The Problem of Trans-Border Information Flows in the Protection of Personal Information

M Malahleka*

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed, open access online law publications

Author

Mthuthukisi Malahleka

Affiliation

Rhodes University,
South Africa

Email

mthuthukisi@hotmail.com

Date Submitted

5 July 2022

Date Revised

12 April 2024

Date Accepted

12 April 2024

Date Published

8 August 2024

Editor

Prof W Erlank

Journal Editor

Prof C Rautenbach

How to cite this contribution

Malahleka M "The Problem of Trans-Border Information Flows in the Protection of Personal Information" *PER / PELJ* 2024(27) - DOI http://dx.doi.org/10.17159/1727-3781/2024/v27i0a14296

DOI
http://dx.doi.org/10.17159/1727-3781/2024/v27i0a14296

Abstract

Cross-border transfers of personal information have become an important integrant of international trade, global economic activities enabler and a component of digital services driver, however, they are faced with the limitations of cross-border personal information transfers and data localisation laws. Various methodologies are used to process and transfer personal information across the borders such as cloud computing. Cloud computing has grown to include more users across different countries through its transnational characteristics on cross-border personal information transfers and triggers the *Protection of Personal Information Act* 4 of 2013 (POPIA) application. POPIA seeks to promote and protect personal information when processed by public or private bodies. Personal information also forms part of privacy which is a fundamental right enshrined under section 14 of the *Constitution of the Republic of South Africa,* 1996. Therefore, the processing of personal information unlawfully across South Africa is a violation of the fundamental right to privacy and the POPIA. A comparative analysis of the provisions of the European Union (EU) General Data Protection Regulation (GDPR) on cross-border data transfers will be used to illustrate the shortcomings of section 72 of the POPIA in the cloud computing context. The GDPR has set a benchmark for international data protection standards and POPIA must comply with those standards if South Africa wants to maintain its status as part of the international information technology market.

Keywords

Cross-border data transfers; personal information; data protection; privacy; cloud computing; *Protection of Personal Information Act*; General Data Protection Regulation.

.....

1 Introduction

Cross-border transfers of personal information[1] have grown rapidly, this includes the volumes of personal information transferred globally and the commercial value attached to such transfers.[2] Cross-border data transfers have been further categorised as commercial catalysts, enablers, hallmarks of the 21st-century globalisation,[3] and a connecting network of the global economy.[4] Based on the estimations done, in 2014 cross-border data transfers added approximately $2.8 trillion to the world's Gross Domestic Product (GDP),[5] along with transfers of digital media content.[6] The use of cloud computing services by various industries across the world is one of the biggest digital drivers allowing massive cross-border data transfers and one of the most prominent emerging personal information processing[7] mechanisms in the Information Technology (IT) space. Its transnational characteristics have grown to include more users across different countries. In cloud computing, data protection and security comprise one of the legal challenges as it is outpacing its legal counterpart for now. The question is how adequate are the provisions of the POPIA in protecting cross-border transfers of personal information and whether the enacted provisions provide adequate personal information protection in a cloud computing context?

* Mthuthukisi Malahleka. LLB (UNISA) LLM (UP) LLM (RU) Cert Compliance Management (UCT). PhD Researcher, School of Law and Economics (Erasmus University Rotterdam, Netherlands) Email: mthuthukisi@hotmail.com. ORCiD: https://orcid.org/0000-0003-4564-8559. Affiliated with Rhodes University: This research is supported by the Rhodes University Postgraduate Funding Office and the University Capacity Development Program. I would like to extend my gratitude towards Rhodes University Faculty of Law for their support in obtaining funding. The views and opinions expressed in this paper are solely those of the author.

1 See s 1 of the *Protection of Personal Information Act* 4 of 2013 (POPIA) for the definition of the term "personal information".

2 Voss 2020 *Washington International Law Journal* 487.

3 Mckinsey Global Institute 2016 https://www.mckinsey.com/~/media/McKinsey/Business%/`2OFunctions/McKinsey%/`20Digital/Our%/o2OInsights/Digital%20globalizationo2OThe%20newo20era/o2ofo2Oglobal/o20flows/MGI-Digitalglobalization-Full-report.ashx; Voss 2020 *Washington International Law Journal* 487.

4 Mckinsey Global Institute 2019 https://www.mckinsey.com/~/media/McKinsey/Featured%/`20Insights/Innovation/Globalizationo2Oino20transitiono2OThe%20future%20fo20trade/o20and%20value%20chains/MGI-Globalizationo2Oin%/o20transition-The-future-of-trade-and-value-chains-Fullreport.ashx; Voss 2020 *Washington International Law Journal* 487.

5 Voss 2020 *Washington International Law Journal* 487.

6 Mckinsey Global Institute 2016 https://www.mckinsey.com/~/media/McKinsey/Business%/`2OFunctions/McKinsey%/`20Digital/Our%/o2OInsights/Digital%20globalizationo2OThe%20newo20era/o2ofo2Oglobal/o20flows/MGI-Digitalglobalization-Full-report.ashx 32; Voss 2020 *Washington International Law Journal* 487.

7 See s 1 of the POPIA for the definition of the term "processing".

Personal information forms part of privacy. Privacy is a personality right protected as a fundamental human right under section 14 of the Constitution,[8] and the *Protection of Personal Information Act* 4 of 2013 (hereinafter POPIA or the Act), which seeks to promote the protection of personal information when processed by public or private bodies.[9] Digital service providers such as cloud computing have gained much value from processing personal information and at the same time, the data subjects[10] benefit from those services.[11] These digital platforms also provide cross-border digital services for free. It is estimated that in 2017, these digital services added between $240 billion and $3.2 trillion to trade-in services worldwide.[12] These trans-border data transfers are ubiquitous in nature, especially with the Internet of Things (IoT), there are large amounts of cross-border data transfers that do not require human interaction or intervention.[13] However, the unlawful processing of personal information across the border violate the right to privacy and the provision of POPIA. This paper intends to illustrate the importance of regulating cross-border data transfers on cloud computing services to protect personal information.

A critical analysis of section 72 under chapter 9 of the POPIA which regulates cross-border data transfers with other relevant sections will be explored using a doctrinal approach. Thereafter, a comparative analysis of Chapter V of the European Union (EU) General Data Protection Regulation (GDPR)[14] on cross-border data transfer provisions will be used to illustrate the shortcomings of section 72 in the cloud computing context. The GDPR has set a benchmark on international data protection standard.[15] POPIA

---

8 The *Constitution of the Republic of South Africa*, 1996 (the Constitution). (In terms of s 14 of the Constitution, the right to privacy includes the claim not to have one's person, home, and property searched or possessions seized. Therefore, it consists of a right to protection against the unlawful collection, retention, dissemination, and use of personal information. The State must then respect, protect, promote and fulfil the rights in the Bill of Rights (including the right to privacy), hence adopting the POPIA. The right to privacy is not absolute; it is subject to limitations under s 36 of the Constitution. However, the cross-border unlawful processing of personal information through cloud computing violates the right to privacy and activates the provisions of the POPIA.)

9 See s 1 of the POPIA for the definition of the terms "public body" and "private body".

10 Section 1 of the POPIA defines "data subject" as the person to whom the personal information relates.

11 Voss 2017 *University of Illinois Journal of Law, Technology and Policy* 472.

12 Voss 2020 *Washington International Law Journal* 488.

13 Kuner *Transborder Data Flows* 3.

14 *General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons Concerning the Processing of Personal Data and the Free Movement of Such Data, and Repealing Directive 95/46/EC* OJ L 119/1 (2016) (the GDPR).

15 Roos 2020 *CILSA* 4.

must comply with the standard set by the GDPR if South Africa (SA) wants to maintain its position on the international IT market.[16] This paper will conclude with recommendations to ensure section 72 guarantees adequate data protection on cross-border data transfers through cloud computing services.

2 Contextualisation of cloud computing

Cloud computing is a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources.[17] Such resources include networks, servers, storage, applications, and services.[18] These resources are delivered through an IT platform for software and other supplementary applications provided via remote file servers across the Internet on a requirements basis.[19] They link remote computers to access remote data storage and computation services from servers located anywhere in the world instead of storing data and software on the client's hard drive.[20] Most importantly, cloud computing involves the cross-border transfer of personal information across various jurisdictions,[21] for multiple clients across the globe.[22] Examples of these cloud computing services include Google Drive, operated by Google, iCloud, operated by Apple, and Microsoft Azure.

2.1 Concerns about data protection on cloud computing services

The cross-border personal information transfers underpin a growing range of economic activities across the globe.[23] It is estimated that over 12 percent of global trade in goods and services take place through e-commerce and most of these digital platforms use cloud computing services to drive their international e-commerce services such as Amazon and Alibaba.[24] Cloud

16 Schwartz 1995 *Iowa L Rev* 487; Roos 2020 *CILSA* abstract.

17 Mell and Grance 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; Hage and Brown date unknown http://www.johnseelybrown.com/cloudcomputingdisruption.pdf.

18 Mell and Grance 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; Hage and Brown date unknown http://www.johnseelybrown.com/cloudcomputingdisruption.pdf.

19 Martin 2011 http://works.bepress.com/timothy_martin/3; Neethling, Potgieter and Roos *Neethling on Personality Rights* 367.

20 Narayanan 2012 *Chicago Journal of International Law* 783-784.

21 Preston 2008 https://www.informationweek.com/software-services/down-to-business-customers-fire-a-few-shots-at-cloud-computing.

22 Van der Merwe *et al ICT Law* 367; Carpenter 2010 *Washington Journal of Law, Technology and Arts* 2.

23 Mattoo and Meltzer 2018 *J Int'l Econ L* 769.

24 Mattoo and Meltzer 2018 *J Int'l Econ L* 770; Manyika *et al* 2016 https://www.mckinsey.com//media/McKinsey/Business%20Functions/McKinsey%2

computing has made it easy to quickly and seamlessly transfer personal information to other jurisdictions or international organisations.[25] Such massive cross-border data transfer have a negative impact on domestic regulations on privacy and data protection objectives when personal information of citizens is transferred to jurisdictions that do not provide adequate data protection instruments. In other words, this can prompt domestic lawmakers to restrict cross-border data transfers which in turn can negatively impact international trade.[26] The lack of control over the hardware of cloud computing services poses risks such as hacking, data breaches, data leaks, and the interception of data.[27] A cloud service client loses exclusive control over the personal information they upload on the cloud and will not always have enough information on how data is processed, where it is accessed, and by whom it is accessed.[28] The cloud service client may also not know all the possible security risks that the information is subject to; therefore, it may not be possible for the client to guarantee adequate security measures to protect such personal information.[29] The Internet knows no boundaries; through cloud computing services, personal information can be easily transferred to countries, third parties or international organisations without adequate data protection and security measures.

