Cross-Border Data Flows and the *Protection of Personal Information Act* 4 of 2013 – Part II: The Data Transfer Provision

J Coetzee*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Juana Coetzee

Affiliation

Stellenbosch University, South Africa

Email

jcoet@sun.ac.za

Date Submitted

25 November 2022

Date Revised

31 May 2024

Date Accepted

31 May 2024

Date Published

7 November 2024

Editor

Prof W Erlank

Journal Editor

Prof C Rautenbach

How to cite this contribution

Coetzee J "Cross-Border Data Flows and the Protection of Personal Information Act 4 of 2013 – Part II: The Data Transfer Provision" *PER / PELJ* 2024(27) - DOI http://dx.doi.org/10.17159/1727-3781/2024/v27i0a15234

DOI
http://dx.doi.org/10.17159/1727-3781/2024/v27i0a15234

Abstract

The *Protection of Personal Information Act* 4 of 2013 (POPIA) was introduced to protect the right to privacy of the South African data subject. The Act prescribes obligations that a responsible party must fulfil to achieve this purpose. However, personal information is very often collected and processed by responsible parties who are outside the Republic. Alternatively personal information is collected by a responsible party in the Republic and then transferred out of the country. Part I of this article discussed the territorial scope provision (section 3) and concluded that it can give rise to interpretative uncertainties with the result that personal information processed by responsible parties outside the Republic would not be covered by the Act. However, responsible parties often move their processing activities out of the country to escape liability. This part of the article analyses the data transfer provision (section 72), a provision that is directed at the regulation of the transfer of data outside the Republic. Section 72 lays down certain conditions before a responsible party can export data out of the Republic to a third party. The discussion will show that the provision has certain shortcomings which could limit its effectiveness in providing the necessary protection if compared to its counterpart in the EU *General Data Protection Regulation* (GDPR). Consequently, legislative revision or clarification by the Information Regulator in the form of a Guidance Note would be welcomed. The article concludes with a brief analysis of the interplay between sections 3 and 72 to illustrate the need for both these provisions in our law.

Keywords

POPI/POPIA; personal information; cross-border data transfers; section 72 POPIA

.....

1 Introduction

Data protection laws are aimed at protecting the processing of a data subject's personal information. However, this protection might be circumvented if the responsible party is located outside the borders of the country that regulates such processing, or by moving the data out of the country, such as when the processing of the data takes place outside the country. To protect a data subject's rights in these circumstances data protection laws include two types of provisions, namely territorial scope provisions and data transfer provisions.

Part I of this article[1] discussed the territorial scope provision of the *Protection of Personal Information Act* 4 of 2013 (hereafter POPIA or the Act). Section 3 of POPIA provides for two instances where the Act finds application, namely (i) if the responsible party is domiciled in the Republic, for example where its business or company is incorporated or controlled from the Republic,[2] or (ii), where it makes use of an automated or non-automated means of processing in the Republic.[3] In part 1 an analysis of these grounds was undertaken which was informed by the interpretation given to Article 4 of the *EU Data Protection Directive*[4] (hereafter DPD) and the current Article 3 of the *EU General Data Protection Regulation*[5] (hereafter GDPR). This interpretation showed that section 3 of POPIA can

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

1 See Coetzee 2024 *PELJ* DOI: http://dx.doi.org/10.17159/1727-3781/2024/v27i0a15233.

2 Section 3(1)(b)(i) of the *Protection of Personal Information Act* 4 of 2013 (POPIA). Part 1 argued that this notion should not be interpreted formalistically or narrowly but that it should include cases where the responsible party conducts a stable activity in the Republic for an indefinite period of time that can be linked to the processing of the data subject's personal information.

3 Section 3(1)(b)(ii) of POPIA. A comparative analysis with the position in the European Union (EU) showed that automated means are equivalent to the use for the automatic processing of personal information of equipment which is located in the Republic, such as servers, computers, cellphones and other devices. Where a responsible party in another country intentionally makes use of equipment, for example, cookies, sensors, banners etc that it controls, or any other mechanism that automatically collects personal information from a data subject through a device located in the Republic of South Africa (RSA), such as when accessing a website, this will bring the responsible party under the ambit of POPIA.

4 *Directive 95/46/EC of the European Parliament and of the Council enacted 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* [1995] OJ L 281/31 (hereafter the DPD).

5 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 (hereafter the GDPR).

find extra-territorial application and bring the processing activities of non-South African responsible parties taking place outside the borders of the country within its reach if a territorial link between the responsible party and the Republic can be established.

However, the cross-border movement of personal data can also take place where a responsible party in the Republic transfers personal information out of the country to be processed in a so-called third-party country. For example, a company incorporated in South Africa exports personal data of its customers and employees to be processed in another country. This aspect is explicitly regulated by the Act in section 72 of POPIA, the so-called data transfer provision. Data transfer provisions do not bring responsible parties or other data processors under the scope of a data protection law such as POPIA. The purpose of a data transfer rule is to make sure that when a data subject's personal information is moved to another country, it will enjoy a level of protection similar to what it would have under POPIA.

South African courts have not dealt with this issue yet; but the issue of international data flows has already landed before the European courts on a number of occasions, such as in the well-known judgments of *Maximillian Schrems v Data Protection Commissioner*[6] (hereafter *Schrems I*) and *Data Protection Commissioner v Facebook Ireland, Maximillian Schrems*[7] (hereafter *Schrems II*) by the European Court of Justice (ECJ). These cases originated in a complaint by Max Schrems brought in Ireland against the Irish Data Protection Commissioner to request that the transfer of his personal data from Facebook Ireland to the servers of Facebook Inc in the United States of America (USA), where the data is processed, be suspended or prohibited. He argued that the laws of the USA did not adequately protect his personal data against the surveillance activities of public authorities in the USA, such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), which infringed his human rights in terms of the Charter of Fundamental Human Rights of the EU. After the Commissioner rejected his complaint, Mr Schrems referred the matter to the High Court (Ireland) for review. The High Court requested a preliminary ruling from the ECJ on the interpretation and validity of the Commissioner's decision and on the Commissioner's adequacy decision underlying the Safe Harbor arrangement between the EU and the USA. In the initial proceedings (*Schrems I*), the ECJ declared the Commissioner's decision, as well as the adequacy decision, invalid and referred the matter back to the Commissioner. After further investigation the Commissioner found that the data had been transferred in terms of standard data

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

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

protection clauses (SCCs) contained in an EU SCC Decision, which fall under an exception to the GDPR's data transfer provision. The Commission furthermore replaced the Safe Harbor agreement with the Privacy Shield. However, Mr Schrems contended that the SCC Decision could not justify the infringement of his human rights by the US authorities which would take place by monitoring his personal information by means of their various monitoring programmes. Subsequently, the Commissioner published a draft decision in which she found that the US security agencies' processing activities were indeed infringing on an EU data subject's human rights and that the SCC Decision fails to provide adequate remedies to address such violations, since they confer contractual rights on the data subject against the data exporter and importer only and not any rights against the US authorities. The Commissioner then approached the High Court on the question of the SCC Decision's validity. The High Court in turn referred the matter to the ECJ to determine various questions relating to the SCCs and the Privacy Shield arrangement that replaced the Safe Harbor arrangement. In *Schrems II* the ECJ declared the Privacy Shield invalid but upheld the use of SCCs. However, it was held that data controllers must still ensure that the standards of data protection in the third country provide adequate protection similar to those in the EU even when SCCs are used.

