all processing activities under the responsibility of the responsible party as envisaged by s 17 of POPIA in line with ss 14 or 52 of the *Promotion of Access to Information Act* 2 of 2000 (PAIA). In regard to the accessibility of multinational entities based outside the Republic, see specifically Information Regulator 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf para 5.2.

89 Kuner 2021 https://ssrn.com/abstract=3827850 12-13.

possible in a balanced approach; therefore, the territorial scope of the Act must be interpreted in a manner that facilitates and fulfils this purpose. However, the discussion has shown that the wording of section 3(1)(b) is open to different interpretations. It is suggested that the interpretation of section 3(1)(b)(i) must not follow a mere formalistic approach that restricts its scope of application to responsible parties who are incorporated or controlled in the Republic but that it must be extended to responsible parties who conduct a stable and constant activity in the Republic. This interpretation would be supported by the interpretation afforded to the comparable territorial scope provision in the DPD, and currently in the GDPR. Guidelines on how to set boundaries for such an extensive interpretation are found in the ECJ case law as well as in the official guidelines of the EDPB. Adopting a comparative approach could also assist in interpreting the notion of automated means of processing in section 3(1)(b)(ii) POPIA. An extensive interpretation is necessitated here to achieve one of the goals of a territorial scope provision, namely to extend the ambit of a data protection law to non-resident responsible parties. In the absence of an extensive interpretation the effectiveness of the POPIA and the complete protection of data subjects' rights that the Act seeks to ensure will not be reached.[90] Section 3(1)(b)(ii) aims to bring the processing activity of a non-South African responsible party under the scope of the data protection law rather than the responsible party itself as a natural or juristic person. It will depend on the circumstances of the case whether the activity concerned will give rise to a territorial connection with the Republic.[91] Nonetheless, no requirement is set that the processing activity must take place in the Republic; a territorial connection between the responsible party and the Republic will suffice.[92] However, if the responsible party transfers the data out of the country to be processed elsewhere the requirements of the data transfer provision of section 72 must be complied with.[93] Moreover, if the information is to be processed by an operator, POPIA also requires a contract between the responsible party and the operator setting out the duties of that party as per the Act.[94]

The comparative analysis has furthermore shown that POPIA has shortcomings, which also existed in the DPD, on which our law is based. In the EU these shortcomings were subsequently addressed by way of the GDPR, which specifically extends its territorial scope provisions to

90 This was the reason given by the court in para 58 of the *Google Spain* case for why the meaning had to be extended.

91 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 5.

92 Article 3(1) of the GDPR expressly states that the processing does not have to take place in the EU.

93 See part II of this article for a discussion of s 72 of POPIA.

94 See ss 20 and 21 of POPIA.

processors (operators) in addition to controllers (responsible parties). It also addresses the issue where data controllers outside the Union make offerings for goods and services targeted at data subjects in the EU or monitor their behaviour. This provision is especially important in the context of online websites. The GDPR furthermore tries to address the responsibility of controllers and processors without an EU establishment who fall under the GDPR because of Article 3(2) by requiring that they appoint a representative in the Union. This is to facilitate enforcement against them.[95] These are aspects that our legislature could consider when contemplating the revision of POPIA.[96] At this juncture it can be mentioned that a guidance note by the South African Information Regulator states that, to ensure the accessibility of a private body a multinational entity based outside the Republic must authorise a person in South Africa as an Information Officer.[97] In the meantime the courts are urged to interpret section 3(1)(b) extensively in order to plug the gaps so that responsible parties do not circumvent the operation of POPIA by moving their operations outside the Republic and also to bring the processing activities of non-South African responsible parties who reach into the Republic under its scope and ambit.

However, the transfer of the personal information of a South African data subject out of the Republic is not restricted to the collection and further processing thereof by responsible parties outside the country but can also occur when responsible parties in the Republic transfer such personal information to a third-party country for processing there. Part II of this article will analyse the applicable provision of section 72. The main purpose of the data transfer rule is to make sure that a data subject's personal information remains protected when transferred out of the country. In many instances the responsible party would already be subject to the scope of POPIA by virtue of section 3, which means that it would have to uphold the data protection principles of the Act in any event. However, where personal information is transferred out of the country and processed by a third party who is not automatically subject to POPIA, section 72 will make this transfer conditional on compliance with requirements that ensure that the same minimum protection afforded by the Act applies to the extra-territorial processing of a South Africa data subject's personal information.

95 Kuner 2021 https://ssrn.com/abstract=3827850 12.

96 See Baumann and Ismail 2021 *CILSA* 34-39 regarding potential amendments.

97 Information Regulator 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf para 5.2. The duties and responsibilities of Information Officers are performed in terms of POPIA and PAIA.