3 The need for POPIA to regulate cross-border data flows

The South African Law Reform Commission (SALRC)[30] proposed a data protection legislation for SA[31] and recommended the adoption of a legislation that met the international standards for data protection, of which they recommended the EU Directive.[32] The Directive affected countries outside the EU, such as SA, because Article 25(1) required them to provide adequate data protection standards before sending personal information from EU countries to third parties in other countries.[33] The determination of data protection adequacy was assessed in consideration of all the

ODigital/Our%20Insights/Digital%20globalization%20The%20new%2era%20f%2O global%20flows/MGIDigitalglobalization-Full-report.ashx.

25 Mattoo and Meltzer 2018 *J Int'l Econ L* 770.

26 Mattoo and Meltzer 2018 *J Int'l Econ L* 770.

27 Peterson 2012 *J Marshall L Rev* 390; Neethling, Potgieter and Roos *Neethling on Personality Rights* 366.

28 Van der Merwe *et al ICT Law* 367.

29 Van der Merwe *et al ICT Law* 367.

30 The mission of the South African Law Reform Commission (SALRC) is the continuous reform of the law of South Africa under the principles and values of the Constitution to meet the needs of a changing society operating under the rule of law.

31 SALRC *Privacy and Data Protection* para 3.2.7; Roos 2020 *CILSA* 4.

32 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals Concerning the Processing of Personal Data and the Free Movement of Such Data* OJ L281/31 (1995) (the Directive).

33 Roos *Law of Data (Privacy) Protection* 226-235; Roos 2020 *CILSA* 2.

circumstances pertaining to data transfer operations. Alternatively the assessment was conducted based on the presence of the rules of law, including general and sectoral, adopted in that country in question as well as the security measures and professional rules complied with in that specific country.[34] The GDPR later replaced the same Directive that the POPIA was built on.[35] The GDPR has a similar requirement under Article 44. As a result, third countries (including SA) must ensure that they provide data protection that meets the GDPR standard.[36] Therefore, POPIA makes such provisions under section 72,[37] regulating cross-border transfers of personal information to countries that do not provide adequate data privacy protection laws. The common standard for cross-border data transfer is an adequate level of data protection in the receiving country, however, there are exceptions, such as contracts and the data subject's consent.[38]

4 The scope of the paper

The discussion in this paper is limited to the provisions of the GDPR and the POPIA on cross-border transfers of personal information.[39] The provisions dealing with definitions of certain concepts, the legal bases for lawful data transfers, the principles of data protection, the rights of subjects, restrictions on onward transfers, and the enforcement mechanisms will be analysed and compared.[40] The discussion is also restricted to the content principles of concepts and the legal bases for lawful cross-border data transfers. A requirement for a finding of adequate protection of personal information on cross-border data transfers is the presence of certain basic data-protection concepts such as appropriate safeguards,[41] which may include binding corporate rules in the third country's data protection legal system. The concepts do not have to be identical to the provisions of the GDPR but must be consistent with it.[42]

For clarity for the discussion in this paper, in the POPIA, a "data controller",[43] as referred to under the GDPR, is called a "responsible party". Even though POPIA uses different terminology from the GDPR, the definition is similar.

34 Article 25(2) of the Directive.
35 The commencement date of the GDPR was 25 May 2018.
36 Article 44 of the GDPR.
37 Neethling, Potgieter and Roos *Neethling on Personality Rights* 406.
38 Neethling, Potgieter and Roos *Neethling on Personality Rights* 406.
39 Mainly Chapter 9 of the POPIA and Chapter V of the GDPR.
40 Article 29 Data Protection Working Party 2017 https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp254_rev01.pdf; Roos 2020 *CILSA* 8.
41 Article 46 of the GDPR.
42 Article 29 Data Protection Working Party 2017 https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp254_rev01.pdf 5.
43 See Art 4(7) of the GDPR for the definition of the term "controller".

The GDPR uses the term "personal data"[44] referring to information or data relating to a natural person identified or identifiable either directly or indirectly, while the POPIA uses the term "personal information". The examples of personal information provided under section 1 of the Act are very much identical to examples furnished under the GDPR for "personal data" under Article 4(1).

4.1 POPIA's scope

POPIA is applicable to responsible parties[45] domiciled or not domiciled in the Republic[46] who make use of automated and in certain circumstances non-automated means within the Republic to process personal information.[47] Suppose the processing involves activities of certain public institutions, such as those involved in combating terrorism, crime, and money laundering, to safeguard against and to prevent any threats to public safety, in that case, they are excluded from the Act.[48] The Act also excludes the processing of personal information by a natural person during any household activity or any processing of personal information that can be classified as purely personal activity.[49] The Act further regulates the processing of personal information that forms part of a filing system or is entered in a record to form a part thereof,[50] by introducing specific conditions to establish minimum requirements for processing personal information.[51] The Act also entails balancing the constitutional values of democracy while allowing the free flow of personal information for economic and social activities in harmony with international data protection standards.[52] POPIA's provisions do not apply only to natural persons,[53] but also to juristic persons.[54] This implies that juristic persons also have the right to privacy.[55] Section 2(1)(a)(ii) makes provisions for the protection of

44 See Art 4(1) of the GDPR for the definition of the term "personal data".
45 See s 1 of the POPIA for the definition of a "responsible party".
46 Section 1 of the POPIA defines "Republic" as the Republic of South Africa.
47 Section 3(1)(*b*) of the POPIA.
48 Section 6(1)(*c*)(i) of the POPIA.
49 Section 6(1) of the POPIA.
50 Sections 3(1)(*a*) and 73 of the POPIA.
51 Chapter 3 of the POPIA; Millard and Bascerano 2016 *PELJ* 3; Allan and Currie 2007 *SAJHR* 573.
52 See the Preamble, sections 2, 3, and 72 of the POPIA; SALRC *Privacy and Data Protection*; Roos *Law of Data (Privacy) Protection* 477-479; Roos 2020 *CILSA* abstract; Neethling, Potgieter and Roos *Neethling on Personality Rights* 281*;* Neethling 2012 *THRHR* 245.
53 See s 1 of the POPIA for the definition of the term "natural person".
54 See s 1 of the POPIA for the definition of the term "juristic person".
55 *Universiteit van Pretoria v Tommie Meyer Films* 1977 4 SA 376 (T) para 456; *Dlomo v Natal Newspapers (Pty) Ltd* 1989 1 SA 945 (A) paras 952E-953D; see also *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 4 SA 293 (A); s 8(4) of the Constitution, which reads that: "a juristic person is entitled to the rights in the Bill of

important interests such as the free flow of personal information within and across the borders of the Republic, therefore, intentional and negligent wrongful processing of personal information across borders of SA, falls within POPIA's scope.

4.2 GDPR's scope

The GDPR make provisions in relation to the protection of fundamental rights and freedoms of natural persons concerning the processing of their data and the free movement of such personal data.[56] The transfer of personal data within the EU community is not prohibited or restricted.[57] The provisions of the GDPR apply to the processing of personal data either wholly or partly through automated means, in other words using digital platforms such as cloud computing intended to be part of a filing system or to form part of a filing system. Personal data processed through non-automated means such as manual documents in a file also intended to be part of a filing system or to form part of a filing system also fall within the provisions of the GDPR.[58] The provisions of the GDPR do not apply to any personal data processed in the course of an activity that falls outside the scope of EU law.[59] If the processing is done by the EU Member States while executing activities that fall within the scope of Chapter 2 of Title V of the Treaty on European Union such processing falls outside the scope of the GDPR.[60] Personal data processed by a natural person in the course of a solely personal activity or in other circumstances household activity is excluded from the provisions of the GDPR.[61] Provisions of the GDPR will also not be applicable if the processing of personal data is carried out by competent authorities to prevent, investigate, detect or prosecute criminal offences or execute criminal penalties, including safeguarding against and preventing threats to public security.[62]

Personal data processed within the confines of the activities of an establishment, in other words a controller or a processor in the EU territory, regardless of whether the processing takes place within the EU territory or

Rights to the extent required by the nature of the rights and the nature of the juristic person". "There is some authority that because juristic persons are not bearers of human dignity, their privacy rights may be attenuated"; *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit* 2001 1 SA 545 (CC) para 18.

56 Article 1(1) of the GDPR.
57 Article (1)(3) of the GDPR.
58 Article (2)(1) of the GDPR.
59 Article 2(2)(*a*) of the GDPR.
60 Article 2(2)(*b*) of the GDPR.
61 Article 2(2)(*c*) of the GDPR.
62 Article 2(2)(*d*) of the GDPR.

not the provisions of the GDPR will be applicable.[63] Processing of personal data by a controller not established in the EU, even if they do not have an establishment in the EU triggers the application of the GDPR provisions. This relates to where processing activities pertain to the offering of goods or services,[64] regardless of whether a payment of the data subject is required, to such data subjects in the EU.[65] This provision also applies to monitoring of data subjects' behaviour as far as it takes place within the EU[66] and further applies to processing personal data in the EU, but in a place where EU Member State law applies under public international law.[67] Processing of any personal data such as the contact details of a legal person, their name as well as the form of that particular legal person, falls outside the GDPR's scope.[68] In other words, a legal person's data is not protected under the GDPR. Processing of the personal data of a deceased person also falls outside the GDPR's scope.[69]

4.3 Comparison

The scope of the GDPR and the POPIA is similar, as highlighted above; however, there are differences in terms of terminology and their broadness in the application. POPIA recognises that juristic persons may, in certain circumstances, be entitled to the right to privacy and a good name.[70] On the other hand, the GDPR does not provide juristic persons with data protection. Under the GDPR, the location of the responsible party is not a determining factor as in the POPIA; as long as the data subject is an EU citizen or resident, the GDPR will apply and that is territorial jurisdiction.[71] POPIA applies only to personal information processed within the borders of SA. This is a challenge for the POPIA as the responsible party can process personal information while domiciled anywhere in the world using cloud computing services. Therefore, personal information processed outside SA using cloud computing services falls outside POPIA's scope as the affected

63 Article 3(1) of the GDPR.
64 Article (3)(2) of the GDPR.
65 Article 3(2)(*a*) of the GDPR.
66 Article 3(2)(*b*) of the GDPR.
67 Article 3(3) of the GDPR.
68 See other legislative acts such as *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data* OJ L 8/1 (2001).
69 Recital (27) of the GDPR.
70 Neethling, Potgieter and Knobel *Neethling-Potgieter-Visser Law of Delict* 342-345; Roos 2020 *CILSA* 9.
71 Neethling, Potgieter and Knobel *Neethling-Potgieter-Visser Law of Delict* 342-345; Roos 2020 *CILSA* 9.

data subjects will have to rely on other legal remedies such as the common law and constitutional law data protection mechanisms.