It is quite common for data protection laws to make use of both territorial scope provisions and data transfer provisions when it comes to regulating the processing of personal information outside the country of the data subject. This is also the case in the GDPR. However, questions have arisen on the efficacy of having two sets of rules regulating the same case, for instance where a foreign data controller (the responsible party) or processor (the operator) is subject to the data protection law of a country by virtue of its territorial scope rule but at the same time the data transfer rule will apply to the transfer of information out of the country.[8] New Zealand and the United Kingdom (UK) recently addressed the interplay between the territorial scope and data transfer provisions in their data protection laws by way of statutory revision and consequently removed the application of data transfer rules in instances where respectively the *Privacy Act* 2020[9] and the UK-GDPR[10] would apply to the third party by virtue of the normal application of the territorial scope rule. This warrants closer investigation of the interplay between and the value of having both rules apply to the same set of facts. Clarity on the content of these laws and their interaction is necessary for several reasons: Data subjects need to know if and how their personal data

8 Kuner 2021 https://ssrn.com/abstract=3827850 5.

9 New Zealand *Privacy Act* 31 of 2020.

10 The *United Kingdom General Data Protection Regulation* (UK-GDPR) took effect on 1 January 2021 and operates alongside the *Data Protection Act* of 2018, which gives effect to the UK-GDPR, and the *Privacy and Electronic Communications (EC Directive) Regulations* 2003.

are protected once the data leaves the borders of the Republic, responsible parties and processors (operators) have to be clear on their duties as they are the ones who have to implement the protective measures, and those who have to enforce the provisions of the Act dealing with the transfer of personal data and its processing in third countries need clarity not only on the content of the rules but also on when the Act applies.

Chapter 9 of POPIA regulates transborder information flows. This chapter comprises a single provision, section 72, which regulates the transfer of personal information by a responsible party in the Republic to a third party in a foreign country. Section 72 is aimed at balancing the free flow of information with the data subject's right to protection of its personal information. Furthermore, the aim is to keep safe personal data that is processed subject to POPIA by requiring that the responsible party ensures an adequate level of protection for the data when the data leaves the country.

Chapter V of the GDPR, on the other hand, contains a number of provisions regulating the processing of EU data subjects' personal information outside the Union.[11] Compared to the GDPR, the SA data transfer rule is more limited in its scope and merely deals with aspects addressed by Articles 44,[12] 46, 47 and 49 of the GDPR. For the purposes of this discussion section 72 will be compared to the equivalent provisions in the GDPR. Note that the GDPR uses different terminology when referring to responsible parties and operators and that they are respectively referred to as "data controllers" and "processors".

In this contribution the aim is to analyse the content and requirements of section 72 of POPIA and compare this provision to its European counterpart to establish its efficacy and whether there is room for improvement. In the final instance, the article investigates the need for having both a territorial scope provision as well as a data transfer rule.

2 The transfer of data provision

2.1 General requirements for the application of section 72

Section 72 of POPIA[13] states:

11 Articles 44-50 of the GDPR; EDPB 2021 https://edpb_guidelines interplaychapterv_article3_adopted_en.pdf para 1.

12 Article 44 of the GDPR includes transfers to international organisations. It also includes transfers by processors to third parties in other countries.

13 This provision tracks that of Art 25 of the DPD. See Roos *Law of Data (Privacy) Protection* 226-235, Roos 2007 *SALJ* 411 *et seq*.

> (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless-
>
> (a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that-
>
> (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and
>
> (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
>
> (b) the data subject consents to the transfer;
>
> (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
>
> (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
>
> (e) the transfer is for the benefit of the data subject, and-
>
> (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
>
> (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Before section 72(1) can find application, certain requirements must be met, namely (i) the transfer must be done by a responsible party in the Republic; (ii) personal information must be transferred out of the Republic; and (iii) the information must be transferred to a third party in another country. However, where special personal information or the personal information of a child is to be transferred out of the Republic, section 57(1)(d) of POPIA determines that the transfer can take place only with the prior authorisation of the Information Regulator if the third-party country does not provide an adequate level of protection as envisaged in section 72.

2.1.1 Transfer by a responsible party in the Republic

According to the Act, a responsible party is "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[14] According to this definition, the term responsible party has a limited meaning and must

[14] Section 1 of POPIA.

be distinguished from an operator or processor who acts on behalf of the responsible party in processing the data, i.e. physically collecting, analysing and storing data. An operator is an independent party who does not come under the direct authority of the responsible party, such as an employee, and who processes data in terms of a contract with or mandate of the responsible party.[15] Unlike the position in Article 44 of the GDPR, section 72 of POPIA does not provide for transfers by operators or processors. Does this mean that a transfer of personal information by an operator in the Republic to a third party outside the Republic will not be subject to section 72? A literal reading of the provision seems to suggest that. This also seems to be the view of some South African authors, who note that this might at most be a breach of section 20(b), and that the contract between the responsible party and the operator must specifically regulate the transfer in these circumstances.[16]

In sections 20 and 21 POPIA deals specifically with situations where an operator processes information on behalf of a responsible party in terms of a contract or mandate. According to section 20 the operator or anyone who processes information on behalf of the responsible party can process such information only with the knowledge or authority of the responsible party,[17] these parties are obliged to treat the information as confidential and they may not disclose such information to a third party unless required by law or in the proper performance of their duties.[18] According to section 21, the responsible party must conclude a written contract[19] with the operator, which must provide that the operator take security measures in regard to such information, and the latter must notify the responsible party if there is reason to believe that a data subject's personal data was accessed or acquired by an unauthorised person.[20] No mention is made of a sub-operator in this section. The responsible party, however, remains the party obliged by the Act to meet the conditions for lawful processing, and if the operator or anyone acting on behalf of the operator or on its instructions fails to do so, the responsible party will remain, true to its name, responsible and liable to the data subject.[21]

If the operator transfers information to another processor, inside or outside the Republic, this is to take place with the knowledge or authority of the responsible party.[22] This implies that if the contract between the responsible

15 Section 1 of POPIA.
16 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.1.3.
17 Section 20(a) of POPIA.
18 Section 20(b) of POPIA.
19 Section 21(1) of POPIA.
20 Section 21(2) of POPIA.
21 Section 8 of POPIA.
22 Section 20(a) of POPIA.

