Cross-border data flows in the digital economy: an analysis between the European Union General Data Protection Regulation and the Southern African Development Community Data Protection Model law

by

Tholoana Rose Ncheke

Submitted in fulfilment of the requirements for the degree

LLM

In the Faculty of Law,

University of Pretoria

October 2020

Supervisor: Dr Sylvia Papadopoulos

Summary

Technology has enabled the transmission of personal data across multiple jurisdictions and data has become central to the emerging digital economy. Whilst this development provides an opportunity for greater economic integration and access to global markets, it also presents a new challenge in respect of the regulation of personal data which is still predominantly based on national laws with limited jurisdiction.

Other regions such as the European Union (EU) have recently introduced regulatory interventions to address the challenges posed by cross border personal data transfers which are enabled by digital technologies, whilst also limiting the hindrance to free data flows. Despite this progress, other regulatory instruments such as the Southern African Development Community (SADC) data protection model law, which provides guidance to SADC member states, are no longer fit for purpose in light of the advancements in technology.

Against this background the study will critically assess and compare the extraterritorial application of the EU General Data Protection Regulation against the SADC data protection law within the context of the growing digital economy. To this end, the study will analyse the objectives and key terminology of the GDPR together with the cross-border data flow provisions. The study will thereafter compare the GDPR provisions with the SADC model law on data protection, focusing on the corresponding cross-border data flow provisions.

Pursuant to the above, the study will focus on determining the compatibility of the SADC model law provisions, vis-à-vis the GDPR provisions in order to make recommendations to bring the SADC model law on par with the GDPR which is hailed as international best practice.

Declaration of originality

This document must be signed and submitted with every essay, report, project, assignment, mini-dissertation, dissertation and/or thesis

Full names of student: Tholoana Rose Ncheke

Student number: 25191773

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.

2. I declare that this mini-dissertation is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.

3. I have not used work previously produced by another student or any other person to hand in as my own.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Table of Contents

List of abbreviations and acronyms

AU	African Union
AfCFTA	African Continental Free Trade Agreement
EU	European Union
EC	European Commission
GDPR	General Data Protection Regulation
ICC	International Chamber of Commerce
ICT	Information and communication technology
IP	Internet Protocol
IMF	International Monetary Fund
ITU	International Telecommunications Union
OECD	Organisation for Economic Co-operation and Development
SADC	Southern African Development Community
UNCTAD	United Nations Conference on Trade and Development
TCP/IP	Transmission Control Protocol/Internet Protocol
UNECA	United Nations Economic Commission for Africa
WTO	World Trade Organisation

Chapter 1

1. Background to the research problem

One of the fundamental features of ICT is its ability to enable the exchange of data. Increased access to ICT networks and services has given rise to the digital economy.[1] Central to the digital economy is the free flow of data both within a specific county and across different jurisdictions.[2] Having recognised both the economic benefits of free flow of data together with the inherent risks, the EU adopted the GDPR in an effort to address the need for adequate data protection.[3]

A salient feature of the GDPR is the cross-border data flow provisions outlined in article 3. The provisions seek to balance uniform data protection both within and beyond the geographical borders of the EU member countries whilst also minimising impediments to the free flow of data.[4]

One other region which adopted a similar approach is SADC which developed a model law on data protection as part of the harmonisation of ICT Policies in Sub-Saharan Africa, an initiative by the ITU and the EC.[5] Ultimately, the model law seeks to provide an enabling data protection regulatory framework which also harnesses the economic benefits of ICT.[6] Notably, the model law was developed and finalised prior to the GDPR and some African counties including SADC countries have relied on regional legislative frameworks such as the SADC model law to guide the development of national data protection legislation and regulatory frameworks.[7]

The extra-territorial application of the GDPR impacts on other legislative frameworks such as the above-cited SADC model law and by extension national legislation which

---

1 Mattoo & Meltzer "International Data Flows and Privacy: The Conflict and Its Resolution" (2018) 21 *Journal of International Economic Law* 769 - 770

2 ICC Trade in the digital economy – A primer on global data flows for policy makers (undated) available at https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed on 10 April 2019)

3 Recital 6,7 *GDPR*

4 Wolters "The security of personal data under the GDPR: a harmonized duty or a shared responsibility?" (2017) 7 *International Data Privacy Law* 165

5 Abrahams "Regulatory Imperatives for the Future of SADC's 'Digital Complexity Ecosystem'" (2017) *The African Journal of Information and Communication* 16

6 Southern African Development Community Model Law: Data Protection

7 Internet Society Personal Data Protection Guidelines for Africa (2018) available at https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed on 15 April 2019)

is based on the model law.[8] This brings the question of compatibility of the respective regulatory frameworks to the fore. This compatibility is arguably necessitated by the economic partnership agreement concluded between the two regions on 10 June 2016 and the implications of data exchange on economic growth.[9] Further, in March 2018 member states of the AU adopted the Agreement establishing the AfCFTA.[10] This Agreement seeks to establish a single market for goods and services through fostering greater integration of the regional economic communities,[11] and progressively eliminating tariff and non-tariff barriers to trade and services.[12] Importantly, the Agreement recognises the importance of the rule of law for economic cooperation and international trade and ultimately the achievement of its objectives.[13] Furthermore, the Agreement places emphasis on the respective regional economic communities as the bedrock of the free trade area.[14]

Against this background, the study will comparatively analyse the SADC model law against the GDPR in order to assess the efficacy of the SADC model law. The comparative analysis will focus on the cross-border provisions within the context of the impact of free flow of data on the promotion of trade and the digital economy.

---

8 De Hert & Czerniawski "Expanding the European data protection scope beyond territory: Article 13 of the General Data Protection Regulation in its wider context" (2016) 6 *International Data Privacy Law* 237.

9 Tralac Economic Partnership Agreement between the European Union and Southern African Development Community Group (2018) available at https://www.tralac.org/documents/resources/faqs/2049-sadc-eu-epa-faqs-july-2018/file.html (accessed on 15 April 2019) .

10 AU Agreement Establishing the African Continental Free Trade Area (2018) available at https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area (accessed 4 December 2019).

11 the regional economic communities listed in the Agreement establishing the African Continental Free Trade Area are: Arab Maghreb Union; the Common Market for Eastern and Southern Africa; the Community of Sahel-Saharan States; the East African Community; the Economic Community of Central African States; the Economic Community of West African States; the Intergovernmental Authority on Development and SADC;

12 AU Agreement Establishing the African Continental Free Trade Area (2018) available at https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area (accessed 4 December 2019).

13 *Ibid.*

14 *Ibid.*

2. The aim of the study

The study will assess and illustrate the impact of the free flow of data on economic activity and in particular, the advancement of the digital economy. To this end, the study will analyse the objectives and scope of application of the GDPR and SADC model law respectively together with their cross-border data flow provisions. The study will thereafter critically compare the GDPR provisions with the SADC model law on data protection, focusing on the corresponding cross-border data flow provisions.

Pursuant to the above, the study will focus on determining the compatibility of the SADC model law provisions, vis-à-vis the GDPR provisions in order to make recommendations to bring the SADC model law on par with the GDPR.

3. The outline of the study

The study will commence with an overview of the development of the digital economy within the EU and the SADC region. In this regard, the study will also highlight the challenges posed by cross-border data flows. This will be followed by an exposition of the GDPR with a focus on the cross-border data flows and the implications for non-EU counties.

For comparative purposes, the study will thereafter provide an outline of the SADC data protection model law and assess the corresponding cross-border data flow provisions. The study will conclude with an outline of key recommendations to address any *lacunae* as identified.

The main themes include the digital economy, regulatory compatibility, data protection and cross-border data flows.

4. Research questions

The study will ultimately aim to answer the following questions:

- What is the digital economy?
- How has the digital economy developed globally and in Africa?
- What are the benefits of the digital economy?
- What are the challenges of the digital economy?
- What is the impact of cross-border data flows on the digital economy?

- How has the EU cross-border data regulatory framework developed?
- Is the current SADC model law framework sufficient?
- What are the key recommendations in order to maximise the benefits of the digital economy?

5. Delimitation

The digital economy entails various aspects including the technological infrastructure, which is used for purposes of communication and transactions, as well as consumer protection considerations. The study will not explore the consumer protection implications. Furthermore, the study will only give a broad overview of technical aspects of ICT and the development thereof without going into great detail as the aim is to analyse and compare the regional regulatory frameworks. Therefore, the technological outline will only be for purposes of giving context to the study.

6. Research methodology

The study will adopt a qualitative research methodology evidenced by an in-depth review and analysis of existing regional instruments as primary resources and various publications including books and journal articles as secondary resources.

Chapter 2: The Evolution of The Digital Economy

2.1 Introduction

The digital economy cannot be understood and discussed without first understanding ICT, the foundation of the digital economy.[15]

It is generally accepted that the main function of ICT is to enable people to transmit information and to communicate using various technologies.[16] As these continue to evolve, there is no doubt that ICT will increasingly change the way we work and interact with one another and will become more integral to our social and economic activities.

Following from the preceding paragraph, the term ICT is generally understood to refer the various types of technologies namely, broadcasting, computing technologies and telecommunications, and overtime this definition further developed to encompass a distinction between analogue and digital technologies.[17] The parlance related to ICT has further developed with the concept of technological convergence – the merger of broadcasting, computing and telecommunications[18] which this discourse will touch on briefly below.

This chapter will give an overview of ICT without going into detail on the specific developments of the underlying infrastructure. Thereafter, the chapter will explore the digital economy as a concept and consider how it has developed with time. The chapter will conclude with a discussion on the implications of the digital economy on cross-border data flows and the regulation thereof.