The GDPR make provisions for the processing of personal data by controllers who can be natural or legal persons.[72] On the other hand, POPIA eliminates natural persons from the scope of being responsible parties and only regulates personal information processed by public and private bodies.[73] Both legislations make provisions that make it possible for personal information to flow freely for economic and social activities in harmony with the international data protection standards,[74] therefore, recognising and regulating cross-border data flows through cloud computing services. The EU is not the only jurisdiction that has adopted data protection legal framework with extraterritorial effect. The following section analysis the extraterritorial provisions of the POPIA on cross-border data transfers.

5 Trans-border data flows under the POPIA

Any public or private body in SA is prohibited in terms of the Act to transfer or initiate the cross border transfer of personal information using cloud computing services to another recipient who is domiciled in another country.[75] Such a transfer can only take place provided the recipient operates or is subject to data protection laws[76] that include binding corporate rules.[77] Binding corporate rules are policies within a group of undertakings.[78] The term "group of undertakings" means a controlling undertaking and its controlled undertakings,[79] which a responsible party should strictly adhere to.[80] It is the type of strict policies applicable when a responsible party or operator within the same group of undertakings in a foreign country is a recipient of personal information transferred across the SA borders.[81] The laws in the receiving country must further include binding agreements that provide adequate data protection[82] and endorse fundamentals for processing personal information in a reasonable manner

72 Article (4)(7) of the GDPR.
73 The preamble of the POPIA.
74 See the preamble, ss 2, 3, and 72 of the POPIA; Art 1(1) of the GDPR; SALRC *Privacy and Data Protection*; Roos *Law of Data (Privacy) Protection* 477-479; Roos 2020 *CILSA* abstract; Neethling, Potgieter and Roos *Neethling on Personality Rights* 281*;* Neethling 2012 *THRHR* 245.
75 Section 72(1) of the POPIA.
76 Section 72(1)(*a*) of the POPIA.
77 Section 72(2)(*a*) of the POPIA.
78 Section 72(2)(*a*) of the POPIA.
79 Section 72(2)(*b*) of the POPIA.
80 Section 72(2)(*b*) of the POPIA.
81 Section 72(2)(*b*) of the POPIA.
82 Section 72(1)(*a*) of the POPIA.

as outlined in the POPIA.[83] It is also a requirement that the processing principles must be identical to the conditions[84] for the processing of personal information of a data subject in a lawful manner regardless of whether the data subject in question is a natural person or a juristic person.[85] Concepts and contents of the binding corporate rules or agreements should be identical to the provisions of section 72 of the POPIA.[86] The foreign or receiving country should provide sufficient data privacy protection laws before the onward personal information transfers also known as further transfers can take place.[87]

5.1 Data subject's consent

Section 72(1)(b) read with sections 4,[88] 5,[89] and 11(1)(a)[90] in particular, provide that before a cloud computing user or operator processes personal information, consent must be obtained from the data subject. This also applies to personal information processed across the borders of SA. The provisions are in line with the Act's purpose and inconsonant with the values of the Constitution, promoting democracy,[91] and openness to progress economically and socially.[92] The objectives of the POPIA on cross-border data transfers are within the information society framework and require eliminating obstacles that might detour the free movement of personal information, provided consent is obtained from data subjects before processing takes place.[93]

5.2 Exclusions

The POPIA does not prohibit the processing of personal information across SA borders in order to perform contractual obligations between the data subject and the responsible party.[94] Pre-contractual measures or initiatives taken upon a request made by the data subject are excluded from the provisions of the Act.[95] POPIA's provisions do not apply if the personal information transferred is required to conclude or perform contractual

83 Section 72(1)(*a*)(i) of the POPIA.
84 Chapter 3 of the POPIA.
85 Section 72(1)(*a*)(i) and (ii) of the POPIA.
86 Section 72(1)(*a*)(ii) of the POPIA.
87 Neethling, Potgieter and Roos *Neethling on Personality Rights* 407.
88 Section 4 of the POPIA deals with the lawful processing of personal information.
89 Section 5 of the POPIA provides the rights of the data subjects.
90 Section 11(1)(*a*) of the POPIA provides: "Consent, justification, and objection —(1) Personal information may only be processed if; (*a*) the data subject or a competent person where the data subject is a child consents to the processing;".
91 The preamble of the POPIA.
92 Section 11(1)(*a*) of the POPIA.
93 Section 11(1)(*a*) of the POPIA and see Gen N 309 in GG 44411 of 1 April 2021.
94 Section 72(1)(*c*) of the POPIA.
95 Section 72(1)(*c*) of the POPIA.

obligations,[96] in the data subject's interest or if such transfer is at the data subject's benefit.[97] The responsible party could evade liability if it's impossible to secure a consent agreement from the data subject, or if it was impossible to secure a consent agreement, chances are high that the data subject would have provided such consent in any case.[98] The above conditions immediately provide a waiver of consent. They leave a gap in stringent efforts to provide sufficient data protection as they allow "assumed" consent leading to abuse by responsible parties to evade liability on unlawful cross-border data transfers.

5.3 Authorisation by the Information Regulator

Responsible parties who conduct cross-border data transfers using cloud computing services are bound to conduct themselves, at minimum, with the conditions set out in the POPIA.[99] Section 57(1)(d) of the Act provides that the Information Regulator's (IR's) consent must be acquired prior to transferring personal information to another country. Ideally, the IR's consent will be secured if personal information is transferred to a jurisdiction with identical data protection legislation to that of the POPIA.[100] Furthermore, the IR has to facilitate cross-border data transfers cooperation in enforcing privacy related legislation through taking part in any measures aimed at such cooperation.[101] The responsible party must ensure that it provides and maintain the data protection and security principles referred to under section 19 of the Act through a written contract with the cloud computing service provider.[102] Where there are reasonable grounds to believe that the personal information stored in the cloud computing service provider servers has been accessed or acquired by an unauthorised person the responsible party must be immediately notified of such events or activities.[103] On the other hand, the responsible parties must inform the data subject about such activities and that they intend to transfer their personal information to another country or an international organisation.[104] The level of data protection provided by that other country or international organisation must be disclosed to the data subject as well.[105] In other words, in terms of the provisions of the POPIA, transparency is key to ensure lawful

96 Section 72(1)(*d*) of the POPIA.
97 Section 72(1)(*d*) of the POPIA.
98 Section 72(1)(*e*)(i) and (ii) of the POPIA.
99 Sections 2, 3, 57, 69, 72, and ch 3 of the POPIA.
100 Section 72(1)(*a*)(i) and (ii) of the POPIA and see s 39 of the POPIA on provisions for the establishment of the Information Regulator.
101 See s 40(1)(*g*) of the POPIA.
102 See s 21(1) of the POPIA (s 19 makes provisions for the security safeguards and security measures for the integrity and confidentiality of personal information).
103 Section 21(2) of the POPIA.
104 Section 18(1)(*g*) of the POPIA.
105 Section 18(1)(*g*) of the POPIA.

processing of personal information across the border. The following paragraphs will discuss provisions of the GDPR on cross-border data transfers.

6 Trans-border data flows under the GDPR

The GDPR's provisions influence and affect international transfers of personal data[106] outside the European Economic Area,[107] by providing data protection and the right to privacy;[108] which are both recognised as fundamental human rights.[109] The Charter of Fundamental Rights provides that everyone has the right to the protection of their personal data,[110] while the European Convention of Human Rights also includes provisions for the protection of the right to privacy.[111] Within the space of data protection,[112] Bradford[113] states that the EU raised the bar, as the GDPR is influencing the data protection laws of other countries, except the US.[114] Despite its differences with US law, the GDPR still impacts US companies' operational practices, through litigation in EU territories stemming from noncompliance with the GDPR provisions.[115] The US companies are also impacted by the GDPR through the adoption of privacy policies to comply with the GDPR's provisions within the spaces where those companies operate in the EU.[116] The influence of voluntary international agreements between US and the EU, such as the US-EU Privacy Shield Framework also impacts the US companies to comply with the GDPR's provisions.[117] This is not the fact with only US companies, SA companies can also fall within one of the above forces of influence to comply with the provisions of the GDPR despite different legal systems. Some EU countries such as Poland, Germany, Spain, and Hungary have constitutional rights to data protection. The *Court of Justice of the European Union* (CJEU) stated that processing personal

106 Yakovleva and Irion 2020 *AJIL Unbound* 10.
107 Yakovleva and Irion 2020 *AJIL Unbound* 10.
108 Yakovleva and Irion 2020 *AJIL Unbound* 10.
109 European Commission 2007 https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charterfundamental-rights_en; Quan 2020 *Frontiers Law China* 272.
110 Article 8(1) of the *Charter of Fundamental Rights of the European Unio*n (2000); Mattoo and Meltzer 2018 *J Int'l Econ L* 771.
111 Article 8 of the *Convention for the Protection of Human Rights and Fundamental Freedoms* (1950).
112 Bradford 2012 *NWULR* 22-26.
113 Bradford 2012 *NWULR* 22.
114 Bradford 2012 *NWULR* 19-35.
115 Bradford 2012 *NWULR* 23.
116 Bradford 2012 *NWULR* 24.
117 Bradford 2012 *NWULR* 24-25.

information is a threat to the right to privacy and, may only be done in terms of the law meaning the EU data protection laws.[118]

It is difficult to bring data out of the EU in terms of the GDPR. However, in the absence of an adequacy finding, data controllers may adopt specific binding corporate rules or model contracts approved by the EU to conduct cross-border data transfers. A controller must be compliant with the domestic data protection laws of a country that has been granted an adequacy decision from the EU,[119] in other words, those state's laws that have been assessed and deemed sufficient to provide adequate data protection. For example, a US organisation may sign up in the bilateral US-EU Privacy Shield Framework[120] for the transatlantic data transfers. The GDPR also envisions a certification scheme to transfer data. The certification mechanism as an alternative could be a less problematic option for compliance for foreign organisations to conduct cross-border data transfers in and out of the EU.