party and the processor does not explicitly provide for the transfer of personal information by a processor to a sub-processor, it can take place only with the knowledge or authorisation of the responsible party. This means that the responsible party, at the very least, must be informed of the processing. It is not clear whether notice must be given prior to the processing taking place or whether mere reporting of the fact would suffice. However, it is submitted that notice must be given before the processing takes place so that the purpose of section 20, and especially that of section 21, is not defeated. Knowledge on the part of the responsible party would possibly be construed as some form of implied authorisation. Therefore, even if section 72 will not find application *per se*, or the processor will not automatically be obliged to comply with its conditions, the responsible party remains obliged to the provisions of POPIA and must make sure that its processors or operators comply with its requirements. The contract or mandate with the processor, therefore, should not only set out the duties of the operator insofar as security measures are concerned but it should also impose duties similar to those in section 72 on an operator who transfers data out of the country. However, in the interest of clarity, and to protect the rights of a data subject, it is submitted that the legislature should explicitly extend the scope of 72 to include operators, as is currently the case in the GDPR. That would spread the risk more evenly if the operator, without the knowledge of the responsible party, fails to comply, or if lack of knowledge on the part of the responsible party might be construed as a loophole that discharges the responsible party from any liability.

Section 72(1) refers to a responsible party in the Republic. Does this require a physical presence in South Africa? The legislature's choice of words differs from that used in section 3(1)(b), which requires either South African domicile[23] or using a means of processing in the Republic.[24] This could give rise to an inference that the data transfer provision will not apply to both categories of responsible parties as envisaged in section 3(1)(b)(i) and (ii), because if that were the intention of the legislature, it could have stated so clearly. On the one hand, if one compares this provision to the DPD on which it was modelled, Article 25 of the DPD refers merely to the transfer of data to a third party but makes no mention of who is making the transfer. There is therefore no indication of any limitation to responsible parties. Article 46 of the GDPR, on the other hand, refers to a controller or processor transferring data from an EU country to a third country without stating any location requirements for these parties. Commentaries state that these parties can be established in or outside the EU but must meet the territorial

23 Section 3(1)(b)(i) of POPIA.
24 Section 3 (1)(b)(ii) of POPIA.

criteria of Article 3.[25] In line with this interpretation, it is submitted that our section 72 should include responsible parties domiciled in South Africa under the broader interpretation of section 3(1)(b)(i), as well as those falling under the ambit of the Act on the basis of section 3(1)(b)(ii) if the means of processing used is located in the Republic.[26] In short, any responsible party who falls under the scope and ambit of POPIA by virtue of section 3(1)(b) and who transfers personal information out of the Republic should meet the conditions of section 72.

However, where a data subject contracts online via a foreign website and provides their personal data on their own initiative by completing the necessary form and the information is transferred out of the Republic, the transfer will not be regulated by section 72. Here it is the data subject who transfers the information and not the responsible party, as required by this section.[27] EU scholarship has challenged this conclusion by arguing that such an interpretation might leave a gap in protection. According to this view, where the responsible party in the third country controls the technical means (i.e. the website) by which data subjects send their information, the responsible party is in control of the actions that result in the data being processed and, therefore, is in effect the party who is sending or making the data available. Consequently, such a responsible party would fall under the ambit of both the territorial scope provision as well as the data transfer provision if the data is exported to a processor or operator in the third country.[28] However, where information so collected is transferred directly back to the responsible party in a third country, the data transfer rule cannot find application as it requires a transfer from a responsible party to a third

25 See EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted-en.pdf paras 9 and 10.

26 See ss 2.3 and 2.4 of part I of this article dealing with the territorial scope provision.

27 EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf 5-6 para 12. In *Bodil Lindqvist* (Case C-101/01) [2003] ECLI:EU:C:2003:596, the European Court of Justice (ECJ) held that there was no data transfer to a third country within the meaning of the DPD when an individual in a Member State of the EU loaded personal data onto an Internet page stored on a site hosted within the EU. This position is confirmed in the context of ch V of the GDPR.

28 Kuner 2021 https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr. He concedes, however, that on this interpretation if the data are transferred directly to the responsible party, a standard contract clause (SCC) concluded under Art 46(2)(c) would not find application as the processor (the responsible party) cannot sign the contract as both the exporter and the importer of the information. Still, the transfer would be protected by virtue of the territorial scope provision. Also see SALRC 2009 https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf 403 where, with reference to the *Bodil Lindqvist* case, it is pointed out that once that information is accessed in a third country there will be a transfer of information; moreover, where the information is uploaded with the intention that it is to be accessed in a third country, that will also constitute a transfer.

party. It would therefore apply only where data collected via the responsible party's website is transferred to an operator in a third country.[29]

If the device used by the data subject is located in the Republic and the responsible party makes use of an automated means of processing located in the Republic[30] that processes data subjects' personal information without their input or consent, POPIA will still find application in these circumstances by virtue of section 3(1)(b)(ii). However, a territorial scope provision *per se* provides a lower level of protection than a data transfer rule as it depends on the application and enforcement of a data protection law against a foreign party in a foreign jurisdiction. In these circumstances, the data transfer provision will afford additional protection.[31] However, this would further depend on whether our courts are amenable to interpreting "responsible party" as used in the context of section 72 according to an extended interpretation of section 3(1)(b)(ii), and as explained above, the data transfer rule will find application only if the transfer is done to a third party.

Furthermore, where data is processed in South Africa by a processor or operator on behalf of a non-South African responsible party and the data is transferred back from the Republic to the responsible party, section 72 will not apply since the first condition is not met, namely that the responsible party in the Republic must be the one exporting the data out of the country.[32] A processor or operator does not determine the purpose and means of processing and therefore cannot function as a responsible party. This differs from the legal position in the GDPR, where processors are subject to the Regulation in terms of the territorial scope rule when the processing takes place in the context of the establishment of a processor in the Union,[33] but they simultaneously also fall under the data transfer rule.[34] Moreover, if data is processed outside the country and sent back to the Republic the import of such information back into the country will not be subject to section 72, as it applies only to data exports out of the Republic. However, this does not mean that information will be unprotected during that time. As previously discussed, section 21 of POPIA determines that there must be a written

29 Also see EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf paras 14 and 15.

30 For example, by using cookies which are "equipment capable of operating automatically in response to instructions given for the purpose of processing information" (see the definition of "automated means" in s 1 of POPIA).

31 Kuner 2021 https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr.

32 In line with what was said above, if a non-South African responsible party falls under the scope of POPIA by virtue of s 3(1)(b)(ii), the responsible party will have to comply with the provisions of the Act, and ss 20 and 21 will find specific application.