Bibliography

Literature

Baumann and Ismail 2021 *CILSA*
Baumann J and Ismail N "The (Extra-)territorial Scope Rules of the New European Data Protection Law from a Private International Law Perspective: A Model for South Africa?" 2021 *CILSA* 1-49

Baumann and Ismail 2021 *TSAR*
Baumann J and Ismail N "The Concept of 'Personal Information' in the Protection of Personal Information Act 4 of 2013: A Comparative Analysis from a European Perspective" 2021 *TSAR* 718-739

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

De Stadler *et al Over-thinking the Protection of Personal Information Act*
De Stadler E *et al Over-thinking the Protection of Personal Information Act* (Juta Cape Town 2021)

Hayward 2021 *UNSW Law Journal*
Hayward B "To Boldly Go, Part I: Developing a Specific Legal Framework for Assessing the Regulation of International Data Trade under the CISG" 2021 *UNSW Law Journal* 878-918

Papadopoulos and Snail ka Mtuse *Cyberlaw@SA IV*
Papadopoulos S and Snail ka Mtuse S (eds) *Cyberlaw@SA IV: The Law of Internet in South Africa* (Van Schaik Pretoria 2022)

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

Roos "Data Privacy Law"
Roos A "Data Privacy Law" in Van der Merwe DP (ed) *Information and Communications Technology Law* 3rd ed (Lexis Nexis Johannesburg 2021) 387-530

Case law

Competition Commission of South Africa v Media 24 (Pty) Ltd 2019 5 SA 598 (CC)

Data Protection Commissioner v Facebook Ireland, Maximillian Schrems (Case C-311/18) [2020] ECLI:EU:C2020:559

Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12) [2014] ECLI:EU:C:2014:317

Google LLC v Commission nationale d' l'informatique et de libertés (CNIL) (Case C-507/17) [2018] ECLI:EU:C:2019:722

Maximillian Schrems v Data Protection Commissioner (Case C-362/14) [2015] ECLI:EU:C:2015:650

R v Secretary of State for Transport (Ex parte Factortame) (Case C-221/89) [1991] ECR I-3905

Verein für Konsumenteninformation v Amazon EU Sarl Case (C-191/15) [2016] EU:C:2016:612

Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabaság Hatóság (NAIH) (C-230/14) [2015] EU:C:2015:639

Legislation

South Africa

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Cybercrimes Act 19 of 2020

Electronic Communications and Transactions Act 25 of 2002

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

International and regional instruments

Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108/1981* (1981)

Directive 95/46/EC of the European Parliament and of the Council enacted 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 L 281/31

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce) [2000] OJ L 178/1

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) OJ L 119/1

UN General Assembly *Transforming our World: The 2030 Agenda for Sustainable Development* UN Doc A/RES/70/1 (2015)

Universal Declaration of Human Rights (1948)

Internet sources

Article 29 - Data Protection Working Party 2002 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf
Article 29 - Data Protection Working Party *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites, 5035/01/EN/Final WP 56, Adopted 30 May 2002* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf accessed 30 March 2022

EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_ consultation_en_1.pdf
European Data Protection Board 2019 *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) Version 2.1 (Adopted 12 November 2019)* https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf accessed 28 April 2022

EDPB 2022 https://edpb_statement_202201_new-trans-atlantic_data-privacy_framework.pdf
European Data Protection Board 2022 *Statement 01/2022 on the Announcement of an Agreement in Principle on a New Trans-Atlantic Data Privacy Framework (Adopted 6 April 2022)* https://edpb_statement_202201_new-trans-atlantic_data-privacy_framework.pdf accessed 28 April 2022

Information Regulator 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf
Information Regulator (South Africa) 2021 *Guidance Note on Information Officers and Deputy Information Officers (1 April 2021)* https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf accessed 13 May 2022

Kuner 2021 https://ssrn.com/abstract=3827850
Kuner C 2021 *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. University of Cambridge Faculty of Law Legal Studies Research Paper Series Paper No*

20/2021, April 2021 https://ssrn.com/abstract=3827850 accessed 30 March 2022

OECD 2013 https://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm
Organisation for Economic Cooperation and Development 2013 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Revised Version 11 July 2013)* https://www.oecd.org/ sti/ieconomy/oecdguidelinesonthe protectionofprivacyandtransborder flowsofpersonaldata.htm accessed 20 March 2022

OECD 2018 https://one.oecd.org/document/TAD/TC/WP(2018)19/ FINAL/En/pdf
Organisation for Economic Cooperation and Development 2018 *Trade and Cross-Border Data Flows: Report by the Working Party of the Trade Committee (21 December 2018) TAD/TC/WP(2018)19/FINAL* https://one.oecd.org/document/TAD/TC/WP(2018)19/FINAL/En/pdf accessed 13 May 2022

SALRC 2009 https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20 and%20data%20protection2009.pdf
South African Law Reform Commission 2009 *Project 124 Privacy and Data Protection Report* https://www.justice.gov.za/salrc/reports/r_prj124_privacy %20and%20data%20protection2009.pdf accessed 28 April 2022

List of Abbreviations

CILSA	Comparative and International Law Journal of South Africa
DPA	Data Protection Authority
DPD	Data Protection Directive (EU)
EDPB	European Data Protection Board
ECJ	European Court of Justice
EU	European Union
GDPR	General Data Protection Regulation (EU)
OECD	Organisation for Economic Cooperation and Development
PAIA	Promotion of Access to Information Act 2 of 2000
POPIA	Protection of Personal Information Act 4 of 2013
RSA	Republic of South Africa
SALRC	South African Law Reform Commission
SDGs	Sustainable Development Goals

TSAR	Tydskrif vir Suid-Afrikaanse Reg
UN	United Nations
UNSW Law Journal	University of North South Wales Law Journal
USA	United States of America