The term "cross-border processing" is defined as the processing of personal data in the context of the activities of establishments of a controller domiciled in more than one EU Member State.[121] The term also means processing personal data in the context of the activities of a single establishment of a controller or processor in the EU.[122] The activities that trigger the processing of personal data must significantly or potentially affect data subjects in more than one country within the EU community.[123] The use of cloud computing services to process personal data can affect data subjects in more than one country within the EU through its transnational characteristic, triggering the GDPR application.

POPIA does not define "cross-border processing" as much as it makes provisions for its protection. "Onward transfers" of personal data remain problematic on cross-border data transfers.[124] Although the term "onward transfers" is not defined in both the GDPR and POPIA, it refers to personal data that has been transferred further from the primary destination, country

118 *Google Spain v Agencia Española de Protección de Datos (AEDP)* 317 ECR (13 May 2014) para 96.

119 EU 2021 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en; Quan 2020 *Frontiers Law China* 273.

120 The EU and US negotiated the US-EU Privacy Shield Framework to allow for the transatlantic transfer of personal data by certified organisations; Ireland's National Public Media 2018 https://www.rte.ie/news/2018/0717/979174-eu-japan/.

121 Article 4(23) of the GDPR.

122 Article 4(23) of the GDPR.

123 Article 4(23) of the GDPR.

124 Esayas 2012 *Computer Law and Security Review* 664; Mouzakiti 2015 *EDPL* 41.

or organisation outside the country of origin to another country also known as the third country.[125] When such transfers take place, it is vital to ensure that the primary destination prohibits an onward transfer if the recipient country, destination or organisation does not provide adequate data protection safeguards. Both the POPIA and the GDPR make such provisions on onward transfers. EU data subjects' personal data can be processed across the EU territory without further precautions under a formal finding from the EU if sufficient data protection in the receiving country, also known as "adequacy finding" is provided.

6.1 Adequacy decision on cross-border data transfers

A determination of adequacy requires countries who are not Member States of the EU to adopt and implement a privacy legislation that is similar or equivalent to the GDPR.[126] This similarity or equivalence should not only relate to the level of data protection, access of government agencies to personal data and data subjects' rights of redress to personal data must be consistent with the GDPR as well. As noted by Kuner, that on a requirement of "equivalent" outcomes, the authorities must compare data protection standards of another country outside the EU community against the standards of the GDPR which is an exercise that is often met with challenges such as resource scarcity to execute such assessments.[127] Some of these challenges will be discussed in detail below.

The transfer of personal data out of the EU can only be carried out based on an adequacy decision,[128] or susceptible to appropriate safeguards,[129] which may include binding corporate rules.[130] Irrespective of the transfer, the crux is that personal data must be sufficiently protected in the receiving country or international organisation[131] that the European Commission (EC) has determined provides adequate data protection.[132] Cross-border data

125 Mouzakiti 2015 *EDPL* 41; Voss 2020 *Washington International Law Journal* 506.

126 *Schrems v Data Protection Commissioner* 310 IEHC (2014) para 73.

127 Kuner 2017 *German Law Journal* 900; Mattoo and Meltzer 2018 *J Int'l Econ L* 776.

128 Article 45 of the GDPR.

129 Article 46 of the GDPR.

130 Article 47 of the GDPR.

131 Article 4(26) of the GDPR states that "international organisation" means an organisation and its subordinate bodies governed by public international law or any other body set up by, or based on, an agreement between two or more countries.

132 Article 45(1) of the GDPR; European Commission 2020 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en Countries that have previously been approved are: Andorra, Argentina, Canada (where the *Personal Information Protection and Electronic Documents Act* is applicable), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay, and New Zealand; Voss 2019 *University of Illinois Journal of Law, Technology and Policy* 459; Voss 2020 *Washington International Law Journal* 507; WorldAtlas 2020

transfers to a country or international organisation that has been granted an adequacy finding does not require any specific authorisation.[133] The EC makes adequate determinations for countries and specific territories or sectors[134] and must be reviewed every four years.[135] The EC further monitors ongoing developments in each approved country that could affect adequacy determination.[136] To assess the standards of data protection instrument(s) of a country outside the EU community, the EC takes certain aspects into account.[137] Some of these aspects include the relevant legislation, recognition and respect for human rights and fundamental freedoms, the rule of law and the establishment of an effective operation of independent Supervisory Authorities (SAs).[138] The SAs are tasked to enforce compliance with privacy and data protection laws, these include assisting and advising data subjects on how to exercise their rights. The SAs also cooperate with other SAs from other EU Member States to promote, protect and enforce data protection laws across the region and ensure uniformity on implementation of such data protection measures.[139]

The EC further considers international commitments the country or international organisation from outside the EU is engaged into,[140] these include binding international instruments or conventions as well as their involvement in regional and multilateral systems predominantly concerning personal data protection.[141] In the absence of an adequacy decision, personal data can only be transferred in and out of the EU if the data controller guarantees appropriate safeguards, data subject's rights, and legal remedies.[142] For example, Japan and the EU reached an agreement to accept each other's data protection frameworks as "equivalent," which opened up the free movement of information between both parties and served as a first attempt at adopting an adequacy decision.[143]

https://www.worldatlas.com/nations.htm. See also EU 2020 https://europa.eu/european-union/about-eu/countries_en.

133 Article 45(1) of the GDPR.

134 Article 45(3) of the GDPR.

135 Article 45(3) of the GDPR.

136 Article 45(4) of the GDPR.

137 Article 45(2) of the GDPR.

138 Article 45(2)(*a*) of the GDPR.

139 Article 45(2)(*b*) of the GDPR.

140 Blume 2015 *IDPL* 34; Roos 2020 *CILSA* 5.

141 Blume 2015 *IDPL* 34; Roos 2020 *CILSA* 5.

142 Articles 45(2)(*a*) and 46(1) of the GDPR.

143 See Ireland's National Public Media 2018 https://www.rte.ie/news/2018/0717/979174-eu-japan/.

6.1.1 Revoking the adequacy decision

The EC shall, following the review, suspend, amend or repeal its decision of an adequacy finding through implementing acts without retroactive effect,[144] adopted under the examination procedure as per the GDPR.[145] These decisions can be taken if a country or an international organisation outside the EU no longer provides an adequate level of data protection required. Before taking such a decisive action, the EC will first consult with the parties in question to remedy the legal defects and ensure adequate data protection.[146] In CJEU's decision in *Schrems and Facebook Ireland v Data Protection Commissioner*[147] the EU-US Privacy Shield Framework was invalidated, as well as its standard contractual clauses. This decision impacted critical mechanisms for transferring personal data from the EU to the US, with important impacts on trade and the development of technologies such as cloud computing and Artificial Intelligence (AI).[148]

In an earlier case of the CJEU decision in *Schrems v Data Protection Commissioner*[149] found that the EC adequacy decisions concerning the EU-US Safe Harbor Agreement were invalid. The EC had to revise and revoke the adequacy decision against the US based on this decision. However, transatlantic data flows are the lifeblood of the economic relations between the EU and the US. Therefore, both parties engaged in another endeavour to adopt an instrument that would pass muster with the CJEU and enable transatlantic data flows hence the EU-US Privacy Shield Framework was adopted.[150] In this case, the applicant, Schrems, was a subscriber on Facebook social media platform which is a US-based company. At the time, Facebook was self-certified and subject to the Safe Harbour agreement. Subscribers agreed with Facebook Ireland Ltd, regulated in terms of the *Irish Data Protection Acts* of 1988 and 2003 on the terms and conditions of using the platform. In the judgment of the High Court, it was proven that some portions or the entire data of subscribers to the platform was

144 Article 45(5) of the GDPR.
145 Article 45(5) of the GDPR.
146 Article 45(6) of the GDPR.
147 *Schrems and Facebook Ireland v Data Protection Commissioner* C-311/18 CJEU (2020).
148 Meltzer 2020 https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ #footnote-1.
149 *Schrems v Data Protection Commissioner* C-362/14 CJEU (2015). See also *Schrems v Data Protection Commissioner* 310 IEHC (2014) (hereinafter the *Schrems* case).
150 Meltzer 2020 https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/ #footnote-1.

transferred by Facebook Ireland to its servers based in the US. Immediately after the "Snowden revelations",[151] Schrems lodged a complaint with the Irish Data Protection Commissioner (DPC). Schrems pointed out that the revelations made by Snowden was proof that data transferred from the EU to the US was not sufficiently protected. Schrems was of the view that the DPC had to enforce its powers and instruct the termination of transatlantic data transfers from Facebook Ireland Ltd to its servers located in the US.[152] On the other hand, the DPC stated that it was bound by the Safe Harbour agreement based on the adequacy decision that was made by the EC therefore, it had no authority to investigate matter,[153] concluding that the applicant's complaint had no legal basis. Schrems disagreed with this reasoning of the DPC and took the matter to the Irish High Court. Justice Hogan, after a careful examination of the Irish and EU legal framework on data protection, concluded that the DPC acted in accordance with the law.[154] However, Hogan noted that Schrems' claims were challenging the provisions of the Safe Harbour agreement, which was not directly challenged in that case. The Judge observed that major developments have occurred since the adoption of the Safe Harbour Agreement. In particular, he mentioned the subsequent adoption of Articles 7 and 8 of the *EU Charter of Fundamental Rights*, on the protection of personal data and the right to privacy, as well as the "Snowden revelations".[155] In light of these developments, the High Court decided to pose certain questions to the CJEU for clarity in order to resolve the matter at hand.[156] The High Court was questioning whether a National Data Protection Authority (NDPA) can investigate any matters on data protection stemming from the Safe Harbour agreement or they are bound by such an agreement not to investigate. The other question was whether, considering developments such as the "Snowden revelations" that had occurred after the Safe Harbour agreement came into force, the NDPA can investigate the matter, following a

151 Edward Joseph Snowden is an American former computer intelligence consultant who leaked highly classified information from the National Security Agency (NSA) in 2013 when he was an employee and subcontractor. His illegal disclosures revealed numerous global surveillance programs, many ran by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments, and prompted a cultural discussion about national security and individual privacy; Wikipedia 2022 https://en.wikipedia.org/wiki/Edward_Snowden.

152 Article 3 of *Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC 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* OJ L 215/7 (2000).

153 *Schrems* case 32.

154 *Schrems* case 68.

155 *Schrems* case 69-71.