2.2 The History and Development of Information and Communication Technologies

The first manifestation of ICT was the telegraph which was introduced in the 1830s.[19] Its main functionality was sending text over wired networks. Its limitation was that it could only transmit information and communication in a specific format and when it

15 Blackman & Srivastava (eds) (2011) Telecommunications Regulation Handbook 4.
16 *Idem* 3.
17 Souter (ed) (2009) The APC ICT Policy Handbook 14.
18 Van der Merwe et al (2016) Information and Communications Technology Law 6.
19 Souter (ed) (2009) 14.

was first introduced it used a code, usually Morse code. This further limited its use and accessibility.[20]

This type of technology evolved into the transatlantic telegraph which first become operational in the early 1850s and was followed by the emergence of a global network which came in place around 1870.[21] During this period, the first international institution which focused on overseeing and co-ordinating matters related to international telegraphy was established in 1865.[22] This institution was first known as the International Telegraph Union and later referred to as the International Telecommunications Union as it is now known.[23]

The next milestone in the evolution of ICT was the introduction of voice transmission technology with the invention of the telephone in the 1870s.[24] Even in the early days, the infrastructure underpinning ICT evolved resulting in the introduction of new and more efficient methods of communication. This was notably the case with the introduction of communications satellites, oceanic cables, and cellular wireless networks.[25]

Following from the above developments, which had a significant impact in exchange of information, was data transmission which was the genesis of the Internet. The Internet has evolved from what was previously known as the ARPANET, an United States defence project, to the World Wide Web as we now know it.[26] The Internet has expanded quite considerably since its first introduction and access thereto has increased exponentially with the number of Internet users estimated at 4,833,521,806 which constitutes around 62.0 %, of the world population as at 30 June 2020.[27]

The brief historical development outlined above clearly demonstrates that each communication technology transmitted information in a specific way namely voice, text

---

20 Souter (2009) 14.

21 *Ibid.*

22 *Ibid.*

23 ITU Overview of ITU's History (undated) available at https://www.itu.int/en/history/Pages/ITUsHistory.aspx (accessed 25-04-2020).

24 Souter (2009) 14.

25 *Idem* 15.

26 Papadopoulos & Snail (eds) (2012) Cypberlaw@SA III: The Law of the Internet in South Africa 1.

27 Internet World Stats Usage and Population Statistics (2020) available at https://www.internetworldstats.com/stats.htm (accessed 25-07-2020).

or data and was therefore only capable of and confined to transmitting information in a particular form and enabling communication through specific means.

Turning to Sub-Saharan Africa, the history of the development of ICT has to be assessed within the context of the wider political history of the continent. The early manifestations of telecommunications technology and infrastructure were used to establish communications between various African countries and their European colonial countries.[28]

It was not until the period between 1988 to 1991 that the access to the Internet was realised with the transmission of the fist data packet from Sub Saharan Africa using fixed telephony.[29] From that period on the region experienced a high mobile growth rate[30] and access to the Internet has increased throughout the region, although it still lags behind in comparison to developed regions.[31]

2.3 Types of Information and Communication Technologies

Whilst this study is not intended to delve into the elaborate technical details of ICT, it is worthwhile to outline and categorise ICT following from the historical evolution outlined above. From this definition the following categories emerge namely computing and information technology, broadcasting, telecommunications, and the Internet.[32]

The first category is mainly used for the analysis of information and management of processes by electronic means.[33] The second category entails simultaneous communication to a large number of viewers or listeners, through either radio or television.[34] The third category, unlike the second category is in respect of one-on-one

---

28 Odedra Sub-Saharan Africa: A Technological Desert (1993) http://www3.cis.gsu.edu/dtruex/courses/IB8710/Articles/Odedra-SubSahara-CACM1993.pdf (accessed 25-04-2020).

29 ITU Study on international internet connectivity in sub-Saharan Africa (2013) https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/IIC_Africa_Final-en.pdf (accessed 25-04-2020).

30 Makulilo (ed) (2016) African Data Privacy laws 10.

31 Mahler *et al* Internet Access in Sub-Saharan Africa (2019) http://documents.worldbank.org/curated/en/518261552658319590/pdf/Internet-Access-in-Sub-Saharan-Africa.pdf (accessed 25-04-2020).

32 Souter (2009) 14.

33 *Ibid.*

34 Van der Merwe et al (2016) 6.

communications between people and computers on an interactive basis. This category includes telephony and business-to-business data communications.[35]

The final category can be described as an interconnected system of networks which connects computers around the world through software protocol known as TCP/IP.[36] The Internet is ultimately an international network of computers that communicate with one another through the use of packet switching.[37]

This categorisation may be regarded as an academic debate with the advent of convergence in terms of which the aforementioned categories are essentially amalgamated into one broad category as the distinction between products, platforms and services becomes more blurred.[38]

2.4 Defining the Digital Economy

The unprecedented advancements in ICT and more particularly the Internet, has and continues to change the way businesses are conducted and has become a significant part of national and international commercial activities and practice.[39] There have been various definitions developed overtime and to date no single definition has been universally adopted. It can be can argued that the challenge with defining the digital economy lies in its intangible nature and the rapid changes to the environment within which it exists and more specifically the changes to the technology which underpins it. The following paragraphs will critically discuss some of the prevalent definitions which have emerged. Further, it will highlight the key characteristics of this concept.

In analysing the definitions of the digital economy which have emerged, it is critical to first consider international and intergovernmental institutions as well as the treaties, conventions and policies of these institutions as they influence the national legislation of countries which have acceded to these international instruments. These institutions include the WTO, UNCTAD, the IMF and the OECD.

---

35 Souter (2009) 14.

36 Chapman The history of the Internet in a Nutshell (2009) available at http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/ (accessed 25-04-2020).

37 Papadopoulos & Snail (eds) (2012) 2.

38 Blackman & Srivastava (eds) (2011) 4.

39 *Ibid.*

The WTO has provided a definition in some of its publications. The significance of the WTO in this context is borne by the role it continues to play in developing a global framework for international trade through agreements concluded between member countries, as well as providing a forum for the resolution of trade disputes.[40] The WTO defines the digital economy as "…the application of *internet-based digital technologies* to the production and trade of goods and services" (own emphasis).[41] This definition refers to goods and services without reference to a specific industry or sector of the economy. This definition is therefore notably broad in scope and arguably encompasses all economic activity and sectors which makes use of (applies) Internet-based digital technologies.

UNCTAD has also provided guidance on how the digital economy can be understood. Similar to the WTO, UNCTAD plays a vital role in the global economy by providing support in respect of *inter alia* trade negotiations, trade policy and regulations.[42] UNCTAD takes a cautionary stance in respect of providing or adopting a precise definition of the digital economy. Instead, UNCTAD outlines the fundamental components of the digital economy which may also be used as a basis for measuring the digital economy.[43] These components are: (i) the core digital and computing infrastructure; (ii) digital and IT sectors which manufacture the aforementioned infrastructure; and (iii) the wider digitalizing sectors.[44] Within this context digitalization is understood as the application of digital data and the Internet to organisational and social processes.[45] This approach recognises the role of technological innovation and the underlying infrastructure as core to the digital economy.[46] Following from the components outlined above, UNCTAD further provides for a narrow definition of the

---

40 WTO What is the WTO? (undated) available at https://www.wto.org/english/thewto_e/thewto_e.htm (accessed 25-04-2020).

41 WTO World Trade Report 2018 The future of world trade: How digital technologies are transforming global commerce (2018) available at https://www.wto.org/english/res_e/publications_e/wtr18_e.htm (accessed 25-04-2020).

42 UNCTAD About UNCTAD (undated) available at https://unctad.org/en/Pages/aboutus.aspx (accessed 25-04-2020).

43 UNCTAD Digital Economy Report 2019 Value creation and capture: implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

44 *Ibid.*

45 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

46 Bukht & Heeks "Defining, Conceptualising and Measuring the Digital Economy" (2018) 13 International Organisations Research Journal 2

digital economy which is confined to digital and platform services.[47] This is a more practical approach as digital and platform services are potentially more distinguishable as a specific or emerging sector of the economy than the wider digitalizing sectors which are included in the broader definition.

The IMF has also considered the concept of the definition. Similar to UNCTAD, the IMF recognises that the digital economy can either be understood very broadly to include all activities that use digitized data, or narrowly to only include online platforms and those activities that exist as a direct result of these platforms.[48] Notably, the IMF generally adopts this narrow definition, essentially confining the use and application of the term 'digital economy' to that section of the economy whose products and services are directly related to online platforms.[49]

The UNECA defines the digital economy as "…the global flow of goods, services and finance through means of digital computing technologies that are unbound by national borders."[50] This definition recognises the inherent transnational nature of the digital economy as enabled by the underlying technological infrastructure. This key characteristic of the digital economy presents prospects of increased economic growth and development through greater access to markets but also poses challenges in respect of conventional regulatory frameworks.[51]

The OECD is another significant institution in respect of the development of broad legal principles through its policies which are adopted across multiple jurisdictions canvassing its membership.[52] Some of its publications have focused on the digital economy wherein it has provided guidance on the definition of the concept. In its 2018 publication titled "*The Digital Economy, Multinational Enterprises and International Investment Policy*" the OECD defined the digital economy as "…the broader economy

---

47 UNCTAD Digital Economy Report 2019 Value creation and capture: implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

48 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

49 *Ibid.*

50 UNECA What is Digital Identity, Digital Trade and Digital Economy for Africa? (undated) available at https://www.uneca.org/dite-africa/pages/what-digital-identity-digital-trade-and-digital-economy-africa (accessed 25-04-2020).

51 Blackman & Srivastava (eds) (2011) 220.

52 OECD About the OECD (undated) available at https://www.oecd.org/about/ (accessed 25-04-2020).

as it undergoes the process of becoming increasingly digital."[53] Whilst this definition is broad similar to that of the WTO and therefore does not distinguish the digital economy as a separate sector from the rest of the economy, the OECD recognises the components of the digital economy as digital data, digital technologies and digital infrastructure.[54] This provides guidance on identifying the enablers and building blocks of the digital economy and therefore the factors to be considered when assessing the development thereof.

The ICC has also contributed to the international discourse on the digital economy as part of its mission in the promotion of international trade and a global approach to regulation.[55] Whilst it has not put forth a definition for consideration, the ICC acknowledges the impact of technologies on economic growth and development[56] and it is this impact which is the essence of the digital economy.