33 Article 3(1) of the GDPR.

34 Article 44 of the GDPR.

contract between the responsible party and the third-party operator that makes provision for security measures. It is submitted that this contract should also make provision that data which is processed outside the country is to be transferred safely back into the Republic. Moreover, section 72(1)(a) provides for a binding agreement between the responsible party and a third-party operator or processor located outside the Republic, which will regulate the export of data and can be used to stipulate conditions for the return of the information as well.[35]

2.1.2 Transfer of data out of the Republic

Transferring data normally entails the transmission of data from one place to another or from one person to another. However, transfers can also take place passively. For example, if personal information is available on a website, the information will not be "transferred" for the purposes of section 72 until a third party in another country has accessed the information.[36] Where data is merely transmitted through a server situated in another country, such as where an email transitions across servers, that does not constitute a transfer of personal information as envisaged by section 72.[37]

2.1.3 Transfer to a third party outside the Republic

The legislator chose to use the term "third party" to refer to the data importer. This includes a range of persons, natural or juristic. The EU regulation states it even more generally by requiring that data is to be transferred to a third country or an international organisation.[38]

Where an employee of a responsible party accesses personal data remotely while outside the Republic, section 72 will not find application because the employee is not a "third party" but a representative of the responsible party.[39] In most instances where personal information is transferred to a third party outside the Republic, the third party will be an operator (processor) or other service provider. "Third parties" may include another

35 See the discussion of SCCs in section 2.2.3 of this article.

36 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.1.3.

37 Papadopoulos and Snail ka Mtuse *Cyberlaw@SA IV* para 10.3.6.3.11.

38 Article 45 of the GDPR. Its predecessor, Art 25 of the DPD, refers only to a third country. Note that there is a discrepancy in POPIA in this regard: while s 72 mentions only "a third party who is in a foreign country", s 18(1)(g) refers to the responsible party's duty to inform the data subject if it intends transferring information to "a third party or international organisation" and also of the level of protection that will be afforded to the information so transferred. The latter section tracks the wording of the GDPR more closely than s 72 does even though it was modelled on the DPD. The discrepancy between ss 72 and 18(1)(g) is quite strange in the light thereof that they deal with the same topic.

39 EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf para 14. The responsible party must ensure that security measures are applied to the information when it is in the possession of the employee as per s 19 of POPIA.

responsible party or a jointly responsible party; however, it will depend on the facts whether the exporter and importer are two separate parties.[40] The general rule is that the third party must not stand under the direct authority or control of the responsible party.[41] Therefore, in a corporate group a transfer to a subsidiary may not be a transfer to a third party if the exporter controls the importer of the data. However, if data are transferred to another entity in the same corporate group who determines or co-determines the purpose and means of the further processing of such data and it meets the requirements of an independent and separate responsible party, or if the importing entity acted as an operator, it would suffice as a third party for the purposes of section 72. For example, if company A in the RSA, which is a subsidiary of parent company B in India, sends the personal data of its customers and employees to company B to be held there in a centralised database, company A will be a responsible party exporting data to an operator (a processor) in a third country. Even if on the facts the data transfer provision does not find application, the responsible party will still be obliged to fulfil its obligations under POPIA and make sure that the data is kept safe and secure, even when it leaves the Republic. Furthermore, a data subject must be notified of the transfer of its personal data,[42] and the data may not be retained beyond the conclusion or performance of the transaction that necessitates the transfer.[43]

Where personal data is exported to a data processor operator outside the Republic, the conditions of sections 20 and 21 must still be met, namely that a contract is to be concluded setting out the duties of the operator. If a responsible party concludes a binding agreement (SCC) with the third party, as envisaged by section 72(1)(a), the conditions of sections 20 and 21 should be included in the agreement if they otherwise do not form part of the standard clauses. Section 72(1)(a)(ii), furthermore, states that if a data importer in a foreign country transfers the data onwards to another country, the processor or operator must be subject to the same conditions as would apply to responsible parties transferring data out of the country. It therefore follows that the law in the third-party country must at a minimum comply with the same principles as those on which POPIA is based. Alternatively such further transfers must be regulated by binding corporate rules (BCRs) or standard contract clauses (SCCs).

---

40 EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf paras 11-16. Where data are disclosed between entities in the same corporate group, this could constitute the transfer of information from one responsible party to another responsible party.

41 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.1.3.

42 Section 18(1)(g) of POPIA.

43 Section 14 of POPIA.

2.2 Conditions for data transfers

Section 72 determines that personal data can be transferred to a third party in another country only if that party is subject to a law, BCRs or a binding agreement with the responsible party that provides an "adequate level of protection". Article 46 of the GDPR requires similar "appropriate safeguards" but the list includes additional measures such as codes of conduct, certification mechanisms, ad hoc contractual clauses and international agreements or administrative arrangements.[44] POPIA also provides for codes of conduct[45] but this is not expressly in connection with the export of data. However, it would not be impossible or inappropriate to make use of these measures to safeguard personal data that is transferred out of the Republic, especially in situations where section 72 cannot find application. As POPIA merely prescribes minimum requirements, the parties are free to increase their duties in this regard at any time. What is important is that whatever measure is used it must be fine-tuned to the circumstances to fill any gaps in POPIA.[46] Responsible parties must also be aware of potential risks that may exist in another country, not only as regards shortcomings in its data protection laws but also in the form of other legislation that, for instance, require the disclosure of information for security purposes.[47]

2.2.1 Law that provides an adequate level of protection

Section 72 does not extend the application of POPIA *per se* so that it will apply automatically to the third party. It merely requires that the third party (the data importer) must be bound to a data protection law providing an adequate level of protection. What does this entail?

A comparative investigation reveals that, whereas section 72(1)(a) requires "an adequate level of protection", Article 46 of the GDPR requires "appropriate safeguards" to ensure "enforceable data subject rights and effective legal remedies for data subjects".[48] Its predecessor, Article 26(1) of the DPD, referred to these measures as "an adequate level of protection", similarly to what is required in section 72 POPIA. However, the requirement of "an adequate level of protection" is set in Article 45 of the GDPR dealing with so-called adequacy decisions. In *Schrems I* the ECJ interpreted "an

---

44 Woods 2020 https://eulawanalysis.blogspot.com/2029/07/you-were-only-supposed-to-blow-the-bloody.html?m=1.

45 Chapter VII of POPIA.

46 See EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf para 23.

47 See the facts in *Schrems I* and *Schrems II*.

48 POPIA makes mention of "safeguards" only in Condition 7, security safeguards in ch 3 dealing with the conditions for the lawful processing of personal information, and also in s 19 in connection with operators and processors who process on behalf of a responsible party.

adequate level of protection" as measures that afford protection "essentially equivalent" to those of the GDPR. In *Schrems II* the ECJ read Articles 45 and 46 together and even though Article 46 requires "appropriate safeguards", the Court used the essentially equivalent test here as well.