156 Europe-v-Facebook Organisation Project 2017 http://europe-v-facebook.org/EN/en.html; Mouzakiti 2015 *EDPL* 46.

complaint.[157] During the hearing, the Commission was asked by the Judge whether it pleaded that the Safe Harbour Agreement is not subject to the provisions of Article 8(3) of the *Charter of Fundamental Rights* provision that compliance with data protection laws must be controlled by an independent body. In its response, the Commission stated that, in its opinion, NDPAs cannot question an adequacy finding issued by the EC.[158] The commission was of the view that if NDPAs were given the authority to question, undermine or set aside an EC's adequacy ascertainment, this could lead to the regulatory fragmentation on trans-border data transfers. Furthermore, the EC would be deprived of its authority and primary function to pronounce on "adequacy decisions".

6.1.2 Issues around the adequacy decision

The process to make an adequacy determination is faced with challenges such as assessing the legal frameworks of other foreign countries, the scarcity of sufficient resources to conduct such assessments and the process itself being time-consuming.[159] The adequacy determination or assessment is conducted based on the entire legal framework of the country in question as opposed to a specific industry, sector, or type of personal data.[160] Observably, the EC's focus on adequacy determination is restricted mostly to a limited number or group of countries, by taking into consideration their GDP.[161] For the countries such as SA that have not yet obtained EC's adequacy determination, they must rely on other data protection mechanisms for cross-border personal data transfers such as "appropriate safeguards" which may include legally binding and enforceable instruments between public bodies or authorities.[162] Such mechanisms are intended to indemnify the insufficiency or lack thereof of data protection instruments in that country,[163] however, they are very expensive to adopt and maintain.[164]

6.2 Appropriate safeguards on cross-border data transfers

Data transfers from the EU to non-EU countries or international organisation can only take place if they have appropriate safeguards,[165] without requiring authorisation from the SA.[166] Legal frameworks that are binding and

157 *Schrems* case 71.
158 CJEU 2015 http://www.europe-v-facebook.org/CJEUhearingnotes.pdf; Mouzakiti 2015 *EDPL* 46.
159 Mouzakiti 2015 *EDPL* 41.
160 Mouzakiti 2015 *EDPL* 41.
161 Mouzakiti 2015 *EDPL* 41.
162 Article 46(1) of the GDPR.
163 Recital 108 of the GDPR.
164 Article 46(2)(*a*) of the GDPR.
165 Article 46(1) of the GDPR.
166 Article 46(2) of the GDPR.

enforceable between public bodies or authorities,[167] or by following Article 47 can make such transfers possible.[168] The EC can adopt a standard clause on data protection under the examination procedure[169] and approve it accordingly to guarantee the security and appropriate safeguard of data stored in the servers of the cloud computing service provider.[170] If a specific code of conduct has been approved by the EC,[171] with binding and enforceable devotions, the data controller in the receiving country should enforce appropriate safeguards, as well as the rights of the data subjects based on an approved certification mechanism.[172] The certification mechanisms and the codes of conduct are both new under the GDPR, however, the EC pronounced its interest and devotion to developing and maximise[173] them for cross-border data transfers. The requirement by the CJEU that countries outside the EU, their data protection laws should be similar or equivalent to the GDPR likely limits the potential utilisation of such mechanisms.[174] Agreements or contractual clauses between data controllers, or the recipient of personal data in another country or international organisation outside the EU can make up and achieve the primary objectives of the appropriate safeguards.[175] Enforceable data subjects' rights must be included within the provisions of the administrative arrangements between public bodies or authorities for them to have the force and be deemed adequate.[176]

POPIA is shallow compared to the GDPR as to what constitutes "appropriate safeguards". They do not prescribe what constitutes a binding agreement and the enforcement mechanisms to ensure adequate data protection.

6.3 The role of binding corporate rules on cross-border data transfers

The GDPR defines binding corporate rules as policies that should be adhered to aimed at protecting personal data when processed by a data controller or processor established within the EU territory.[177] These policies

167 Article 46(2)(*a*) of the GDPR.
168 Articles 46(2)(*b*) and 47 of the GDPR provide binding corporate rules.
169 Articles 46(2)(*c*) and 93(2) of the GDPR.
170 Article 46(2)(*d*) of the GDPR.
171 Articles 40 and 46(2)(*e*) of the GDPR.
172 Article 46(2)(*f*) of the GDPR.
173 Mattoo and Meltzer 2018 *J Int'l Econ L* 776.
174 Mattoo and Meltzer 2018 *J Int'l Econ L* 776.
175 Article 46(3)(*a*) of the GDPR.
176 Article 46(3)(*b*) of the GDPR.
177 Article 4(20) of the GDPR.

are applicable for data transfers to a data controller or processor in another country outside the EU within a group of undertakings,[178] or enterprises operating or in pursuit of a joint economic interest.[179] Members within the group of enterprises or undertakings, including their employees should apply, enforce and be bound by the binding corporate rules.[180] These members and their employees should further enforce data subject's rights concerning the transfer of their data to another jurisdiction outside of the EU[181] through the realisation of data protection principles of the GDPR.[182]

Structures and contact details of the group of enterprises or undertakings must be specified in the binding corporate rules.[183] Any transfers or set of data transfers, including the types of personal data, the data processing mechanism used, and the purpose(s) for the transfer must be specified in the binding corporate rules. Categories of data subjects impacted and the details of the country or countries in question are also to be included in the binding corporate rules.[184] Binding corporate rules must be legally binding, both in and outside the EU jurisdiction,[185] however, they do not bind the general data protection principles.[186] Data protection principles such as data minimisation, quality of data, purpose limitation, period of data storage limitations, data protection by design and default, and the legal basis for processing special categories of personal data, measures to ensure data security, and the requirements on onward transfers should be included. The data subjects' rights regarding the processing of their personal data such as the right not to solely be subject to automated processing decisions and profiling and the means to enforce those rights must be specified in the binding corporate rules.[187]

The binding corporate rules must further provide data subjects with an unconditional right to bring complaints before a competent and independent SA or before the courts of that country in question.[188] In the event that binding corporate rules have been breached or violated, the affected data

178 Article 4(19) of the GDPR defines the term "group of undertakings" as controlling and controlled undertakings.
179 Article 4(20) of the GDPR.
180 Article 47(1)(*a*) of the GDPR.
181 Article 47(1)(*b*) of the GDPR.
182 Article 47(1)(*c*) of the GDPR.
183 Article 47(2)(*a*) of the GDPR.
184 Article 47(2)(*b*) of the GDPR.
185 Article 47(2)(*c*) of the GDPR.
186 Article 47(2)(*d*) of the GDPR.
187 Article 47(2)(*e*) of the GDPR.
188 Article 47(2)(*e*) of the GDPR.

subject must be compensated or obtain redress where appropriate.[189] Section 99 of the POPIA has a similar provision.[190] However, the POPIA does not specify it under section 72 but provides it as a general provision under a different section and not specifically for cross-border data transfers. The controller processing personal data of EU data subjects has an obligation to explicitly establish an acceptance on one of the EU countries for any violations of the binding corporate rules.[191] The data controller shall then be exempt fully or partly from that liability if it can prove that it is not responsible for the breach or violation of binding corporate rules that led to the damage.[192] In this instance, it is the role of the EC to specify procedures and formats on how information can be exchanged between data controllers, data processors, and SAs for binding corporate rules within the confines of the GDPR. All the implementing acts for binding corporate rules should be adopted after having gone through the examination procedure as outlined in the GDPR.[193]

Section 72 of the POPIA has a similar definition for the term "binding corporate rules".[194] However, the GDPR does not merely define the term; it also outlines how the binding corporate rules should be designed, their scope, application, and enforcement mechanisms. However, all the requirements for the binding corporate rules under the GDPR, are covered under chapter 3 of the POPIA. Although covered in a general application section other than section 72, both legislations provide a similar cross-border data flow mechanism for binding corporate rules.

Challenges with binding corporate rules were highlighted in *Schrems and Facebook Ireland v Data Protection Commissioner*. In this case, the challenge was against the availability of binding corporate rules when the government of the receiving country was not using personal data in consonant with EU privacy and data protection laws.[195] The other challenge patterns to expensive, lengthy and protracted implementation phases and approval processes of binding corporate rules. The binding corporate rules are also not suitable and user-friendly for small businesses whose operations involve cross-border digital services to and from the EU.[196]

189 Article 47(2)(*e*) of the GDPR.
190 Section 99(1) of the POPIA.
191 Article 47(2)(*f*) of the GDPR.
192 Article 47(2)(*f*) of the GDPR.
193 Articles 47(3) and 93(2) of the GDPR.
194 Section 72(2)(*a*) of the POPIA.
195 See High Court Commercial 2016 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362.
196 Mattoo and Meltzer 2018 *J Int'l Econ L* 776.

6.4 Unauthorised data transfers or disclosures in and out of the EU

Transferring personal data out of the EU without the necessary disclosure or authorisation is deemed unlawful.[197] Data transfers and disclosures based on court judgments, enforceable decisions made by any tribunal and any authorised administrative decisions are recognised and enforceable based on an international convention or agreement.[198] Some of the international agreements include a Mutual Legal Assistance (MLA) treaty between the country outside the EU community and one of the EU countries. However, the MLAs should not be detrimental or in conflict to other principles for lawful data transfers.[199] An example of such an agreement is the EU–US Privacy Shield Framework. Section 40(1)(c) of the POPIA makes provisions for MLAs with third countries as well.