There are scholars from other jurisdictions who have also noted the fluidity of this concept and how it can vary in scope depending on the particular definition adopted. From the definitions proposed by the respective international institutions cited in the preceding paragraphs, one of the recommended approaches to providing a comprehensive yet concise definition is to first identify the core characteristics of the digital economy.[57] To this end, when assessing the various definitions and approaches outlined above, it is broadly accepted that firstly the digital economy cannot exist without the underlying ICT infrastructure and by extension the production thereof as this is the foundation of the digital economy.[58] This core is also referred in other articles as the digital sector.[59] Secondly and following from the first assessment, the digital economy encompasses those business processes and sectors of the economy which exists solely as a result of ICT equipment and infrastructure, such as online platforms

---

53 OECD The Digital Economy, Multinational Enterprises And International Investment Policy (2018) available at http://www.oecd.org/investment/investment-policy/The-digital-economy-multinational-enterprises-and-international-investment-policy.pdf (accessed 25-04-2020).

54 *Ibid.*

55 ICC Our mission (undated) available at https://iccwbo.org/about-us/who-we-are/our-mission/ (accessed 25-04-2020).

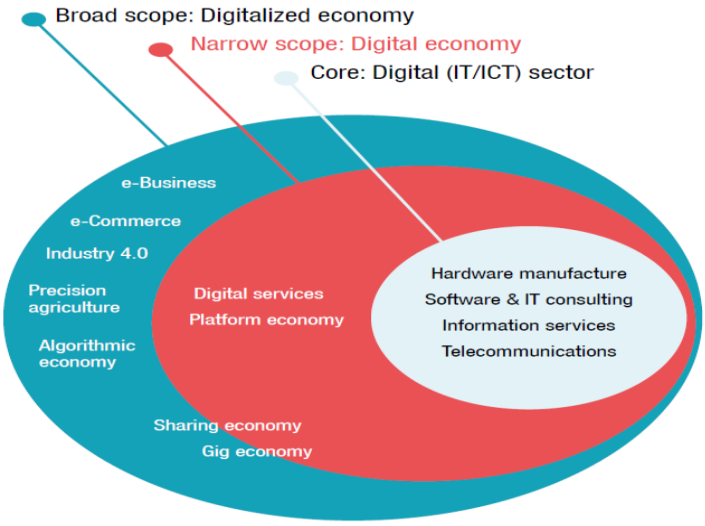
56 ICC Trade In The Digital Economy: A Primer On Global Data Flows For Policymakers (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

57 Bukht & Heeks (2018) 13 *International Organisations Research Journal* 5.

58 *Idem* 11.

59 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

and platform-enabled services.[60] Whilst some definitions, as noted above extend the definition to all economic activities that use digitalised data, this approach will inevitably include all sectors of the modern economy as they are increasingly making use of digital technology. This is well illustrated in the figure below:[61]



In response to the impact of technologies on the economy, governments across the world have developed and revised policies and legislation.[62] Legislation not only has to address and promote country-specific policy objectives, as a general principle it must also be compatible with foreign and to the extent applicable, international legal or regulatory frameworks. Further, adopting a flexible approach is essential when considering the rapid rate at which technologies develop and evolve vis-à-vis the time it takes for policies and laws to be developed and adopted.

Globally, the digital economy is part of a greater digital ecosystem and therefore any regulatory response aimed at addressing the emergence as well as promoting the advancement thereof must be guided by the principles of consistency and harmonisation.[63] This is further necessitated by the pervasive nature of digital technologies and the Internet which transcend geographic boundaries and old industry

60 *Ibid.*

61 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

62 Blackman & Srivastava (eds) (2011) 4.

63 Abrahams (2017) 20 *AJIC* 13.

or sector classifications.[64] Therefore, the global nature of the Internet and underlying infrastructure necessitate a global or at least a co-ordinated approach in the development of policy as well as regulatory interventions.[65] Furthermore, there must be due cognisance of foreign and international law.

2.5 The Development and Growth of the Digital Economy

As outlined above, there is no universal definition of the digital economy. This poses a challenge in respect of determining both the level of the digital economy as well as the rate at which it is developing within a particular country, a particular region and globally. This challenge is further exacerbated by the continuous increase in digitally enabled economic activity together with the advancements in the underlying technologies.[66]

This section will not endeavour to provide the statistical detail in respect of the development and growth of the digital economy. Rather, this section will outline the essential considerations for the measurement and assessment of the digital economy.

Efforts to measure the digital economy have been premised along the same parameters used for purposes of defining the digital economy. These parameters are either confined by adopting a narrow definition or extended in scope by adopting a broader definition.

Where a narrow definition is adopted, the data considered for purposes of measuring the digital economy primarily focuses on the core ICT/digital sector which entails ICT goods and services including online platforms and platform-enabled economic activity.[67] The statistics in respect of the various types of ICT infrastructure as enablers

64 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

65 Blackman & Srivastava (eds) (2011) Telecommunications Regulation Handbook 220.

66 Bukht & Heeks (2018) 13 *International Organisations Research Journal* 11

67 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

of the digital economy have been used as indicators of both the level and rate at which the digital economy is developing at a particular point in time.[68]

A broad measurement approach which is premised on a broad definition assess the use of various digital technologies in performing different economic activities.[69] However, this approach is to be used with great circumspection as there is an overall concern regarding possible mis-measurement, this in turn highlights the need to develop an international classification system for measuring the digital economy in order to accurately identify and quantify the digital activities and products to be included.[70]

To this end, international institutions such as UNCTAD, OECD, the ITU and regional bodies such as the EU have begun working towards the development of frameworks and scorecards for measuring the digital economy. These frameworks and scorecards measure various indicators focusing on the core ICT sector including ICT occupations and trade in ICT goods and services.[71] The other indicators focus on Internet-enabled economic activity such as e-commerce and all Internet subscription expenditure.[72] UNCTAD is also in the process of establishing a working group on measuring the digital economy in order to *inter alia* support policy development and identity specific measurement opportunities for developing countries.[73]

A further dimension to the debate around the digital economy is the digital divide between the global north and the global south as a lot of developing countries lack the basic level of ICT infrastructure.[74] However, as with the rest of the world, the digital

---

68 OECD Harnessing the digital economy for developing countries (2016) available at https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en (accessed 25-04-2020).

69 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

70 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

71 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

72 Bukht & Heeks (2018) 13 *International Organisations Research Journal* 16

73 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

74 OECD Harnessing the digital economy for developing counties (2016) available at https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en (accessed 25-04-2020).

sector in Africa is growing at an accelerated pace[75] through the steady increase of access to mobile and fixed broadband infrastructure.[76] This growth presents developing regions such as Africa with an opportunity to develop adequate legal and institutional frameworks which will promote an enabling environment for the growth and development of the digital economy as well as facilitate regional integration.[77]

Notwithstanding the lack of consistent statistical data due to the challenges with measuring of the digital economy, such information is nevertheless significant as provides critical guidance for the development of progressive, practical regulatory frameworks which will harness the opportunities presented by the digital economy whilst also addressing some challenges and mitigating inherent risks.[78]

2.6 Implications of Cross-Border Data Flows

One of the key characteristics of the digital economy is the transnational production and consumption of goods and services.[79] This is enabled by the global reach of the platforms used by consumers for communication and facilitation of various commercial transactions.[80] The preceding paragraphs have illustrated the critical role of technological infrastructure as the foundation of the digital economy. This section will analyse the significance of cross-border data flows and the implications thereof for regulation of this aspect of the digital economy in particular.

Whilst the measurement of the digital economy is still the subject of much debate, cross-border data flows have undoubtedly contributed to the growth of the global

---

75 IMF Measuring the Digital Economy (2018) available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020).

76 ITU Measuring digital development Facts and figures 2019 (2019) available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (accessed 25-04-2020).

77 AU-EU Digital Economy Task Force (undated) available at https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf (accessed 25-04-2020).

78 OECD The Digital Economy, Multinational Enterprises and International Investment Policy (2018) available at http://www.oecd.org/investment/investment-policy/The-digital-economy-multinational-enterprises-and-international-investment-policy.pdf (accessed 25-04-2020).

79 OECD Harnessing the digital economy for developing countries (2016) available at https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en (accessed 25-04-2020).

80 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

GDP[81] through *inter alia* global employment in the core ICT sector and through ICT services exports.[82] Within this context reference to 'data' includes data created by the users through their engagement on online platforms as well as transactional data.[83]

The efficiency of the digital economy relies not only on the digital data itself but importantly, it also relies on the unhindered flow of digital data across multiple jurisdictions.[84] The role of data has also gained prominence through the emergence of data-centric technologies such as cloud computing, block-chain, the Internet-of-Things and processes such as big data analytics.[85] In addition, cross-border data flows have the potential to contribute to greater economic integration within regional and global markets[86] and promote socio-economic development, in particular for developing economies.[87]

The transnational nature of the digital economy and underlying flows of data have raised new dynamics and challenges in respect of developing appropriate regulatory frameworks.[88] Data privacy and protection have therefore become the focus of regulators in various jurisdictions as they seek to achieve the maximum benefits of the digital economy whilst also providing adequate protection in respect of the data itself. Effective regulatory frameworks are guided by the national context and socio-

---

81 McKinsey Global Institute The ascendancy of international data flows (2017) available at https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows (accessed 25-04-2020).

82 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

83 OECD Harnessing the digital economy for developing countries (2016) available at https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en (accessed 25-04-2020). S1 of the Electronic Communications and Transactions Act 25 of 2002 (hereafter ECT Act) defines data as electronic representations of information in any form

84 ICC Trade In The Digital Economy: A Primer On Global Data Flows For Policymakers (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

85 *Ibid.*

86 Research ICT Africa Measurement of the digital economy (2018) available at https://researchictafrica.net/wp/wp-content/uploads/2018/12/2018_Measurement-of-the-digital-economy_Africa-E-Week.pdf (accessed 25-04-2020).

87 ICC Trade In The Digital Economy: A Primer On Global Data Flows For Policymakers (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

88 Blackman & Srivastava (eds) (2011) 205.

economic objectives of a specific country as well as international best practice.[89] Therefore, an enabling regulatory framework ought to be interoperable to ensure legal certainty.[90]

The next chapter will critically analyse two regional frameworks on data protection, namely the EU GDPR[91] and the SADC Model Law on Data Protection,[92] focusing on their significance in respect of legal harmonisation and regulatory interoperability.