Therefore, an adequate level of protection would be met when the law of the third party's country upholds principles or conditions for reasonable processing that are substantially similar to those subscribed to in POPIA. These conditions are accountability;[49] a processing limitation;[50] a purpose specification;[51] further processing limitation;[52] information quality;[53] openness;[54] security safeguards;[55] and data subject participation.[56] In addition, the instrument must also contain measures similar to those required in section 72 to protect the onward transfer of the data subject's personal data. In essence, this means that third parties must apply protective measures that are "substantially similar" to the conditions stated in POPIA when they process personal data imported from South Africa and that "substantially similar" principles must apply when such data is transferred from that country to yet another country. Section 72 therefore does not require that all POPIA's provisions must be upheld by the third party but merely that the foreign law must subscribe to substantially similar principles and conditions for data processing as those set out in POPIA.

The Act does not afford the Information Regulator or another body, institution or official with any duty or authority to determine whether the law of the third-party country provides such an adequate level of protection. It would seem that it is the duty of the responsible party to make that determination. In practice this would mean that the responsible party must obtain legal advice every time it makes use of a processor in another country to ensure that the requirements of section 72 are met. South African commentators have expressed doubt as to whether legal practitioners would feel comfortable doing so as it requires remarkable expertise, which most do not have. They furthermore fear that this will give rise to data localisation as responsible parties might avoid transferring data to other destinations, which will have cost implications and will affect the free flow of

49 Section 8 of POPIA.
50 Sections 9-12 of POPIA.
51 Section 13-14 of POPIA.
52 Section 15 of POPIA.
53 Section 16 of POPIA.
54 Section 17-18 of POPIA.
55 Section 19-22 of POPIA.
56 Section 23-25 of POPIA.

information negatively and deter investment.[57] There is therefore a clear need for the Information Regulator to provide guidance in this regard.[58]

If compared to the position in the EU, Article 45 of the GDPR provides for an adequacy decision which could perhaps simplify matters. This entails that the EU Commission may decide that a third country or an international organisation offers an adequate level of data protection, which will then apply to all Member States.[59] This makes it easier for a data controller as it immediately knows it is safe to transfer data to a third-party country that has received an adequacy decision. What is interesting is that a wide range of factors are taken into consideration before an adequacy decision is given. Apart from the principles and conditions of the country's data protection laws the Commission also takes into account whether the country supports the rule of law, protects human rights, and generally has effective enforcement procedures available, among other things.[60] Although section 72 of POPIA does not contain a similar provision, it would be worthwhile to consider these aspects in addition to inquiring whether the third-party country's laws have substantial similarities with POPIA when determining whether an adequate level of protection exists in that country.

Because of the immense burden placed on responsible parties, they might instead want to make use of agreements (SCCs) with the data importer to protect the rights of the data subject. However, as the discussion of that measure will show, this might place a similar burden on a responsible party.

2.2.2 Binding corporate rules

Section 72(1) allows the export of data across borders within a group of undertakings if BCRs provide an adequate level of protection. BCRs are defined in section 72(2)(a) as "personal information processing policies

---

57 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.1.

58 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.1.

59 Recital 103 of the GDPR.

60 Recital 104 of the GDPR indicates the following factors to be considered when coming to such a decision: how the third country respects the rule of law, its access to justice and its conformity with international human rights norms and standards, its general and sectoral law, including its legislation concerning public security, defence and national security, as well as its public order and criminal law, together with other criteria such as its specific processing activities and the scope of its applicable legal standards and legislation; the third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the EU; it should ensure independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress. Recital 105, furthermore, mentions the third country's international commitments and its participation in multilateral or regional systems.

within a group of undertakings" which the responsible party is part of. A "group of undertakings", in turn, is defined in section 72(2)(b) as "a controlling undertaking and its controlled undertakings". This would cover situations where transnational companies deal with the processing of data in different locations but in the same corporate structure. Normally section 72 will not find application if data is transferred from a responsible party to a co- or jointly responsible party in the same corporate structure but in another country where the importer is not acting as a different responsible party, as data is not exported to a third party as required by the section. However, this must be determined on a case-to-case basis.[61] Notwithstanding, BCRs that provide an adequate level of protection could address any uncertainties in this regard.

The meaning and content of the term "adequate level of protection" is the same as is required in the context of a law that provides adequate protection. It is submitted that BCRs should not only provide levels of protection similar to those provided in POPIA but also mechanisms that can ensure effective enforcement of these obligations. Article 47(1) of the GDPR requires that a corporate group's BCRs must expressly make provision for the acceptance of liability or audit and verification processes, as well as confer enforceable rights on data subjects.[62] Although POPIA does not require any of these, it is prudent that BCRs should address these aspects in the absence of any other contractual agreements. Article 47(2) of the GDPR furthermore lists specific content that must be specified in corporate rules, amongst others the nature of the personal data to be transferred; the type and purpose of the processing; the conditions under which the processing will take place; the identification of the third countries in question; the binding nature and enforcement of the rules; the rights of data subjects; and complaint procedures. Article 47 of the GDPR also contains other requirements that are more stringent than those in its POPIA counterpart. BCRs furthermore must be pre-approved by a competent supervisory authority, which is not required by POPIA. Again, guidance from the Information Regulator would be useful on the content of these agreements, and the GDPR could provide some valuable direction in this regard.

2.2.3 Binding agreement

The third way personal data can be transferred out of the country is via a binding agreement between the responsible party and the third party, which provides an adequate level of protection in that it upholds substantially the same principles or conditions for data processing as those subscribed to by

61 EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf para 16.

62 See Kuner 2021 https://ssrn.com/abstract=3827850 27.

POPIA. The agreement must also contain a provision(s) similar to that of section 72 regulating further transborder data flows. No definition is provided for a "binding agreement between the responsible party and the third party". However, in practice such agreements usually take the form of standard data protection clauses or standard contract clauses (SCCs).

The GDPR requires that, for SCCs to function as an appropriate safeguard, they must be "adopted by the Commission in accordance with the examination procedure referred to in Article 93(2)"[63] or "adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2)".[64] The EU Commission formulated SCCs to ensure appropriate data protection safeguards for international data transfers as required by the GDPR. These clauses serve as minimum requirements. They may be supplemented or included in wider contracts if the latter do not contradict the SCCs or prejudice the fundamental rights or freedoms of data subjects.[65] The EU Regulation furthermore makes provision for SCCs that are specifically applicable to onward transfers. The SCCs were formulated in 2001 under the DPD, and were thereafter revised in 2010 after the GDPR had been introduced[66] and again amended in 2016[67] after *Schrems 1*. The SCCs came under scrutiny in *Schrems II* but the ECJ held that they are valid. However, "the widespread use of new and more complex processing operations often requiring multiple data importers and exporters, long and complex processing chains, and evolving business relationships"[68] necessitated further revision, and a new set of clauses was published in 2021.[69] The 2021 SCCs were a direct result of the decision in *Schrems II*.

Neither POPIA nor its regulations make provision for pre-approved standard clauses or for the Regulator to approve any other standard agreements (apart from codes of conduct). It would seem that the burden is on the responsible party to enter into the appropriate agreement with the third party

63 Article 46(2)(c) of the GDPR.

64 Article 46(2)(d) of the GDPR.

65 Recital 3 of *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contract clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31.