6.5 Derogations for specific situations

Transferring personal data to countries or international organisation outside the EU in the absence of the appropriate safeguards, including binding corporate rules and the adequacy decision can occur only under specific conditions.[200] The first condition is that before any personal data is transferred, the data subject should explicitly consent to the proposed transfer, and be informed by the controller of the risks that could emerge from such transfer owing to the lack of appropriate safeguards and adequacy determination by the EC.[201] POPIA also has a similar provision,[202] although it does not detail the condition as much as the GDPR does. The second condition is that the transfer must be necessary to execute contractual obligations between the controller and the data subject or at the request of the data subject to implement pre-contractual measures.[203]

Thirdly, the data transfer must be necessary for the execution or performance of one or more contractual obligations for the data subject's benefit between the controller and another party other than the data subject.[204] Fourthly, data transfer can only take place in the interest of the public for important reasons.[205] The fifth condition allows data transfers when one is defending a legal claim and exercising or establishing their

197 Article 48 of the GDPR.
198 Article 48 of the GDPR.
199 Article 48 of the GDPR.
200 Article 49(1) of the GDPR.
201 Article 49(1)(*a*) of the GDPR.
202 Section 72(1)(*b*) of the POPIA.
203 Article 49(1)(*b*) of the GDPR.
204 Article 49(1)(*c*) of the GDPR.
205 Article 49(1)(*d*) of the GDPR.

rights.[206] The sixth condition allows data transfers where the data subject is physically impaired or legally incapable to provide consent when such transfer is necessary to protect the vital interests of the data subject or other persons.[207] The seventh condition is around the transfer stemming from a record intended to provide information to the public.[208] The data contained in such a record must be made available for consultation and scrutiny by the public or anyone with a legitimate interest, however, the EU or Member State must lay down the conditions and laws for consultation to take place.[209]

The eighth condition states that data transfers may occur only if not repetitive.[210] The data transferred must be restricted to a number of data subjects or for valid legitimate interests pursued by the controller. The legitimate interests pursued should not override the interests, rights and freedoms of the data subject. The ninth condition requires data controllers to inform the SA of the transfer prior. Before approaching the SA, the data control must have first assessed all the circumstances around the data transfer and, by relying on that assessment, controllers are required to provide suitable personal data protection safeguards.[211] The data subject must be informed by the data controller of the data transfer as well as the legitimate interests pursued.[212] The tenth condition allows the EU or Member State to limit the transferring of certain categories of personal data out of the EU in the absence of an adequacy determination to the receiving country or international organisation. The controller as a user of cloud computing services and the cloud computing service provider must compile an assessment and appropriate safeguards adopted for data protection within their contractual agreement.[213]

So far none of the above derogations have proven to be appropriate for controllers who transfer personal data out of the EU. For instance, these derogations require explicit consent by the data subject of the possible risks of such transfers but it must be "informed consent" which raises the stakes.[214] These derogations limit the necessity for the execution of contractual obligations as a basis for transferring data out of the EU. In many

206 Article 49(1)(*e*) of the GDPR.
207 Article 49(1)(*f*) of the GDPR.
208 Article 49(1)(*f*) of the GDPR.
209 Article 49(1)(*g*) of the GDPR.
210 Article 49(1)(*g*) of the GDPR.
211 Article 49(1)(*g*) of the GDPR.
212 Article 49(1)(*g*) of the GDPR.
213 Article 49(6) of the GDPR.
214 Article 49(1)(*a*) of the GDPR; Mattoo and Meltzer 2018 *J Int'l Econ L* 777.

instances, data controllers do not have contractual agreements with data subjects such as when personal data is processed from the website on the internet or monitoring data subjects' behaviours online. These scenarios normally do not forge or create contractual obligations or relationships. To transfer data out of the EU countries to pursue a legitimate interest is heavily restricted and cannot be utilised for large quantities and frequent data transfers.[215]

6.6 International cooperation on cross-border data transfers

The EC and SAs take appropriate steps to ensure that the EU citizen's personal data is processed lawfully.[216] These bodies have developed effective mechanisms through international cooperation to facilitate successful implementation and enforcement of data protection legislation.[217] These mechanisms include; investigative assistance, exchange of information, notification, appropriate safeguards and complaint referral for data protection.[218] The EC engages with suitable stakeholders to discuss further international cooperation in enforcing data protection legislation.[219] The EC also engages in activities such as promoting information exchange on personal data protection and practices, including issues of jurisdictional conflicts with countries out of the EU.[220] Fortunately, POPIA and the GDPR make similar provisions on data protection. The GDPR provides a more updated data protection law rather than implementing completely new concepts on data protection.[221]

6.7 Comparison

The GDPR sets a uniform standard and data processing principles for all EU countries, whilst POPIA is limited to SA. Although the IR is established under section 39 of the POPIA, which performs similar functions as the SAs under the GDPR, the POPIA does not explicitly clarify the duties of the IR on international data transfers to the extent that the GDPR does on SAs. There is no mention of the IR or its role under section 72 of the POPIA. The role of the IR on cross-border data flows is briefly mentioned under section 57(d), where its authorisation for cross-border data transfers is required. In contrast, Article 48 of the GDPR requires the SA to authorise cross-border

215 Article 49(1)(*a*) of the GDPR; Mattoo and Meltzer 2018 *J Int'l Econ L* 777.
216 Article 50 of the GDPR.
217 Article 50(1)(*a*) of the GDPR.
218 Article 50(1)(*b*) of the GDPR.
219 Article 50(1)(*c*) of the GDPR.
220 Article 50(1)(*d*) of the GDPR.
221 Yav 2018 *International Journal Data Protection Officer, Privacy Officer and Privacy Counsel* 19.

personal data transfers. Non-compliance with section 72 is classified as interference with protecting personal information in section 73(1)(b).[222] However, under section 107 for penalties attached to the contravention of a specific provision of the Act, there is no mention of section 72 contravention. At this moment, it is unclear what explicit penalties are attached to unlawful cross-border personal information transfers under POPIA. On the other hand, Articles 82 and 83 of the GDPR are very specific on the penalties attached when one of the GDPR's provisions is breached on cross-border data transfers.

The difference in notification requirements and penalties regards more stringent time constraints and more severe fines imposed by the GDPR. The GDPR places a duty on any breaching organisation to report to SAs within 72 hours of discovering a breach. POPIA is very vague in this regard and does not provide a specific timeline. Perhaps more worryingly for the organisations affected, the fines in the GDPR for breaches are significantly severe, up to 20 million euros compared to POPIA's R10m fine. The GDPR also allows penalties to be calculated as a percentage of the global annual revenue of companies (whichever of the two amounts is larger). POPIA provides for criminal sanctions for the unlawful processing of personal information in general which is a provision that the GDPR does not have.

7 Challenges of GDPR on cross-border data transfers regulation for South Africa

Since the GDPR came into force, some businesses, including big role players in the digital space have resorted to exit the EU market due to compliance challenges with the GDPR, and high possibilities of facing lawsuits for non-compliance.[223] Since 2018 Data Protection Authorities in the EU have received a range of complaints and initiated a number of GDPR enforcement actions. The French NDPA imposed f50 million fine in January 2019 against Google, which is currently dabbed the largest penalty to date for the breach of data privacy. The fine was imposed against Google for its failure to be transparent on how user's data is processed using search engine.[224] This case shows that online privacy protection could cause great

222 Section 73(1)(*b*) of the POPIA states that –for the purposes of Chapter 10 of the POPIA, "interference with the protection of the personal information of a data subject consists, in relation to that data subject, of – (a) any breach of the conditions for the lawful processing of personal information as referred to in Chapter 3; (b) non-compliance with section 22,54,69,70,71 or 72; or (c) a breach of the provisions of a code of conduct issued in terms of section 60".

223 Quan 2020 *Frontiers Law China* 272.

224 Kayali 2019 https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/; see also Charlet 2019 https://news.bloomberglaw.com/privacy-

uncertainty for internet companies, increasing the cost of compliance for domestic companies and foreign investors. For countries like SA, the cross-border provisions of the GDPR pose a challenge. Significant portions of SA's export services, including to the EU, rely much on cross-border data transfers. However, SA has adopted the POPIA which currently hasn't been to an EC's adequacy assessment. Some of the SA's exports in goods and services to the EU comprise of information technology-driven and software-enabled services.[225] Developing countries such as SA are further faced with a dilemma: these countries can either adopt domestic privacy regulations similar to the GDPR, or their companies can adopt company-specific or transaction-specific expenses of using binding corporate rules or standard contractual clauses which are both costly and time-consuming.[226]

Despite the GDPR having a legitimate aim to protect EU data subjects, on the other hand, it makes the movement of data internationally more challenging. Obtaining an EC adequacy decision on data privacy laws for a country out of the EU enables unrestricted access to the markets in the EU. However, prematurely stringent privacy legislations have the potential to hurt the efficiency, and development of financial sector and other markets by restricting international data flows. It is, therefore, suggested that POPIA be amended to comply with the GDPR standards on cross-border data transfers and approach the EC for an adequacy determination.

8 Recommendations

One could argue that the differences highlighted above between the POPIA and the GDPR on cross-border data transfers are not substantial enough to derail an adequate finding of the POPIA by the EC on cross-border data transfers.[227] However, it would be prudent for the legislature to bolster the provisions that do not reach the standard set by the GDPR to meet the international data protection standard.[228]

8.1 Data portability

POPIA must consider adopting the provisions such as Article 20 of the GDPR on data portability. EU data subjects can order that their data be transferred from one controller to another. This is a matter which POPIA does not explicitly address, which is highly recommended to be adopted on cross-border data flows. This means EU data subjects can choose which

and-data-security/big-google-privacy-fine-may-set-bar-for-eu-privacy-penalties; Quan 2020 *Frontiers Law China* 273.

225 Mattoo and Meltzer 2018 *J Int'l Econ L* 777.

226 Mattoo and Meltzer 2018 *J Int'l Econ L* 770.

227 Roos 2020 *CILSA* 31.

228 Roos 2020 *CILSA* 31.

jurisdictions their personal information can be transferred to; they are more empowered to control their personal information than their SA counterparts.

8.2 Cloud computing-specific provision

A cloud computing-specific provision is recommended within the regulations because a data subject had control over software, hardware and data before introducing cloud computing services into the IT space. The user of cloud computing pays for the use of software as well as the hardware which is typically owned by the cloud computing service provider, and the only asset the user owns is data.[229] Providing a legal framework for a specific remedial mechanism can strengthen the trust of users of cloud computing services, knowing that they have some protection and remedial mechanism for international data transfers. The regulator must also consider the penalties for contravening the provisions of cross-border data transfers, as currently, there is no specific and explicit penalty attached to the unlawful processing of personal information across SA borders.[230] POPIA should be stringent enough to address the privacy concerns arising from international data breaches as stated under Articles 44, 82, 83, and 84 of the GDPR. The lawmakers should avoid creating arbitrary rules in the process that would unnecessarily limit other rights such as protecting the free flow of data within and outside SA, access to information, and innovation and development since cloud computing has become widely used to drive economic activities across the globe. A careful balance of both responsible parties' and data subjects' rights must be ensured to allow responsible parties to freely enjoy using cloud computing platforms without violating the informational privacy of the data subjects.