89 UNCTAD Digital Economy Report 2019 Value Creation and Capture: Implications for developing countries (2019) available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020).

90 ICC Trade In The Digital Economy: A Primer On Global Data Flows For Policymakers (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

91 EU Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (2016) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 25-04-2020)

92 SADC Data Protection: Model Law (2013) available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 25-04-2020)

Chapter 3: Regional approaches to the regulation of cross-border data flows

3.1 Introduction

Innovation in technology has enabled the ever-increasing collection and global dissemination of personal data.[93] This has necessitated the review of legislative frameworks in order to address *inter alia* data protection concerns beyond national borders[94] as well as to create a sense of trust for the data subjects in respect of the protection of their personal data.[95]

This chapter will critically analyse two legal regional frameworks on data protection, namely Regulation 2016/679 of the European Parliament and of the Council 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, often referred to as the GDPR and the SADC's Model Law on Data Protection.

3.2 The European Union General Data Protection Regulation

3.2.1 The objectives of GDPR

The EU Charter of Fundamental Rights recognises the protection of personal data as a fundamental right and provides for the rights of access to and rectification of data, and also provides guidance in respect of the processing of such data.[96] This right finds further expression in article 16 of the Treaty on the Functioning of the EU which also provides for the development of regulatory and institutional frameworks to give effect to these rights.[97]

The rights and protections granted under the above-cited instruments are the cornerstone of the GDPR. Importantly, the GDPR seeks to *inter alia* harmonize the protection of personal data in order to ensure consistent levels of personal data

---

93 Wolters "The security of personal data under the GDPR: a harmonized duty or a shared responsibility?" (2017) 7 *International Data Privacy Law* 165.

94 Blackman & Srivastava (eds) (2011) Telecommunications Regulation Handbook 220.

95 ICC "Trade in the digital economy – A primer on global data flows for policy makers" (2016) available at https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed on 10 April 2019)

96 Article 8 *EU Charter of Fundamental Rights.*

97 Article 16 *Treaty on the Functioning of the EU*.

protection throughout the EU whilst also promoting the free flow personal data between EU member states.[98] Furthermore, the GDPR recognises challenges posed by global data flows which are enabled by innovation and the accelerated pace at which technology changes and continues to develop.[99]

3.2.2 Scope of application

As stated, the GDPR seeks to protect personal information specifically with respect to the processing thereof.[100] To this end, the GDPR identifies specific processing activities which fall within its ambit as well as those processing activities which are expressly excluded from its scope. Given that the GDPR has been adopted by EU member states, its scope of application cannot be assessed accurately without consideration of the geographical nexus.

Generally, the GDPR applies to the processing of personal data which is conducted either wholly or partly by automated means.[101] In addition, the GDPR applies to the processing of personal data by non-automated means only to the extent that the personal data forms part of or are intended to form part of a filing system.[102]

The GDPR further delineates its jurisdiction with reference to a set of factors in respect of the location of either the data subject, processor or controller.[103] Firstly, the GDPR applies to the processing of personal data by an establishment of a controller or a processor located within the territory of the EU irrespective of where the processing takes place.[104] This ground of jurisdiction provides certainty as technology enables personal data to be processed across multiple jurisdictions. Any reference to the location of the processing and therefore the location of the equipment would impede the objectives of the GDPR.[105] Secondly, where the data subject is within the territory of the EU but neither the processor nor controller is established within the territory of

98 Wolters (2017) 7 *International Data Privacy Law* 165.
99 Van der Merwe et al (2016) 384.
100 Article 2(1) *GDPR.*
101 *Ibid.*
102 *Ibid.*
103 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 236.
104 Article 3(1) *GDPR.*
105 Bu-Pasha "Cross-border issues under EU data protection law with regards to personal data protection" (2017) 26 *Information & Communications Technology Law* 218.

the EU, the GDPR only applies to the extent that the processing of personal data relates to either the offering of goods or services, or the monitoring of the data subject's behaviour in so far as the data subject's behaviour takes place within the territory of the EU.[106] It is important to note that this provision only requires that goods and services be offered to the data subject, irrespective of whether or not the data subject concludes a transaction and makes any subsequent payment.[107]

The GDPR therefore recognises the complexity posed by the multi-jurisdictional processing which is enabled by technology. To this end, it seeks to provide objective guidelines in order to determine whether or not the GDPR applies to a particular set of circumstances.

Notwithstanding the preceding paragraphs, the GDPR does not apply to the processing of personal data by a natural person which is conducted purely in the course of a personal or household activity.[108] The GDPR also excludes the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.[109] Furthermore, the GDPR does not apply to the processing of personal data which is conducted within the course of an activity which falls outside the scope of EU law.[110] EU law in this context refers to both the treaties and regulations, as well as directives and decisions which emanate from these treaties.[111] The scope of the GDPR further excludes the processing of personal data which is conducted by EU members states where such processing falls within the scope of Chapter 2 of Title V of the Treaty of the EU which deals with external action and specific provisions on the common foreign and security policy.[112]

The GDPR makes additional provision for EU member states to limit its scope through national legislation where such restriction is in the interests of national or public security, defence, the prevention, investigation, detection or prosecution of criminal

106 Article 3(2) *GDPR.*
107 Article 3(2)(a) *GDPR.*
108 Article 2(2)(c) *GDPR.*
109 Article 2(2)(d) *GDPR.*
110 Article 2(2)(a) *GDPR.*
111 EU EU Law (undated) available at https://europa.eu/european-union/law_en (accessed 28-05-2020).
112 Article 2(2)(b) *GDPR.*

offences or the execution of criminal penalties including safeguarding against and preventing threats to public security.[113] EU member states may also limit the scope where it is in the economic or financial interests of the EU or a specific member state,[114] or it is for the protection of judicial independence and judicial proceedings,[115] or for the prevention, investigation, detection and prosecution of breaches of ethics in respect of regulated professions.[116] The GDPR may be further limited to the extent necessary for the protection of the data subject or the rights and freedoms of others[117] such as the right to freedom of expression or for the enforcement of civil law claims.[118]

3.2.3 Key terminology and definitions

Whilst the foundational instruments of the GDPR entrench the right to the protection of personal data and outlines the principles in respect of processing thereof, they do not define 'personal data' nor do they define any of the other concepts in respect of the regulated activities. The GDPR provisions are therefore essential as they provide substance and legal certainty to the fundamental and ancillary rights by providing definitions of the various terms used as well as outlining the essential principles to be adhered to. The key terms which will be outlined in this section include 'personal data', 'data subject', 'processing', 'controller', and 'processor'.[119]

Central to the right of personal data protection is the understanding of the legal definition of personal data as the rights and obligations attach thereto. Article 4(1) defines personal data as *any* information relating to an identified person (own emphasis), or identifiable natural person, who is also referred to as the data subject. The GDPR provides that an identifiable natural person is one who can be identified, either directly or indirectly with reference to an identifier such as a name, an identification number, location data, an online identifier or by any one or more factors

113 Article 23(1) *GDPR.*
114 Article 23(1)(e) *GDPR.*
115 Article 23(1)(f) *GDPR.*
116 Article 23(1)(g) *GDPR.*
117 Article 23(1)(i) *GDPR.*
118 Article 23(1)(j) *GDPR.*
119 Article 4 *GDPR.*

specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[120]

From the above definition it is clear that only the data of a natural person or that can be linked to a natural person falls within the scope of the GDPR, therefore juristic persons cannot claim protection of their data pursuant to the GDPR. The definition of personal data is notably broad as the use of the word "any" indicates that the definition encompasses all types of information pertaining to an identified or identifiable natural person irrespective of its format.[121] Within the context of digital technologies, personal data can therefore include all aspects and forms of the digital print of a user engaging on online platforms such as tracking cookies.[122]

Similarly, the inclusion of the words "such as" in the definition of an 'identifiable person' make provision for the identification of a natural person through other identifiers beyond those listed, as they are not a *numerus clausus*. Therefore, identifiers such as an IP address can constitute personal data and fall within the provisions of the GDPR to the extent that it can be used to identify a natural person.[123] This was confirmed by the Court of Justice of the EU in the case between Patrick Breyer and Bundesrepublik Deutschland[124] where it considered whether a dynamic IP address can be used in combination with other factors to identify a natural person. Importantly, the court reiterated the guidelines outlined in recital 26 which recognises the circumstances under which pseudonymous identifiers can be attributed to a natural person. In determining whether a person is identifiable by means of such identifiers, there must be due consideration of all the means reasonably likely to be used either by either the controller or any other person to identify the person in question.[125] The reasonableness of the means will be determined on the basis of associated costs, the amount of time required for identification as well as the available technology at the

120 Article 4(1) *GDPR.*

121 Calder (2018) *EU GDPR: a pocket guide* 18.

122 Hoofnagle et al "The European Union general data protection regulation: what it is and what it means" (2019) 28 *Information & Communications Technology Law* 72.

123 ITGP PTIP (2017) *EU General Data Protection Regulation (GDPR) : An Implementation and Compliance Guide* 20.

124 Case C-582/14

125 Recital 26 *GDPR.*

time of processing.[126] This was also confirmed by the Court of Justice in the above-cited case.

Notably, the GDPR does not make any distinction between a data subject with reference to their nationality, citizenship, or country of residence.[127] Therefore, all data subjects enjoy protection under the GDPR subject to the provisions on the GDPR's scope of application outlined in article 2 read together with article 3.

The rights and primary obligations provided for in the GDPR relate to the processing of personal data. The GDPR defines 'processing' as any operation or set of operations which is performed on personal data or on sets of personal data, irrespective of whether such operations are conducted by automated means.[128] The GDPR further provides that the operations encompassed by this definition include the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[129] When considering the operations outlined above, it is evident that the definition of processes encompasses every activity in respect of the life-cycle of personal data particularly as the definition is not exhaustive.[130] It can be argued that extensive scope of this definition further entrenches the right to personal data protection.