66 *Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46* [2010] OJ L 39/5.

67 *Commission Implementing Decision (EU) 2016/2297 of 16 December 2016* [2016] OJ L 344/100.

68 *Schrems II* para 6.

69 *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contract clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31.

to ensure that an adequate level of protection is in place when the third party processes the information received. This is quite a heavy burden, especially in that the responsible party remains responsible for the lawful processing of a data subject's personal data throughout the lifespan of such data. Again, guidance by the Information Regulator is needed in this regard. The way the GDPR provides direction in these matters is commended and could serve as a useful example.

Furthermore, even if the appropriate SCC is in place section 72 does not make the provisions of POPIA applicable to the third party *per se* but it merely ensures that the data subject's personal information enjoys protection equal to that provided by POPIA. That immediately raises the question as to the rights of a South African data subject if its personal data is processed unlawfully in a foreign country by a third party after the data was transferred there by a responsible party in the Republic. It seems that POPIA places the liability squarely on responsible parties. They must make sure that the transfer takes place subject to the processing conditions of POPIA. Furthermore, it is the responsible party's duty to inform the data subject of the transfer of its personal data.[70] If the transfer does not take place in accordance with the conditions set out in section 72(1)(a), the data subject can approach the Information Regulator for assistance, alternatively the courts. However, in practice the fact that the responsible party failed to meet the conditions of section 72 will have no real effect until the data subject becomes aware that its information was processed in a manner inconsistent with the Act, and then its rights would be enforceable against the responsible party, and not the third party *per se.*

In the context of the EU's pre-approved SCCs, recital 12 of the 2021 Commission Implementing Decision on standard contractual clauses for the transfer of data to third countries[71] states that with some exceptions, data subjects who are not parties to the contract between the responsible party and the third party should be able to invoke and enforce the contract clauses as third-party beneficiaries if the choice-of-law of these contracts make provision for the enforcement of third-party rights. The data importer must also submit to the jurisdiction and other administrative requirements of the country (recital 13) and to compensation for the data subject (recital 14). In South Africa a data subject's rights are primarily enforceable against the responsible party unless a SCC between the responsible party and a third party makes specific provision for a right of recourse against the third party. Apart from a *stipulatio alteri*, our law normally does not provide rights to

70 Section 18(1)(g) of POPIA.

71 *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contract clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31.

someone who is not a party to the original contract. Moreover, if such a right is to be enforced in a third-party country, that could complicate matters even further, as that would depend on the law of that country and whether third-party rights are enforceable there.

In *Schrems II* the ECJ stated that SCCs as a tool for cross-border data transfers will suffice only if the third-party country in addition also has data protection provisions in place that are equivalent to those in the GDPR. This is quite a strict interpretation aimed at the protection of privacy rights. A literal reading of section 72(1)(a) does not seem to require this. However, only time will tell how South African courts or the Information Regulator will approach this matter.

2.3 Exceptions

Section 72(1)(b)-(e) furthermore contains certain derogations or exceptions where a third party does not have to comply with the conditions for data processing, such as where the data subject consented to the transfer, where the transfer is necessary in the interest of the data subject, or where the risks are relatively small. These derogations are allowed based on public policy as it is in the interest of the public or the data subject that the transfer takes place. As a result, these exceptions must be interpreted restrictively.[72]

2.3.1 The data subject consented to the transfer

POPIA defines consent as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".[73] Here, section 72(1)(b) states that the data subject can consent to the transfer of its personal data to a third party outside the Republic. If the necessary consent is obtained, the transfer can take place without the need for the requirements of section 72(1)(a) to be met. As the latter requirements place a heavy burden on the responsible party, it is conceivable that in most cases a responsible party will rely on the consent of the data subject to avoid meeting the stringent requirements of paragraph (a). Consent is often seen as the "backdoor" for responsible parties; but consent must be given freely and unambiguously and must be informed and specific consent. This means that the data subject must not be pressurised or unduly influenced in giving consent. Furthermore, the responsible party must inform the data subject what personal information is to be transferred out of the Republic, to where and to whom, for what purpose(s), and how it will be used.[74] Consent must be explicit, either in the form of an express statement or an affirmative act; consent cannot be implied. For example, where consent is indicated by checking a box on an online contract form, a

72 Kuner 2021 https://ssrn.com/abstract=3827850 5.
73 Section 1 of POPIA.
74 Section 18 of POPIA.

data subject's failure to uncheck or deselect a pre-ticked consent box cannot be interpreted as implied consent. The data subject must also be informed of its right to withdraw consent at any time, as well as the possible risks and safeguards that will be in place.[75] In the long run, data subject consent cannot be maintained as a sustainable solution to protect exports of personal data, and companies should revisit their data protection policies in light of the requirements of section 72(1)(a).

2.3.2 The transfer is necessary for the conclusion or performance of a contract between the data subject and the responsible party

Section 72(1)(c) authorises the transfer of personal data that is necessary to perform a contract between the data subject and the responsible party. This paragraph will apply primarily in connection with the conclusion, payment, delivery and other performance aspects of transactions. These transfers all take place in the context of a contract already concluded between a data subject and the responsible party. Typical examples are transfers of personal information to reserve an airline ticket for a passenger; a travel agent transferring a traveller's information to a hotel in a foreign country to book his stay there; the transfer of personal data to effect an international credit card payment; or the transfer of personal information by a bank in South Africa to a foreign bank to execute a client's payment.[76] Data transfers to implement measures to be taken by the responsible party on the request of the data subject prior to the conclusion of a contract are also allowed; for example, where personal data is needed to process a quote requested by the data subject.[77]

Data transferred under this paragraph is restricted to necessary information, necessity being determined with reference to the purpose of the contract between the responsible party and the data subject.[78] This is a fact-based assessment, and the responsible party must always consider whether other less intrusive alternatives are available.[79] This exception will apply only to occasional transfers and not in the case of routine transfers.[80]

---

75 See recitals 32 and 43 of the GDPR.

76 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.3; SALRC 2009 https://www.justice.gov.za/salrc/reports/r_prj 124_privacy%20and%20data%20protection2009.pdf 408.

77 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 6.3.1.

78 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.3.

79 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 6.3.1.

80 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.3.