8.3 Multi-faceted approach

SA data protection laws must consider adopting a multi-faceted approach. Certain bodies and organisations have recommended a multi-faceted approach, including the International Telecommunication Union and the Organisation for Economic Cooperation and Development. Should SA take this route, like other jurisdictions such as Australia this approach will be a solution that will place SA in the world stage for sufficient data protection mechanism. Besides, this is a move and approach that has been called for

229 Ahmed 2010 http://ssrn.com/abstract=1712565.

230 Section 107 of the POPIA makes provisions for Penalties. "Any person convicted of an offence in terms of the POPIA is liable in the case of an infringement of; (*a*) section 100, 103 (1), 104 (2), 105 (1), 106 (1), (3) or (4) to a fine or imprisonment for a period not exceeding 10 years, or to both a fine and such imprisonment; or (*b*) section 59, 101, 102, 103 (2) or 104 (1), to a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment".

by many commentators across the world.[231] The multi-faceted approach includes adopting strong legislation which SA already has although it needs revision, general public awareness and education on cloud computing, international cooperation with other jurisdictions, industry partnerships and other technical measures.

8.4 Data governance

The concept of data governance framework is adopted to formalise the functions, policies, and procedures as well as the roles, within which the organisation that processes personal data must adhere to and view such data as a strategic asset.[232] The identification and transfer of sensitive data must be monitored within the organisation,[233] to comply with legislation and leverage data protection.[234] The data governance framework also ensures data quality and availability,[235] to help responsible parties comply with various different data privacy laws.[236] Metadata on, the other hand is another tool that helps data subjects to exercise their rights under specific legislation, such as the right to access their personal information. Metadata undoubtedly assists to guarantee good data governance as technological developments adopted by different industries nowadays, such as cloud computing, create challenges for compliance with the laws. Some of these challenges in cloud computing are created through the movement of data around within the "cloud", and then the location of data at any specific time gets lost or unknown.[237] This may necessitate restrictions on cross-border transfer if the data location is in a country that has not yet received an adequacy determination under the GDPR or does not meet the requirements of the POPIA on onward transfers of personal information.[238] Cloud computing service agreements with users must stipulate who will process data and where such data will be stored. In addition to that, effective control over and allocating clear responsibility for processing activities must be ensured and stipulated in the same agreement.[239] When drafting and negotiating a cloud computing service agreement, the user must apply his, her or its mind carefully about personal data management.[240]

---

231 Mokowadi-Tladi *Regulation of Unsolicited Electronic Communication* 303.
232 See Cohn 2015 *ISJLP* 813; Voss 2020 *Washington International Law Journal* 518.
233 Power and Trope 2006 *Business Law* 251.
234 Power and Trope 2005 *Business Law* 472.
235 Engels 2019 *Intereconomics* 217.
236 Engels 2019 *Intereconomics* 217.
237 Yoo and Blanchette *Regulating the Cloud* 186.
238 Yoo and Blanchette *Regulating the Cloud* 155.
239 See Article 29 Data Protect Working Party 2012 https://ec.europa.eu/justice/article29/documentation/opinion/recommendations/files/2012/wpl96_en.pdf.
240 Voss and Woodcock *Navigating EU Privacy and Data Protection Laws* 190.

Organisations and industries that adopt good data governance frameworks stand a good chance to comply with different data privacy legislations applicable to their cross-border data transfers supply chain. The users of cloud computing services must start by mapping and understanding data processing mechanisms and where their data is as a first step for good data governance.[241] As the GDPR applies to many international companies, it requires provisions of accountability and assesses companies' international data transfers supply chain for GDPR compliance and POPIA must adopt a similar approach. Based on the above recommendation, contracts and agreements are vital to ensure compliance downstream. These contracts and agreements must also ensure security and transparency as important principles to address and guarantee data protection for any future possible onward transfers.

9 Final remarks

The analysis of section 72 of the POPIA and article 44 of the GDPR provided above, shows that section 72 does to a certain extent provide some level of data protection on cross border data flows. However, the provisions of section 72 lack adequacy as compared to the similar provision under the GDPR on cross boarder data transfers regulation. Section 72 does not protect all the categories of personal data transfers to another country except those that meet the provisions as set out under section 72. The enforcement mechanisms and remedies for the breach of section 72 are vague as discussed above. In terms of the onward transfer of personal information to third countries or parties outside SA, section 72 lacks the enforcement adequacy to hold the recipient accountable in ensuring that further transfers are lawful, and the third party or country does provide adequate data protection and remedies for the unlawful processing. The comparison of section 72 and article 44 have identified some explicit and specific shortcomings of the Act on cross boarder data transfers through cloud computing services. POPIA has not yet been presented (*at the time of the research*) before the EC for adequacy assessment, which entails, transferring personal information to and from the EU remains extensively restricted. The Act was built upon the provisions of the EU Directive that has been repealed and replaced by a new data protection regulation (GDPR), this observation creates an idea that POPIA is based on an outdated legislation despite some provisions of the Directive being present in the GDPR. Therefore, provisions of section 72 could be met with some challenges when its assessment by the EC is conducted for an adequacy decision should that procedure be initiated in future. The revision of section 72 regulating cross-border data flows through cloud computing services is

241 Voss 2020 *Washington International Law Journal* 527.

the best option to improve data protection laws. The above-proposed recommendations would have to deal with all forms of processing personal information across the SA borders, whether automated or non-automated means through cloud computing services. The use of cloud computing services keeps increasing annually across almost all industries, so the more use of cloud computing becomes a threat to the right to informational privacy. Lawmakers must preserve, guard, and protect the right to informational privacy against international data breaches through cloud computing platforms.

Bibliography

Literature

Allan and Currie 2007 *SAJHR*
Allan K and Currie ID "Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa" 2007 *SAJHR* 570-586

Blume 2015 *IDPL*
Blume P "EU Adequacy Decisions: The Proposed New Possibilities" 2015 *IDPL* 34-39

Bradford 2012 *NWULR*
Bradford A "The Brussels Effect" 2012 *NWULR* 19-35

Carpenter 2010 *Washington Journal of Law, Technology and Arts*
Carpenter RH Jr "Walking from Cloud to Cloud: The Portability Issue in Cloud Computing" 2010 *Washington Journal of Law, Technology and Arts* 1-14

Cohn 2015 *ISJLP*
Cohn BL "Data Governance: A Quality Imperative in the Era of Big Data, Open Data, and Beyond" 2015 *ISJLP* 811-826

Engels 2019 *Intereconomics*
Engels B "Data Governance as the Enabler of the Data Economy" 2019 *Intereconomics* 216-222

Esayas 2012 *Computer Law and Security Review*
Esayas SY "A Walk in the Cloud and Cloudy It Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data" 2012 *Computer Law and Security Review* 662-678

Kuner 2017 *German Law Journal*

Kuner C "Reality and Illusion in EU Data Transfer Regulation Post Schrems" 2017 *German Law Journal* 881-918

Kuner *Transborder Data Flows*
Kuner C *Transborder Data Flows and Data Privacy Law* (Oxford University Press Oxford 2013)

Mattoo and Meltzer 2018 *J Int'l Econ L*
Mattoo A and Meltzer JP "International Data Flows and Privacy: The Conflict and Its Resolution" 2018 *J Int'l Econ L* 769-789

Millard and Bascerano 2016 *PELJ*
Millard D and Bascerano EG "Employers' Statutory Vicarious Liability in Terms of the Protection of Personal Information Act" 2016 *PELJ* 1-38

Mokowadi-Tladi *Regulation of Unsolicited Electronic Communication*
Mokowadi-Tladi SE *The Regulation of Unsolicited Electronic Communication (Spam) in South Africa: A Comparative Study* (LLD-thesis University of South Africa 2017)

Mouzakiti 2015 *EDPL*
Mouzakiti F "Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive" 2015 *EDPL* 39-51

Narayanan 2012 *Chicago Journal of International Law*
Narayanan V "Harnessing the Cloud: International Law Implications of Cloud-Computing" 2012 *Chicago Journal of International Law* 783-809

Neethling 2012 *THRHR*
Neethling J "Features of the Protection of Personal Information Bill, 2009 and the Law of Delict" 2012 *THRHR* 241-255

Neethling, Potgieter and Knobel *Neethling-Potgieter-Visser Law of Delict*
Neethling J, Potgieter J and Knobel JC *Neethling-Potgieter-Visser Law of Delict* 7th ed (LexisNexis Durban 2014)

Neethling, Potgieter and Roos *Neethling on Personality Rights*
Neethling J, Potgieter J and Roos A *Neethling on Personality Rights* 2nd ed (LexisNexis Durban 2019)

Peterson 2012 *J Marshall L Rev*
Peterson T "Cloudy with a Chance of Waiver: How Cloud Computing Complicates the Attorney-Client Privilege" 2012 *J Marshall L Rev* 383-408

Power and Trope 2005 *Business Law*

Power EM and Trope RL "Lessons in Data Governance: A Survey of Legal Developments in Data Management, Privacy and Security" 2005 *Business Law* 471-516

Power and Trope 2006 *Business Law*
Power EM and Trope RL "The 2006 Survey of Legal Developments in Data Management, Privacy, and Information Security: The Continuing Evolution of Data Governance" 2006 *Business Law* 251-294

Quan 2020 *Frontiers Law China*
Quan X "The Governance of Cross-Border Data Flows in Trade Agreements: Is the CPTPP Framework an Ideal Way Out?" 2020 *Frontiers Law China* 253-279

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

Roos *Law of Data (Privacy) Protection*
Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (LLD-thesis University of South Africa 2003)

SALRC *Privacy and Data Protection*
South African Law Reform Commission *Discussion Paper 109, Project 124: Privacy and Data Protection* (SALRC Pretoria 2005)

Schwartz 1995 *Iowa L Rev*
Schwartz PM "European Data Protection Law and Restrictions on International Data Flows" 1995 *Iowa L Rev* 471-496

Van der Merwe *et al ICT Law*
Van der Merwe DP *et al Information and Communications Technology Law* 2nd ed (LexisNexis Durban 2016)

Voss 2017 *University of Illinois Journal of Law, Technology, and Policy*
Voss WG "Internet, New Technologies, and Value: Taking Share of Economic Surveillance" 2017 *University of Illinois Journal of Law, Technology and Policy* 469-485

Voss 2019 *University of Illinois Journal of Law, Technology, and Policy*
Voss WG "Obstacles to Transatlantic Harmonization of Data Privacy Law in Context" 2019 *University of Illinois Journal of Law, Technology and Policy* 405-463

Voss 2020 *Washington International Law Journal*
Voss WG "Cross-Border Data Flows, the GDPR, and Data Governance" 2020 *Washington International Law Journal* 485-532

Voss and Woodcock *Navigating EU Privacy and Data Protection Laws*
Voss WG and Woodcock K *Navigating EU Privacy and Data Protection Laws* (American Bar Association Cleveland 2016)

Yakovleva and Irion 2020 *AJIL Unbound*
Yakovleva S and Irion K "Toward Compatibility of EU Trade Policy with the General Data Protection Regulation" 2020 *AJIL Unbound* 10-14