The GDPR identifies the processor and controller as the primary role-players in the protection of personal data and therefore imposes specific obligations upon them. A processor is defined as a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.[131] A controller refers to either a natural or legal person, public authority, agency or other body which alone or jointly with others, determines both the purposes and the means of the processing of personal data.[132] The GDPR further provides that where the purposes and means of such processing are determined by EU law or the national law of a specific EU member state, then the controller may also be identified and provided for by such EU

126 *Ibid.*
127 Calder (2018) 37.
128 Article 4(2) *GDPR.*
129 Article 4(2) *GDPR.*
130 Hoofnagle et al (2019) 28 *Information & Communications Technology Law* 72.
131 Article 4(8) *GDPR*.
132 Article 4(7) *GDPR.*

law or the national law of the respective EU member state, whichever may be applicable.[133] Notwithstanding the distinction between a processor and controller, it is possible for the same entity to be both a controller and a processor.[134]

In order to provide clarity on the practices and measures to be implemented to ensure the protection of personal, the GDPR prescribes six principles for the processing of personal data. These principles provide guidance and a framework for assessment to ensure the effective implementation and compliance with the GDPR and are therefore central to the GDPR.[135] The following paragraphs will outline the principles and they will also be discussed in the next chapter.

The first principle requires that personal data be processed lawfully, fairly and in a transparent manner in relation to the data subject.[136] The overall objective of this principle is to ensure that data subjects are made aware that their personal data is to be used, and that they are also informed of the purpose thereof.[137] Article 6(1) provides further clarity on the requirement of 'lawfulness' in particular and the factors which will be taken into consideration when assessing this aspect. For the avoidance of doubt, processing will only be considered lawful where the data subject has given consent to the processing of their personal data, where the processing is necessary for either the performance of a contract to which the data subject is party or where it is necessary to take steps at the request of the data subject prior to concluding a contract, or where it is necessary for compliance with the controller's legal obligation.[138] Furthermore, processing will be lawful, where it is necessary to protect the data subject's vital interests or that of another natural person, where it is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller or where it is necessary for purposes of legitimate interests pursued by the controller or by a third party except where the processing is carried out by a public authority pursuant to their task.[139] Notwithstanding

133 Article 4(7) *GDPR.*
134 Calder (2018) 21.
135 Calder (2018) 37.
136 Article 5(1)(a) *GDPR.*
137 Calder (2018) 48.
138 Article 6(1)(a), (b)(c) *GDPR*.
139 Article 6(1)(d),(e),(f) *GDPR*.

the enumerated conditions of lawfulness, the GDPR only requires compliance with respect to only one of the listed conditions.[140]

The requirement of fairness seeks to mitigate against the use of the personal data in a manner which may have unjustifiably adverse consequences for the data subject.[141] This is further strengthened by the transparency requirement which seeks to ensure that data controllers are forthcoming about the use of the personal data.[142]

However, GDPR provides that the legitimate interests pursued by a controller may be overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, particularly where the data subject concerned is a child.[143]

The second principle requires that personal data be collected for specified, explicit and legitimate purposes.[144] The purpose for which the data is to be used must therefore be clearly defined, and ambiguous language must be avoided in this regard.[145] In the event that the personal data is further processed, such further processing must be compatible with the purpose for which the personal data was originally processed.[146] In order to assess the compatibility of any further processing, there must be a clear nexus between the initial and subsequent processing, other factors to be considered include the data subject's reasonable expectations and the nature of the data itself.[147]

The third principle reinforces the second principle and requires that the personal data be adequate, relevant, and limited to the extent necessary in relation to the purpose for which the personal data is processed.[148] Therefore, there must be a direct correlation between the data and the purpose for which it is processed.[149]

The fourth principle requires that the personal data be accurate and kept up to date, and where necessary the personal data must be rectified or erased to maintain the

---

140 ITGP PTIP (2017) 20.
141 ITGP PTIP (2017) 101.
142 *Ibid.*
143 Article 6(1)(f) *GDPR.*
144 Article 5(1)(b) *GDPR.*
145 ITGP PTIP (2017) 108.
146 Article 5(1)(b) *GDPR.*
147 Hoofnagle et al (2019) 28 *Information & Communications Technology Law* 77.
148 Article 5(1)(c) *GDPR.*
149 ITGP PTIP (2017) 109.

accuracy thereof.[150] This principle effectively grants data subjects the right to rectification of any inaccurate or incomplete data, which must be effected without delay.[151]

The fifth principle requires that the personal data be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.[152] This effectively means that if the purpose for which the data was processed has lapsed, there is no longer a basis upon which the data may be stored or retained.[153] Whilst the GDPR prescribes that personal data be retained for a limited duration, storage for longer periods is permitted but only where the personal data will be processed solely for archiving purposes in the public interest, or where it is processed for scientific, historical or statistical purposes.[154] This provision is subject to the implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.[155]

The sixth and last principle requires that personal data be processed in a manner that ensures appropriate security thereof through the use of appropriate technical or organisational measures.[156] This includes ensuring protection against any unauthorised or unlawful processing, accidental loss, destruction or damage, through the use of appropriate technical or organisational measures.[157] Compliance with this principle requires that the necessity of access to personal data be scrutinised, and the personal data must therefore be treated as confidential.[158] This principle also further reinforces the need to ensure that the data is kept accurate and complete as any damage, loss or destruction including partial loss or destruction will have to be rectified.

These principles are not unique to the GDPR and have also been adopted from the OECD Privacy Guidelines on data protection.[159]

---

150 Article 5(1)(d) *GDPR.*
151 ITGP PTIP (2017) 111.
152 Article 5(1)(e) *GDPR.*
153 ITGP PTIP (2017) 113.
154 Article 5 (1)(e) *GDPR.*
155 *Ibid.*
156 Article 5 (1)(f) *GDPR.*
157 *Ibid.*
158 ITGP PTIP (2017) 115.
159 Van der Merwe *et al* (2016) 372.

3.2.4 Cross-border data flow provisions

Cross-border data flows are key enablers for economic development,[160] which is illustrated by the correlation between increasing data flows and the growth of gross domestic product.[161] The jurisdiction of legislative frameworks has been traditionally based solely on the territoriality principle, however this is becoming less effective in the advent of the Internet and pervasive digital technologies.[162]

Whilst there is currently no globally adopted legislative framework for data protection, uneven data protection can and has been addressed through co-ordination between national legislators, guided by common principles and objectives.[163] In the absence of an international law on personal data protection, the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data which were first published in 1980, were the first expression of an international framework for data protection in an effort to harmonise data protection legislation at a national level whilst ensuring unhindered transmission thereof across multiple countries.[164] This framework has also often been used in the development of national legislation.[165]

A salient feature of the GDPR is its extra-territorial application outlined in article 3. This article extends the GDPR's scope of application to encompass data controllers or data processors established outside the EU who process personal data for purposes of monitoring the behaviour of data subjects who are in the EU.[166] Such monitoring can be through the application of tracking cookies.[167] The GDPR's extraterritorial application also extends to instances where the processing activities of non-EU

---

160 ICC *Trade In The Digital Economy* (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

161 McKinsey Global Institute *The Ascendancy Of International Data Flows* (2017) available at https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows (accessed 25-04-2020).

162 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 230.

163 Kong "Data Protection and transborder flow in the European and global context" (2010) 21 *European Journal of International Law* 442.

164 Van der Merwe *et al* (2016) 373.

165 *Ibid.*

166 Hoofnagle et al (2019) 28 *Information & Communications Technology Law* 74.

167 *Ibid.*

controllers or processors relate to the offering of goods and services to data subjects in the EU.[168]

Furthermore, the GDPR prescribes the circumstances under which personal data may be transferred to non-EU countries or international organisations, thus further expanding the jurisdiction of the GDPR. To this end, article 45(1) provides for the transfer of personal data to a third country or an international organisation where the EC has upon assessment, satisfied itself that the third country or the international organisation under consideration ensures an adequate level of protection. In order to determine the adequacy of the protection level, the GDPR prescribes the factors to be considered, which includes the rule of law and relevant legislation.[169] The factors further include respect for human rights and fundamental freedoms, existence of an effective, independent supervisory authority in the third country or to which an international organisation is subject, the international commitments that the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, particularly in relation to the protection of personal data.[170] Notably, such assessments are only feasible where third countries recognise privacy and personal data protection as fundamental rights and have appropriate legislative and institutional frameworks.[171] These provision are in accordance with the GDPR's objective of ensuring adequate levels of protection even where personal data is transferred to third countries or to an international organisation.[172]

In the absence of an adequacy assessment and a finding in the affirmative, the GDPR makes provision for cross-border transfers of personal data if the controller or processor has provided appropriate safeguards, provided that enforceable data subject rights and effective legal remedies for data subjects are available.[173] The requisite safeguards may be in the form of a legally binding and enforceable instrument between public entities, binding corporate rules, standard data protection

168 Article 3(2)(a) *GDPR.*
169 Article 45(2) *GDPR.*
170 *Ibid.*
171 Mattoo and Meltzer (2018) 21 *Journal of International Economic Law* 770.
172 *Idem* 775.
173 Article 46(1) *GDPR.*

clauses either adopted or approved by the EC, an approved code of conduct or an approved certification mechanism.[174]

The binding corporate rules refer to data protection policies adhered to by the controller or processor which is established in the territory of a member state for the purpose of transfers or a set of transfers of personal data to a controller or processor which is in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.[175] For the avoidance of doubt, article 4(18) defines an enterprise as a natural or legal person engaged in economic activity, irrespective of its legal form and includes partnerships or associations regularly engaged in economic activity. The binding corporate rules therefore enable the transfer of personal data within a multinational corporation operating across different jurisdictions whilst ensuring an adequate level of protection.[176] Importantly, the binding corporate rules include the general data protection principles in addition to the rights of data subjects.[177]

Similarly, the standard contractual clauses seek to ensure that contracts also provide a consistent level of protection and the same rights to data subjects as provided in the GDPR.[178] The codes of conduct may be used by associations or other bodies representing controllers or processors provided they are aligned with the data protection standard of the GDPR.[179] The purpose of certification is to demonstrate compliance by the controller or processor in respect of the processing operations through seals and marks.[180]

These provisions effectively extend the scope of the GDPR far beyond the national borders of the EU member states. Whilst there are seemingly various grounds upon which data transfers outside of the EU may be permitted, all these grounds remain subject to the principles outlined in the GDPR. Therefore, countries which are yet to develop data protection legislation will certainly need to consider the framework of the EU particularly in the interest of international trade.