2.3.3 The transfer is necessary for the conclusion of a contract between the responsible party and a third party in the interest of the data subject

The exception in section 72(1)(d) differs from that in section 72(1)(c) in that the contract concluded is between the responsible party and a third party (and not between the responsible party and the data subject) and it is concluded in the interest of the data subject. For example, where a data subject is the beneficiary of a payment to be made by another person to the responsible party or contracts concluded on behalf of juristic persons still to be formed. As in the previous exception, the transfer of the personal data must be necessary and occasional.[81]

2.3.4 The transfer is to the benefit of the data subject in circumstances where consent could not reasonably be obtained

Section 72(1)(e) applies to transfers of personal data to the benefit of the data subject where it is reasonably impracticable to obtain the data subject's consent to the transfer, but if it were reasonably practicable to do so, the data subject would most likely have given consent. This exception would apply to situations where the data subject is physically or legally incapable of giving consent, such as where an unconscious South African needs medical assistance in a foreign country and his medical aid in South Africa is asked to disclose personal medical information.[82]

Section 72(1)(e) furthermore states that transfers to the benefit of a third party will also be exempted. Where paragraph (d) dealt with contracts between the responsible party and a third party only, paragraph (e) has a broader scope. It covers transfers made to third parties in general and not only in connection with a contract between a responsible party and a third party. Again, transfers will be restricted to necessary transfers.[83] Public interest might be a guideline here, for example, where medical or other records are to be shared in times of a global pandemic or natural disasters.

2.4 Conclusion

Data transfer rules aim to protect personal data that would have been protected by a country's data protection laws if the data were not moved out of the country. POPIA does not protect all transfers of personal data to another country but merely those that meet the criteria set out in section 72, namely that there must be a transfer of a data subject's personal information

81 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.4.

82 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.5.

83 De Stadler *et al Over-thinking the Protection of Personal Information Act* para 14.2.3.4.

by a responsible party in the Republic to a third party in another country. Section 72 does not extend the application of POPIA to the third party, but makes the transfer dependent on certain conditions, unless it falls under one of the exceptions. Personal data can be transferred to a third party in another country only if an adequate level of protection has been set in place, either in the form of the third country's laws, a BCR between the responsible party and the third party, or a binding agreement between the responsible party and the third party. An adequate level of protection would exist if the instrument used displays a level of protection substantially similar to the principles and conditions on which POPIA is based. Section 18(1)(g) also places an obligation on a responsible party who intends transferring information to a third country or an international organisation to inform the data subject of the level of protection afforded to the information by that country or organisation.

The discussion has shown that this places an extremely high burden on the responsible party to decide on the adequacy of these measures, which most responsible parties and legal practitioners would not be qualified to make. When it comes to the data protection laws of a third country, it cannot be expected that a responsible party will be acquainted with the laws of another country to the extent that it can make this call.[84] The same problem occurs in the context of BCRs and SCCs as these instruments must also contain a level of protection substantially similar to that afforded by POPIA, which places the burden on the responsible party. It is submitted that the Information Regulator must provide guidance here. Guidance can also be sought in the data transfer rules of the GDPR to improve our rule.

These days, most websites contain a link to their owners' data privacy policies. Usually these policies are incorporated impliedly into the agreement between the data subject and the service provider. As a matter of course, these agreements would require data subjects' consent to the processing of their personal information, which would function as a general exception to the conditions posed by section 72. Consideration of whether the data privacy policy was adequately brought to the knowledge of the party and consequently incorporated into the agreement is beyond the scope of this article but it is an important factor that must be kept in mind to ensure that consent was informed and specific.[85] When it comes to providing consent, the data subject must be fully aware of what she is consenting to and what the legal effect of such consent would be.

---

84 A similar concern has been raised in the context of the GDPR, where data controllers are required to verify whether the same level of protection that is enjoyed by data subjects in the EU exists in the third country. See *Schrems II* para 142; Kuner 2020 https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation.

85 See Van Deventer 2021 *SALJ* 219.

Furthermore, as the consent must be express or at least in the form of an affirmative act it cannot simply be assumed or implied. Moreover, even though this article has not attempted to discuss the criteria or standards to determine whether data subjects can trust the technology or the surveillance measures in place in third countries to which data is transferred, this aspect is one that must be taken into consideration as well.[86]

3 Interaction between territorial scope and transfer of data provisions

The effect of the provisions relating to territorial scope is to afford a data protection law extra-territorial force. If it brings a foreign responsible party or an operator under its scope of application, the question is whether there is still a need for data transfer rules, as they might result in unnecessary duplication. This question is especially pertinent as data transfer rules do not result in the extra-territorial application of the data protection law but merely make the transfer dependent on certain conditions that require a form of protection substantially similar to that of the data protection law. The UK and New Zealand have recently amended their data protection laws so that the data transfer rule will not apply if the data importer otherwise falls under the scope of their respective data protection laws by virtue of the territorial scope provision.

The final version of the European Data Protection Board (EDPB) guidelines on the territorial scope of Article 3 of the GDPR was published in November 2019.[87] The document makes no mention of the interrelationship between the territorial scope rule in Article 3 and the data transfer rules in chapter V, except that the interaction will be investigated further and additional guidance will be published if necessary. However, an unpublished draft of 14 September 2018 stated that the data transfer rules compensate for the lack of protection that otherwise would arise if personal data which is protected under the territorial provision is moved outside the EU. The relationship between the two sets of rules is therefore "complementary or compensatory".[88]

The question of their interaction and the need for having both territorial scope rules and data transfer rules applying to the same situation might perhaps be best answered by starting with the rationale for these rules. The discussion in parts I and II of this article has shown that the rationale for having territorial scope and data transfer rules is the same, namely to

86 See *Schrems I* and *Schrems II*; Hoffman 2021 *North Carolina Journal of Law and Technology* 573.

87 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

88 EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf 3.

prevent the circumvention of data protection laws by moving the data outside the jurisdiction of that law.[89] Territorial rules protect data subjects whose personal information is processed by parties from outside by bringing the foreign party under the scope of application of the data protection law, while data transfer rules are directed at information that leaves the country to be processed abroad, which can operate only if certain conditions underlying the data protection law are met. In the former case the data protection act will apply directly while in the latter case the act will not apply, but conditions equivalent to those of the act will apply.[90] The immediate effect of territorial scope rules is that the act has to be enforced in a foreign jurisdiction, which could result in a lower level of protection than that afforded by a data transfer rule.[91]

In the EU context it has been suggested that the two types of rules are to be merged into one provision that specifically provides for situations where they might potentially overlap, but this would require a revision of the GDPR.[92] According to Kuner,[93] there is little evidence that the co-existence in the GDPR of these rules presents problems, and where efforts have been made to coordinate them, little was said on the reasons for doing so. He therefore sees no potential for real conflict between these rules in the GDPR, as both provisions are based on the same principles and conditions contained in the Regulation.[94] The only difference is that enforcement mechanisms can be set out in agreements in the case of the data transfer rule, which is not possible where the GDPR applies directly under the territorial scope rule. It is his conclusion that the rules work *in tandem*.[95]

If compared to the South African legal position, the potential for overlap is greater in the context of the GDPR as its data transfer rule also covers the export of data from a processor (an operator) in the Union to a third party in another country.[96] If the EU operator acts on the instructions of a non-EU responsible party (a controller) who, for example, collects personal information by means of cookies installed on accessing the latter's website, both could be subject to the GDPR on the basis of the territorial scope provision, but the former also has to meet the conditions of the data transfer