Yav 2018 *International Journal Data Protection Officer, Privacy Officer, and Privacy Counsel*
Yav C "Perspectives on the GDPR from South Africa" 2018 *International Journal Data Protection Officer, Privacy Officer, and Privacy Counsel* 19-20

Yoo and Blanchette *Regulating the Cloud*
Yoo CS and Blanchette JF *Regulating the Cloud: Policy for Computing Infrastructure* (MIT Press Cambridge, Mass 2015)

Case law

South Africa

Dlomo v Natal Newspapers (Pty) Ltd 1989 1 SA 945 (A)

Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd; In re Hyundai Motor Distributors (Pty) Ltd v Smit 2001 1 SA 545 (CC)

Janit v Motor Industry Fund Administrators (Pty) Ltd 1995 4 SA 293 (A)

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

European Union

Google Spain v Agencia Española de Protección de Datos 317 ECR (13 May 2014)

Schrems and Facebook Ireland v Data Protection Commissioner C-311/18 CJEU (2020)

Schrems v Data Protection Commissioner 310 IEHC (2014)

Schrems v Data Protection Commissioner C-362/14 CJEU (2015)

Legislation

Ireland

Irish Data Protection Act 25 of 1988

Irish Data Protection (Amendment) Act 6 of 2003

South Africa

Constitution of the Republic of South Africa, 1996

Protection of Personal Information Act 4 of 2013

European Union

Commission Decision 2000/520/EC of 26 July 2000 Pursuant to Directive 95/46/EC 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 OJ L 215/7 (2000)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals Concerning the Processing of Personal Data and the Free Movement of Such Data OJ L281/31 (1995)

EU-US Privacy Shield C(2016) 4176 (2016)

EU-US Safe Harbor Agreement (2000)

General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons Concerning the Processing of Personal Data and the Free Movement of Such Data, and Repealing Directive 95/46/EC OJ L 119/1 (2016)

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data OJ L 8/1 (2001)

Government publications

Gen N 309 in GG 44411 of 1 April 2021

International instruments

Charter of Fundamental Rights of the European Union (2000)

Convention for the Protection of Human Rights and Fundamental Freedoms (1950)

Treaty on European Union (2009)

Internet sources

Ahmed 2010 http://ssrn.com/abstract=1712565
Ahmed S 2010 *Data Portability: Key to Cloud Portability and Interoperability* http://ssrn.com/abstract=1712565 accessed 7 May 2022

Article 29 Data Protect Working Party 2012 https://ec.europa.eu/justice/article29/documentation/opinion/recommendations/files/2012/wpl96_en.pdf
Article 29 Data Protect Working Party 2012 *Opinion 05/2012 on the Cloud Computing WP 196* https://ec.europa.eu/justice/article29/documentation/opinion/recommendations/files/2012/wpl96_en.pdf accessed 22 April 2022

Article 29 Data Protection Working Party 2017 https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp254_rev01.pdf
Article 29 Data Protection Working Party 2017 *Adequacy Referential 18/EN WP254 rev.01 (28 November 2017)* https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp254_rev01.pdf accessed 6 April 2024

Charlet 2019 https://news.bloomberglaw.com/privacy-and-data-security/big-google-privacy-fine-may-set-bar-foreuprivacy-penalties
Charlet D 2019 *Big Google Privacy Fine May Set Bar for EU Privacy Penalties,* https://news.bloomberglaw.com/privacy-and-data-security/big-google-privacy-fine-may-set-bar-foreuprivacy-penalties accessed 26 August 2022

CJEU 2015 http://www.europe-v-facebook.org/CJEUhearingnotes.pdf
Court of Justice of the European Union 2015 *Procedure, Protocol of the Hearing* http://www.europe-v-facebook.org/CJEUhearingnotes.pdf accessed 19 September 2022

EU 2020 https://europa.eu/european-union/about-eu/countries_en
European Union 2020 *Country Profiles* https://europa.eu/european-union/about-eu/countries_en accessed 9 April 2024

EU 2021 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
European Union 2021 *Data Protection under GDPR* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data- non-eu-countries-en accessed 5 September 2022

Europe-v-Facebook Organisation Project 2017 http://europe-v-facebook.org/EN/en.html
Europe-v-Facebook Organisation Project 2017 *C-362/14 – Schrems Further Files Concerning the Schrems Case before the CJEU* http://europe-v-facebook.org/EN/en.html accessed 19 September 2022

European Commission 2007 https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charterfundamental-rights_en
European Commission 2007 *EU Charter of Fundamental Rights and Freedoms 2007/C 303/01* https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charterfundamental-rights_en accessed 05 September 2022

European Commission 2020 https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
European Commission 2020 *Adequacy Decision*: *How the EU Determines if a Non-EU Country has an Adequate Level of Data Protection* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en accessed 6 September 2022

Hage and Brown date unknown http://www.johnseely brown.com/cloudcomputingdisruption.pdf
Hage J and Brown JS date unknown *Cloud Computing – Storms on the Horizon* http://www.johnseelybrown.com/cloudcomputingdisruption.pdf accessed 15 April 2022

High Court Commercial 2016 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362
The High Court Commercial 2016 *The Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems, Request for a Preliminary Ruling under Article 267 TFEU (2016) No 4809 P* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362 accessed 27 August 2022

Ireland's National Public Media 2018 https://www.rte.ie/news/2018/0717/979174-eu-japan/
Ireland's National Public Media 2018 *European Union and Japan Sign Historic Trade Deal* https://www.rte.ie/news/2018/0717/979174-eu-japan/ accessed 29 August 2022

Kayali 2019 https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/
Kayali L 2019 *France Hits Google with 50 Million Fine for GDPR Violation* https://www.politico.eu/article/france-hits-google-with-e50-million-fine-for-gdpr-violation/ accessed 19 August 2022

Manyika *et al* 2016 https://www.mckinsey.com//media/McKinsey/Business%20Functions/McKinsey%2ODigital/Our%20Insights/Digital%20globalization%20The%20new%2era%20f%2Oglobal%20flows/MGI-Digitalglobalization-Full-report.ashx
Manyika J *et al* 2016 *Digital Globalization: The New Era of Global Flows* https://www.mckinsey.com//media/McKinsey/Business%20Functions/McKinsey%2ODigital/Our%20Insights/Digital%20globalization%20The%20new%2era%20f%2Oglobal%20flows/MGI-Digitalglobalization-Full-report.ashx accessed13 September 2022

Martin 2011 http://works.bepress.com/timothy_martin/3
Martin TD 2011 *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing* http://works.bepress.com/timothy_martin/3 accessed 21 April 2022

Mckinsey Global Institute 2016 https://www.mckinsey.com/~/media/McKinsey/Business%/`2OFunctions/McKinsey%/`20Digital/Our%/o2Olnsights/Digital%20globalizationo2OThe%20newo20era/o2ofo2Oglobal/o20flows/MGI-Digital-globalization-Full-report.ashx
Mckinsey Global Institute 2016 *Digital Globalisation: The New Era of Global Flows* https://www.mckinsey.com/~/media/McKinsey/Business%/`2OFunctions/McKinsey%/`20Digital/Our%/o2Olnsights/Digital%20globalizationo2OThe%20newo20era/o2ofo2Oglobal/o20flows/MGI-Digital-globalization-Full-report.ashx accessed 7 September 2022

Mckinsey Global Institute 2019 https://www.mckinsey.com/~/media/McKinsey/Featured%/`20Insights/Innovation/Globalizationo2Oino20transitiono2OThe%20future%20fo20trade/o20and%20value%20chains/MGI-Globalizationo2Oin%/o20transition-The-future-of-trade-and-value-chains-Fullreport.ashx
Mckinsey Global Institute 2019 *Globalization in Transition: The Future of Trade and Value Chains* https://www.mckinsey.com/~/media/

McKinsey/Featured%/`20Insights/Innovation/Globalizationo2Oino20transitiono2OThe%20future%20fo20trade/o20and%20value%20chains/MGI-Globalizationo2Oin%/o20transition-The-future-of-trade-and-value-chains-Fullreport.ashx accessed 7 September 2022

Mell and Grance 2011 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
Mell P and Grance T 2011 *The NIST Definition of Cloud Computing* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf accessed 19 April 2022

Meltzer 2020 https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national security/#footnote-1
Meltzer JP 2020 *The Court of Justice of the European Union in Schrems II: The Impact of the GDPR on Data Flows, and National Security* https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/#footnote-1 accessed 9 April 2022

Preston 2008 https://www.informationweek.com/software-services/down-to-business-customers-fire-a-few-shots-at-cloud-computing
Preston B 2008 *Down to Business: Customers Fire a Few Shots at Cloud Computing* https://www.informationweek.com/software-services/down-to-business-customers-fire-a-few-shots-at-cloud-computing accessed 14 April 2022

Wikipedia 2022 https://en.wikipedia.org/wiki/Edward_Snowden
Wikipedia 2022 *Edward Snowden* https://en.wikipedia.org/wiki/Edward_Snowden accessed 26 September 2022

WorldAtlas 2020 https://www.worldatlas.com/nations.htm
WorldAtlas 2020 *How Many Countries Are in the World?* Https://www.worldatlas.com/nations.htm accessed13 September 2022

List of Abbreviations

AI	Artificial Intelligence
AJIL Unbound	American Journal of International Law Unbound
CILSA	Comparative and International Law Journal of Southern Africa
CJEU	Court of Justice of the European Union
GDP	Gross Domestic Product

DPC	Data Protection Commissioner
EC	European Commission
EDPL	European Data Protection Law Review
EU	European Union
GDPR	General Data Protection Regulation
IDPL	International Data Privacy Law
IoT	Internet of Things
Iowa L Rev	Iowa Law Review
IR	Information Regulator
ISJLP	I/S: A Journal Law and Policy for Information Society
IT	information technology
J Int'l Econ L	Journal International Economic Law
J Marshall L Rev	John Marshall Law Review
MLA	Mutual Legal Assistance
NDPA	National Data Protection Authority
NSA	National Security Agency
NWULR	Northwestern University Law Review
PELJ	Potchefstroom Electronic Law Journal
POPIA	Protection of Personal Information Act 4 of 2013
SA	South Africa
SA	Supervisory Authority
SAJHR	South African Journal on Human Rights
SALRC	South African Law Reform Commission
THRHR	Tydskrif vir Hedendaagse Romeins-Hollandse Reg / Journal of Contemporary Roman-Dutch Law
US	United States