---

174 Article 46(2) *GDPR.*
175 Article 4(20) *GDPR.*
176 Mattoo and Meltzer (2018) 21 *Journal of International Economic Law* 776.
177 Article 47(2) *GDPR.*
178 Mattoo and Meltzer (2018) 21 *Journal of International Economic Law* 776.
179 Article 40(2) *GDPR.*
180 Article 42(1) *GDPR.*

3.3 The SADC Data Protection Model Law

SADC evolved from the Southern African Development Co-ordination Conference and was formally established in 1992 following the adoption of the SADC Declaration and Treaty.[181] One of the objectives of SADC is to facilitate regional economic integration amongst members states through the establishment of *inter alia* a common market and to this end it also seeks to address tariff and non-tariff barriers.[182]

In 2001 the heads of state from SADC adopted the Declaration on ICT in recognition of the potential of ICT to promote SADC's objective of economic development.[183] Against this objective, the Declaration noted the need for a coherent, co-ordinated regional strategy and policy for ICT.[184]

Further on in 2008 under the auspices of the AU, the ministers responsible for ICT within the region adopted the AU Reference Framework for Harmonisation of Telecommunication and ICT Policies and Regulations in Africa.[185] In the same year, the ITU working collaboratively with the EC launched a global initiative in Sub-Saharan Africa with the objective of harmonizing ICT policies within the region through various model laws, one of which is the model law on data protection.[186] Notably, the SADC model law is not legally binding on SADC member states.[187]

---

181 SADC *History and Treaty* (2012) available at https://www.sadc.int/about-sadc/overview/history-and-treaty/ (accessed 28-05-2020).

182 WTO *Regional Integration in Africa* (2011) available at https://www.wto.org/english/res_e/reser_e/ersd201114_e.pdf (accessed 28-05-2020).

183 SADC *Declaration on Information and Communication Technology* (2001) available at https://www.sadc.int/documents-publications/show/Declaration_on_Information_and_Communication_Technology2001.pdf (accessed 28-05-2020).

184 *Ibid.*

185 ITU *Support for Harmonization of ICT Policies in Sub-Sahara Africa* (undated) available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/hipssa/Pages/default.aspx (accessed 28-05-2020)

186 ITU *Support for Harmonization of ICT Policies in Sub-Sahara Africa Implementation strategy* (undated) available at https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/HIPSSA_implementation_strategy_EN_090608.pdf (accessed 28-05-2020).

187 Makulilo (2016) African Data Privacy laws 37.

3.3.1 Objectives of the model law

Regional policy on ICT is increasingly critical in this age of globalisation[188] especially given ease with which personal data is transmitted across country borders.[189] This therefore requires a level of interoperability with respect to national regulatory frameworks.[190] The SADC model law was developed to provide guidance to national legislators, and ensure governments develop uniform, enabling regulatory frameworks which will also promote the development of ICT.[191]

The model law was also constructed to combat the various violations in respect of personal data which may arise as a result of the collection, processing, transmission, storage and use thereof.[192] Currently, only one of the sixteen SADC member-countries has no data protection law or proposed legislation, the rest have enforceable legislation or have begun the process of developing data protection laws.[193] The concept of the right to privacy, which is at the centre of data protection legislation is a relatively new concept in Africa.[194] The SADC model law therefore also plays a critical role in fostering a culture of a right to privacy and an understanding of the associated responsibilities.

3.3.2 Scope of application

The model law is intended to be transposed into national law and its scope of application will therefore be determined by the jurisdiction of the member country which has adopted it. The model law also provides general principles in respect of its jurisdiction including guidance on how to determine its applicability with reference to the location of the data controller's establishment.[195]

---

188 Jobodwana "Telecommunications Liberalisation in Africa: Proposed regulatory model for SADC region" (2009) 4 *Journal of Digital Forensics, Security and Law* 91.

189 Mattoo & Meltzer (2018) 21 *Journal of International Economic Law* 769.

190 Naude & Papadopoulos "Data protection in South Africa: the Protection of Personal Information Act 4 of 2013 in light of recent international developments" (2) (2016) 51 *THRHR* 220.

191 Abrahams (2017) 20 *AJIC* 16.

192 SADC 2013 Data Protection: Southern African Development Community Model Law.

193 Research ICT Africa SADC Parliamentary Forum Session IV: *Harnessing the opportunities of the digital economy in SADC* (2019) available at https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_SADC-Parliemantary-Forum.pdf (accessed on 30-05-2020).

194 Makulilo (ed) (2016) African Data Privacy laws 15.

195 Article 2(1) *Data Protection: SADC Model Law.*

In terms of the general principle, the model law applies to the processing of personal data irrespective of whether it is performed in part or wholly by automated means.[196] Where personal data forms part of or is intended to form part of a filing system, the model law only applies to the extent that the personal data is not processed by automated means.[197]

The model law further applies where the controller is established within the territory of the respective country which has enacted it through national legislation or where the national laws of the country under consideration apply by virtue of international public law.[198] Where the controller is not permanently established in the specific country, the model law only applies where the means used to process personal data are located in that country provided these means are not used solely for purposes of transit through the said country.[199]

For the avoidance of doubt, the model law explicitly outlines the limitation of its scope of application. To this end, the model law provides that it does not apply where personal data is processed purely only for purposes of personal or household activities.[200]

The model law provides additional exemptions in respect of personal data which is processed solely for purposes of literary and artistic expression as well as professional journalism which is guided by ethical rules.[201] Notwithstanding such exemption, the data controller is required to appoint a data protection officer belonging to a media enterprise. [202] The appointed data protection officer must in turn maintain a register of the processing conducted by the data controller and must also independently ensure compliance with the applicable provisions of the model law.[203]

Furthermore, member states may exclude provisions of this model law in the interests of preserving state security, defence, public safety, as well as the prevention, investigation, proof of criminal offences, prosecution of offenders or the execution of

196 *Ibid.*
197 *Ibid.*
198 Article 2(2)(a) *Data Protection: SADC Model Law*.
199 Article 2(2)(b) *Data Protection: SADC Model Law.*
200 Article 2(4).
201 Article 42(2)(a).
202 Article 42(2)(b).
203 *Ibid.*

criminal sentences or security measures or violation of professional codes of conduct in cases of a regulated profession.[204]

3.3.3 Key terminology and definitions

Central to the model law are the concepts of ‘data’, ‘personal data’, ‘data subject’, ‘processing’, ‘controller’, and ‘processor’. These terms are not unique to the model law and have been used in other similar legislative frameworks including the GDPR. This similarity is in line with one of the key objectives of this model law as outlined in its preamble namely to ensure a uniform level of personal data protection. The similarity also reflects the influence of other European instruments aimed at personal data protection.[205] Therefore, in order to assess and determine the model law’s scope of application we well as the rights and obligations which flow therefrom, we must first consider these key concepts together with their assigned definitions.

The model law defines personal data as any data relating to a data subject.[206] For purposes of this term data is defined as all representations of information irrespective of its format or medium.[207]

The concept of personal data is defined and used in relation to a data subject which is defined as an individual who is the subject of processed personal data and who is either identified or identifiable.[208] A data subject is identifiable if they can be identified, directly or indirectly with reference to either an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.[209] Notwithstanding the identifiers and factors highlighted above, when determining whether a data subject is identifiable, there must be due consideration of all the means reasonably likely to be used either by the controller or by any other person to identify the data subject.[210] Notably, the model law does not prescribe the types of identifiers which are envisaged, therefore a data subject may be identified

204 Article 42(1).
205 Makulilo (2016) 19.
206 Article 1(14).
207 Article 1(3).
208 Article 1(8).
209 Article 1(9)(a).
210 Article 1(9)(b).

through any means provided such means are considered as reasonable likely to be used for this purpose.

The use of the word 'processed' in the definition of data subject delineates the circumstances to which the model law specifically applies. Therefore, a full assessment of the application of the model law requires due consideration of the definition of 'processing'. For purposes of this model law, processing of personal data refers to any operation or set of operations which is performed upon personal data, whether or not by automatic means.[211] The model law provides examples of what would constitute processing namely obtaining, recording or holding the data.[212] Furthermore, processing includes organization, adaptation or alteration, retrieval, consultation, use, alignment, combination, blocking, erasures or destruction of the data.[213] These examples are not an exhaustive list, however, they illustrate the various forms of processing.

Both the definitions of 'personal data' and 'processing' are notably wide in scope. This is to ensure the model law provides comprehensive protection to data subjects in relation to their personal data. However, it must always be borne in mind that these definitions must be interpreted and applied with due cognisance of article 2(4) which provides the circumstances under which the model law generally does not apply, namely where the personal data is processed exclusively in the course of personal or household activities.

The model law affords the data subject rights vis-à-vis either the data processor or data controller depending on the particular circumstances, which are also referred to simply as a processor and controller. A data processor is a natural or legal person, or public body which processes personal data for and on behalf of the controller, or under the data controller's instruction.[214] This definition does not extend to persons who are authorised to process the data under the direct authority of the data controller.[215] Therefore if an employee is processing personal data in execution of their duties, they will not be considered as a data processor for purposes of this model law.

---

211 Article1(15).
212 Article 1(15).
213 Article 1(15).
214 Article 1(6).
215 *Ibid.*

A data controller is any natural person, legal person or public body which either independently or jointly with others determines the purpose and means of processing of personal data.[216] It is conceivable that the purpose and means of processing may also be determined by legislation, or another type instrument with legal effect namely a decree or an ordinance. Where the purpose and means of processing are determined by such other means, the model law provides that the controller will be deemed to be either the natural person, legal person or public body that has been designated as such in the legislation, decree or ordinance, whichever is applicable.[217]

Similar to the GDPR, the model law prescribes general rules on the processing of personal data. The model law recognises the importance of safeguarding the interests of the data subject by requiring the data controller to ensure that personal data which is processed is adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed.[218] The model law further requires that the personal data must be accurate, updated where necessary and any inaccurate or incomplete data must be rectified or eased.[219] The personal data must be retained in a form which enables the identification of data subjects for no longer than necessary in relation to the purpose for which the personal data was collected or processed.[220] Whilst the model law makes provision for the retention of personal data for a prolonged period, this is strictly subject to the application of appropriate safeguards as determined by an independent administrative authority which is responsible for ensuring compliance with the model law.[221] Furthermore, the controller bears the onus of taking all appropriate measures which will ensure that personal data shall be accessible, remain accessible and shall also be capable of being processed irrespective of the type of technology.[222] The controller also bears the onus of ensuring that persons working under their authority comply with the obligations outlined above.[223]

---

216 Article 1(4).
217 *Ibid.*
218 Article 11(1)(a).
219 Article 11(1)(b).
220 Article 11(1)(c).
221 *Ibid.*
222 Article 11(2).
223 Article 11(3).