89 Kuner 2021 https://ssrn.com/abstract=3827850 23.
90 Kuner 2021 https://ssrn.com/abstract=3827850 24-25.
91 Kuner 2021 https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr.
92 See Kuner 2021 https://ssrn.com/abstract=3827850 33-35 for suggested formulations.
93 Kuner 2021 https://ssrn.com/abstract=3827850 21.
94 Kuner 2021 https://ssrn.com/abstract=3827850 22.
95 Kuner 2021 https://ssrn.com/abstract=3827850 31.
96 Moreover, Art 3(2) of the GDPR extended the territorial scope provision to include processing activities by controllers or processors outside the Union when goods or services are offered to data subjects in the EU or where they monitor the behaviour of data subjects in the EU.

rule when the data are transferred back to the responsible party. In this example both rules will have the same effect. However, in the South African context the data transfer rule will not apply as, firstly, the operator transferring the data out of the country is not a responsible party as required by section 72 POPIA, and secondly, the importer is a responsible party and not a third party as required. In this example the data subject's personal information can be protected based on POPIA only by virtue of an extensive interpretation of the territorial scope provision of section 3(1)(b) bringing the non-South African responsible party under the scope of the Act and not under the data transfer rule. It is difficult to imagine a situation where a potential conflict could arise between the two rules in the light of the requirements set by POPIA.

Therefore, from a South African point of view it would seem that there is a need for both rules, as they will supplement and complement each other rather than overlap. From an enforcement point of view, the data transfer rule might be more beneficial as it is often difficult to enforce the data protection law outside the borders of a country. A data transfer rule acts proactively by restricting the transfer of data to cases that meet stringent conditions. On the other hand, territorial scope provisions find application only where a foreign responsible party is brought under the ambit of the Act to address an already committed transgression of the data protection law. In that sense they act retroactively.[97] Under POPIA the data transfer provision is part of the duties of responsible parties and its application is restricted to data exports by these parties. This article has noted that there is an overlap between the data transfer rule and the content of sections 20 and 21 of POPIA, but potentially duplication will take place only where the responsible party and the data importer conclude an agreement containing SCCs. Even here, this is not a real overlap as the SCC can supplement shortcomings in the agreement concluded by virtue of section 21 POPIA and vice versa.

The question should rather be whether the data transfer rule achieves its goal of protecting the data subject's rights. The discussion of section 72 and the comparative analysis with the counterpart provisions in the GDPR have identified very specific shortcomings. Restricting the operation of this rule to exports by responsible parties leaves a gap when data is exported by an operator. Although the responsible party remains liable for the processing of personal data during the lifespan of the data, the only provisions dealing directly with operators are those of sections 20 and 21, which means that any conditions imposed on exports of data by operators must be stipulated in the contract between the responsible party and the operator. The discussion has shown that responsible parties must include very specific

97 Kuner 2021 https://ssrn.com/abstract=3827850 24-25.

conditions on such exports in their agreements with operators. Furthermore, the data transfer rule can function effectively only when the phrase "responsible party in the Republic" is interpreted extensively to cover those who reach into the Republic to collect, monitor and otherwise process data subjects' personal data. Even if there were a potential for both the data transfer rule and the territorial scope rule to apply to the same scenario, the advantages of the data transfer rule justify that they operate *in tandem*. However, the absence of a measure similar to the adequacy decision used in the EU, or that of regulated pro-forma SCCs and BCCs, might leave the data transfer rule without teeth. Section 72(1) will operate to its full potential only if clear guidance is provided on the content of these measures. Until then, the practical reality might be that South African data subjects primarily will have to rely on POPIA's territorial scope provision, which in turn needs to be interpreted expansively for the Act to protect South African data subjects adequately.

Bibliography

Literature

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

Hoffman 2021 *North Carolina Journal of Law and Technology*
Hoffman DA "Schrems II and Tik Tok: Two Sides of the Same Coin" 2021 *North Carolina Journal of Law and Technology* 573-616

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

Roos 2007 *SALJ*
Roos A "Data Protection: Explaining the International Backdrop and Evaluating the Current South African Position" 2007 *SALJ* 400-436

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

Van Deventer 2021 *SALJ*
Van Deventer S "Problems Relating to the Formation of Online Contracts: A South African Perspective" 2021 *SALJ* 219-257

Case law

Bodil Lindqvist (Case C-101/01) [2003] ECLI:EU:C:2003:596

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

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

Legislation

New Zealand

Privacy Act 31 of 2020

South Africa

Protection of Personal Information Act 4 of 2013

United Kingdom

Data Protection Act of 2018 (implementing the *United Kingdom General Data Protection Regulation*)

International and regional instruments

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contract clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council [2021] OJ L 199/31

Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 [2010] OJ L 39/5

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 [2016] OJ L 344/100

Directive 95/46/EC of the European Parliament and of the Council enacted 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31

Privacy and Electronic Communications (EC Directive) Regulations, 2003

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

Internet sources

EDPB 2019 https://edpb_guidelines_3_2018_territorial_scope_after_ public_ consultation_en_1.pdf

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

EDPB 2021 https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf
European Data Protection Board 2021 *Guidelines 05/2021 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR (Adopted 18 November 2021)* https://edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf accessed 30 March 2022

Kuner 2020 https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation
Kuner C 2020 *The Schrems II Judgment of the Court of Justice and the Future of Data Transfer Regulation* https://europeanlawblog.eu/2020/07/17/the-schrems-ii-judgment-of-the-court-of-justice-and-the-future-of-data-transfer-regulation accessed 30 March 2022

Kuner 2021 https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr
Kuner C 2021 *Exploring the Awkward Secret of Data Transfer Regulation: the EDPB Guidelines on Article 3 and Chapter V GDPR* https://europeanlawblog.eu/2021/12/13/exploring-the-awkward-secret-of-data-transfer-regulation-the-edpb-guidelines-on-article-3-and-chapter-v-gdpr accessed 31 December 2021

Kuner 2021 https://ssrn.com/abstract=3827850
Kuner C 2021 *Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection. University of Cambridge Faculty of Law Legal Studies Research Paper Series Paper No 20/2021, April 2021* https://ssrn.com/abstract=3827850 accessed 30 March 2022

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

Woods 2020 https://eulawanalysis.blogspot.com/2029/07/you-were-only-supposed-to-blow-the-bloody.html?m=1
Woods L 2020 *"You Were Only Supposed to Blow the Bloody Doors Off!" Schrems II and External Transfers of Personal Data*

https://eulawanalysis.blogspot.com/2029/07/you-were-only-supposed-to-blow-the-bloody.html?m=1 accessed 17 March 2022

List of Abbreviations

BCRs	binding corporate rules
DPD	Data Protection Directive (EU)
ECJ	European Court of Justice
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation (EU)
POPIA	Protection of Personal Information Act 4 of 2013
RSA	Republic of South Africa
SALJ	South African Law Journal
SCC	standard contract clause
UK	United Kingdom
UK-GDPR	United Kingdom General Data Protection Regulation
USA	United States of America