The model law also incorporates other data protection principles through imposing additional obligations on the data controller. Firstly, the data controller is required to ensure that the processing of personal data is necessary and is processed fairly and lawfully.[224] Secondly, the data controller must ensure that the personal data is collected for a specified, explicit and legitimate purposes and is not further processed in a way which is contrary to the specified purposes.[225] In the case of non-sensitive data, processing is permitted in the absence of the data subject's consent where the data may be material as evidence in proving an offence, or is necessary for either the controller's compliance with an obligation or by virtue of law, or where the processing is necessary to protect the data subject's vital interest.[226] Furthermore, processing of personal data is permitted in the absence of a data subject's consent where the personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or a third party to whom the data is disclosed.[227]

These rules make provision for processing subject to the data subject's consent which is defined as any manifestation of specific, unequivocal, freely given, informed expression of will by which the data subject or his/her legal, judicial or legally appointed representative accepts that his/her personal data be processed.[228]

3.3.4 Cross-border data flow provisions

Whilst the model law includes provisions on the cross-border transmission on personal data, it is conceivable that not all countries within the SADC region will necessarily transpose it into national legislation or even have any legislating on data protection. It is further conceivable that personal data may be transferred to a country outside the SADC region and therefore not be subject SADC regional instruments. To ensure legal certainty, the model law also provides guidance on the transmission of personal data to a member state which has not adopted the model law or where the personal data is transmitted to a non-SADC member state or to an international organisation.[229]

---

224 Article 12(1).
225 Article 13(1).
226 Article14(1).
227 *Ibid.*
228 Article 1(2).
229 Article 43 – 44.

In instances where personal data is transmitted to a country which has adopted the model law, such transmission is permissible where the recipient has established the necessity of the personal data for purposes of performing a task which is in the public interest, or that such transmission is subject to authority exercised by a public body.[230]

The model law further provides for the transnational transmission of personal data where the recipient has discharged the onus of establishing the aforementioned necessity and does not have any reason to believe the data subject's interests may be prejudiced.[231] In addition to establishing the necessity of the cross-border transmission, the recipient must also ensure that the necessity can be subsequently verified.[232] Where personal data is transferred under the circumstances outlined in the preceding paragraph, article 43(1)(b)(ii) provides that the controller bears the responsibility of verifying the recipient's competence to ensure adherence to the model law. The controller is further required to conduct a provisional assessment on the necessity of the transborder transmission of the personal data.[233] If there is any doubt cast upon the relied upon necessity, the controller is required to seek further information from the recipient.[234] As a general principle, recipient may only process personal data to the extent required by the underlying purpose.[235]

Where personal data is to be transmitted to a non-SADC member state or to a SADC state which has not transposed the model law in national legislation which meets specific requirements, such transfer is only permissible to on the specific grounds provided for in the model law. Firstly, the country of the recipient must ensure an adequate level of protection in respect of the personal data and the data must be transferred with the sole objective of enabling the execution of tasks which are covered by the competence of the controller.[236] This requirement also applies where the personal data is transferred to an international organisation.[237] In assessing the level of adequacy, the factors taken into consideration include but are not limited to the nature of the data, the purpose and duration of the processing operation(s), the

230 Article 43 (1)(a)1.
231 Article 43 (1)(b)(i) & (iii).
232 Article 43(1)(b)(iii).
233 *Ibid.*
234 Article 43(1)(b)(ii) .
235 Article 43(1)(c).
236 Article 44(1)(a).
237 *Ibid*.

recipient third country or international organisation, the enforceable legislation, as well as the applicable professional rules of law and security measures.[238]

Where the recipient's country does not have adequate levels of protection, the transborder transmission of data is nevertheless permissible in prescribed circumstances in order to minimise the obstruction to free flow of personal data. The model law therefore permits transborder transmission of personal data where the data subject has unambiguously consented to their personal data being processed, or where the transfer is pursuant to a contract concluded either between the data subject and the controller or between the data controller and a third party. [239] The model law also permits the transfer of personal data where it is pursuant to the implementation of pre-contractual measures as requested by the data subject, or for the performance of an existing contract in the data subject's interest.[240]

Whilst the model law defines and distinguishes between a processor and a controller, the model law does not define 'recipient' notwithstanding the specific obligations imposed thereupon as well as the obligations imposed upon the controller in relation to the recipient. It is foreseeable that some entities may not be the ultimate recipients of the personal data but may receive it temporarily. Nevertheless, the term has been used to refer to a person who receives data and applied them for various purposes[241]

The model law also provides for the transborder transmission of personal data where the transfer is pursuant to significant public interest objectives or for the establishment, exercise or defence of legal claims, or for the protection of the data subject's vital interests.[242] Furthermore, transborder transmissions are permissible where the personal data is transferred from a register which is intended provide information to the general public and is open to the public or a specific person who has demonstrated a legitimate interest regarding the personal data.[243] However, this provision may only be invoked within the context of a legislative or other regulatory instrument.[244]

---

238 Article 44(1)(b).
239 Article 45(1)(a),(b) & (c).
240 *Ibid.*
241 Van der Merwe *et al* (2016) 369.
242 Article 45(1)(d) &(e) *Data Protection: SADC Model Law*.
243 Article 45(1)(f) *id.*
244 *Ibid.*

Notwithstanding the above provisions, an independent administrative authority which is responsible for ensuring compliance with all aspects of this model law may authorise transborder transmission of personal data to a country outside the SADC which does not ensure an adequate level of protection where the controller ensures adequate safeguards and the exercise of corresponding rights with respect to the protection of privacy and fundamental rights as well as freedoms of individuals.[245] Furthermore, an independent administrative authority is also empowered to determine the circumstances under which personal data to countries outside of SADC is not authorised.[246]

The following chapter will focus on the compatibility of the SADC model law with a particular focus on the cross-broader data transmission provisions.

[245] Article 45(2).
[246] Article 44(2).

Chapter 4: Compatibility of the SADC Data Protection Model Law

The previous chapter outlined the EU GDPR and the SADC model law on data protection with particular attention to their objectives, scope of application, key terminology, definitions as well as the general rules on processing personal data. The chapter thereafter concluded with an outline of the respective provisions on cross-border data transfers.

The EU GDPR has been hailed as the most progressive data protection regulatory instrument in the digital era and its impact transcends beyond the territory of the EU.[247] This chapter will critically assess the compatibility of the SADC model law, focusing on the data protection principles and identifying the divergence in the regulation of cross-border data flows in the SADC model law vis-à-vis the EU GDPR. In conclusion, the chapter will discuss the impact of divergent regulation on the digital economy.

4.1 Data protection principles

Whilst the application of national legislation is generally confined to the territory a particular country, data transfers are inherently transnational as a result of the underlying technology, this has in turn necessitated a level of harmonisation of national legislation through agreed international standards.[248] To this end, the OECD developed the Guidelines Governing the protection of Transborder Flows of Personal Data which were first adopted in September 1980.[249]

The purpose of these Guidelines was to establish internationally agreed upon rules which would be incorporated into national legislation across different jurisdiction thereby also developing common practices.[250] These rules which have come to be referred to as data protection principles have provided the foundation for the

247 Buttarelli "The EU GDPR as a clarion call for a new global digital gold standard" (2016) 6 *International Data Privacy Law* 77.

248 *Ibid.*

249 Van der Merwe *et al* (2016) 371.

250 *Ibid.*

interoperability of various data protection regulatory frameworks which have been developed over time.[251]

The OECD Privacy Guidelines provide eight specific data protection principles.[252] The first principle, the collection limitation principle, seeks to ensure that any collection of personal data is limited, and that personal data is obtained lawfully, by fair means and to the extent appropriate with the knowledge or consent of the data subject.[253] In order for this principle to be met, there must be a justification for processing personal data with reference to the factual circumstances.[254] Furthermore, the interests as well as the reasonable expectations of the data subject must be duly considered.[255]

The second principle pertains to the quality of the data and requires that the personal data must be relevant to the purpose for which it is to be used.[256] This principle also requires that the personal data must be accurate, complete and kept up-to-date where necessary depending on the purpose for which the personal data is held.[257] Data controllers must therefore exercise caution when processing personal data and take reasonable steps to ensure and maintain the accuracy thereof.[258]

Following from the second principle, the third principle seeks to ensure that personal data is collected for a defined purpose, which must be defined at the time that the personal data is collected and must be used in accordance therewith. In the event that the personal data is further used or processed, such further use or processing should not be incompatible to the original purpose for which the data was processed.[259] This principle also provides guidance in the assessment of the amount and nature of data required and the length of time that the personal data may be retained.[260]

In terms of the fourth principle, personal data should not be disclosed, made available or otherwise used for purposes other than those cited for purposes of the third principle

---

251 OECD Thirty Years After The OECD Privacy Guidelines (2011) available at http://www.oecd.org/sti/ieconomy/49710223.pdf (accessed 3-07-2020).

252 *Ibid.*

253 Van der Merwe *et al* (2016) 374.

254 Roos "Core principles of data protection law" (2006) *The Comparative and International Law Journal of Southern Africa* 108.

255 *Idem* 110.

256 Van der Merwe *et al* (2016) 374.

257 Roos (2006) *The Comparative and International Law Journal of Southern Africa* 115

258 *Ibid.*

259 Van der Merwe *et al* (2016) 374.

260 Roos (2006) *The Comparative and International Law Journal of Southern Africa* 111.

(purpose limitation) outlined above unless the data subject has expressly consented to the disclosure or the disclosure is required by law.[261]

The fifth principle provides that reasonable safeguards must be used to protect personal data from loss, unauthorised access or use, destruction, modification, or disclosure.[262] The level of security measures implemented must be correlate with the risks.[263]

The sixth principle requires the availability of means of establishing the existence and nature of personal data, the main purposes of their use, the identity as well as the usual residence of the data controller.[264] This principle essentially requires a general policy of openness with respect to the personal data and gives data subjects a level of participation in respect of their personal data.[265]

The seventh principle which follows from the provisions of the sixth principle seeks to ensure that data subjects have access to their personal data by giving them the right to obtain confirmation from a data controller of whether the data controller has data relating to the data subject.[266] Furthermore, the data controller must communicate to the data subject within a reasonable time, at a charge that is not excessive, in a reasonable manner and in a form that is readily intelligible to the data subject.[267] In the event that the data controller denies the data subject any of the rights outlined above, the data subject must be given reasons for the denial and must be able to challenge such denial.[268] The data subject also has the overall right to challenge data relating to him and if successful, the data subject is entitled to have the data erased, rectified, completed, or amended.[269]

The last principle amplifies the data subject's rights by providing that a data controller is accountable for complying with the measures which give effect to the principles set

261 Van der Merwe *et al* (2016) 374.
262 Van der Merwe *et al* (2016) 375.
263 Roos (2006) *The Comparative and International Law Journal of Southern Africa* 125.
264 *Idem* 117.
265 Van der Merwe *et al* (2016) 375.
266 Roos (2006) *The Comparative and International Law Journal of Southern Africa* 119.
267 *Ibid.*
268 Van der Merwe *et al* (2016) 375.
269 *Ibid.*

out above.[270] Data subjects must therefore have recourse against the data controller in instances of infringements.[271]

Notwithstanding that the OCED Guidelines are non-binding, they have been implemented through national legislation and incorporated in regional data protection regulatory frameworks.[272]

The EU's GDPR encompasses the essence of all eight data protection principles which are succinctly outlined in Article 5 and further elaborated in other articles albeit with a variation in the wording. The GDPR enumerates the following six principles: (i) lawfulness, fairness, and transparency; (ii) purpose limitation; (iii) data minimisation; (iv) accuracy; (v) storage limitation; (vi) integrity and confidentiality; and further provides that the data controller bears the onus of compliance in this regard. The following paragraphs will evaluate the SADC model law against the GDPR in order to critically assess the extent of its convergence with the latter.

The first principle of lawfulness, fairness, and transparency is partially adopted in Article 12 of the SADC model law in that the SADC model law only requires that personal data be processed lawfully and fairly and does not explicitly require for personal data to be processed in a transparent manner. However, this does not impact on the overall protection provided through application of this principle when it is applied together with the other data protection principles encompassed in the model law. Furthermore, the data controller will have to illustrate that the personal data is processed lawfully which will effectively require transparency from the data controller.

The second principle of purpose limitation is comprehensively incorporated in article 13 of the SADC model law as the model law also includes the same exemptions wherein further processing for historical research, scientific or statistical purposes will not be considered to be incompatible with the initial purpose for which the personal data is processed. Notably, the GDPR also provides that further processing for

---

270 Roos (2006) *The Comparative and International Law Journal of Southern Africa* 126.

271 *Ibid.*

272 OECD Thirty Years After The OECD Privacy Guidelines (2011) available at http://www.oecd.org/sti/ieconomy/49710223.pdf (accessed 3-07-2020).

archiving purposes shall not be deemed incompatible with the purpose limitation principle.[273]

The data minimisation principle which amplifies the purpose limitation principle similarly finds expression in article 11(1)(a). The SADC model law also includes the GDPR accuracy principle in article 11(1)(b), however, whereas the GDPR requires that inaccurate data be rectified or eased without delay,[274] the SADC model law only requires the data controller to take every reasonable step to ensure that incomplete or inaccurate data is erased or rectified. It can be argued that the GDPR provides the data subject with more effective relief by expressly regulating the timeframe within which incomplete or inaccurate personal data must be rectified or erased, which could in turn serve as grounds upon which a data subject can seek recourse from a court of law.

The storage limitation principle is provided for in article 11(1)(c) of the SADC model law. However, whereas the GDPR permits prolonged retention of personal data where it will be processed exclusively for archiving purposes in the public interest, statistical, scientific or historical research purposes, the SADC model law does not permit prolonged retention for archiving purposes on public interest grounds. The SADC model law only permits prolonged retention where it is for statistical, scientific, or historical research purposes. The determination of archiving which will be considered to be in the public interest will have to be assessed on a case by case basis as the GDPR itself does not provide further guidance on this aspect.

Central to the objects of personal data protection regulation is the adoption of adequate security measures to safeguard the personal data against *inter alia* unauthorised access and use or loss. To this end, both the GDPR and SADC model law prescribe the use of appropriate security safeguards. Whilst it is generally understood that the appropriateness of the security safeguards will be guided by the possible risks and the cost of implementation of the technological solutions available,[275] the GDPR goes further by providing some examples of the measures that can be implemented such as a legally binding and enforceable instrument between

273 Article 5(1)(b) *GDPR.*
274 Article 5(1)(d) *GDPR.*
275 Wolters (2017) 7 *International Data Privacy Law* 172.

public authorities or bodies, binding corporate rules, standard protection clauses, an approved code of conduct, or an approved certification mechanism.[276] The GDPR amplifies this particular principle by including a privacy by design requirement in terms of which the appropriate technical and organisational measures must be implemented at the time when the means of processing are determined as well as when the actual processing takes place.[277] Furthermore, the controller must the implement appropriate technical and organisational measures which by default ensure that only the personal data which is necessary for the underlying purpose is processed.[278] The GDPR also prohibits personal data from being made accessible to an indefinite number of natural persons without any intervention.[279]

Similarly, article 24 of the SADC model law requires that both the controller and the processor implement the appropriate security measures to mitigate against the aforementioned risks in line with the GDPR's integrity and confidentiality principle. The model law further provides that when determining the appropriate levels of security, the factors to be considered are the state of technological development and the cost of implementing the measures vis-à-vis the nature of the data to be protected and the potential risks to the data subject.[280] However, unlike the GDPR, the model law does not identity the types of measures which can qualify as adequate safeguards. This may cause uncertainty regarding the acceptable security measures.

Notably both the SADC model law and GDPR adopt a technology-neutral approach as neither of them prescribe a specific type of technology, but rather focus on the objectives of the measures against which the efficacy thereof will be assessed. This enhances the flexibility of both these regulatory frameworks and the ease with which they can adapt to the changing technology landscape.

In order to ensure judicial certainty and clear recourse for data subjects, the SADC model law incorporates the GDPR accountability principle in article 30 wherein it directs the data controller to ensure compliance therewith, which includes adopting the

276 Article 46(2) *GDPR.*
277 Article 25(1) *GDPR.*
278 Article 25(2) *GDPR*
279 *Ibid.*
280 Article 24(1)(b) *Data Protection: SADC Model Law.*

necessary internal mechanisms to demonstrate compliance to both the data subject and the relevant data protection authority.

4.2 Divergence of cross-border data flow regulation

Transnational data flows have become one of the key drivers of economic development and the growing digital economy.[281] However, the economic benefits objectives need to be cautiously weighed against the need to ensure adequate data privacy and protection. The regulation of transnational transmission of personal data has been given careful consideration in both the GDPR and the SADC model law. Both regulatory instruments recognise the need to minimise any hindrance to data transfers whilst providing judicial certainty on personal data protection, the legal obligations in respect thereof and the recourse available to data subjects. To this end, the GDPR adopts a general rule in terms of which transmission of personal data to third countries is permitted provided that such transmission is subject to the principles and conditions prescribed therein.[282]

Part XI of the SADC model law distinguishes between transmission of personal data to SADC member states which have adopted the model law through national legislation, vis-à-vis transmission of personal data to either SADC member states which have not adopted the model law through national legislation or transmission of personal data to non-SADC member states or to an international organisation. Where personal data is transferred to a SADC members country which has adopted the model law through national legislation, the recipient of the personal data must establish that the personal data is necessary for purposes of a task which is in the public interest or subject to the exercise of a public body.[283] The model law further permits the cross-border data transfer where the recipient has established the necessity of the data transfer and there is no reason to assume the data subjects interest may be prejudiced.[284] Whether transmission of personal data is indeed in the public interest

---

281 ICC *Trade in the digital economy - A primer on global data flows for policy makers* (2016) available at https://iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed 25-04-2020).

282 Article 44 *GDPR.*

283 Article 43(1)(a)(1) *Data Protection: SADC Model Law*.

284 Article 43(b)(i) *Data Protection: SADC Model Law.*

will have to be determined on a case-by-case basis as the model law does not provide further guidance in respect of this provision. In order to safeguard the interests of the data subject, the controller must verify the competence of the recipient and to this end the controller must conduct a provisional evaluation of the necessity,[285] and the recipient must also ensure that the necessity can be subsequently verified.[286]

Both the GDPR and SADC model law derogate from these general principles and provide for the transmission of personal data to third countries on the basis that the third country is deemed to provide an adequate level of protection. To this end both frameworks provide guidance in respect of the adequacy assessment and the factors to be considered. The common factors are the general and sectoral legislation, professional rules and security measures as provided in articles 44(1)(b) of the SADC model law and article 45(2)(a) of the GDPR, respectively. The GDPR provides comprehensive guidance as it prescribes further factors for consideration namely the respect for human rights and fundamental freedoms,[287] effective administrative and judicial redress for data subjects whose personal data is being transferred,[288] the existence of an effective, functioning independent supervisory authority in the third country,[289] as well as the international commitments which the third country is subject to.[290] Furthermore, the GDPR empowers the EC to conduct the adequacy assessment. However, the SADC model law on the other hand does not indicate the institution or public body which is empowered to conduct the assessment. The practical implications of this *lacuna* are far reaching as it is not clear how the outcome of the assessment will be confirmed - whether it will be through a declaration, regulation, or government notice. Furthermore, there is no provision for the review of the decision or revocation thereof.

In keeping with the underlying objective of free flow of data, the SADC model law provides for the cross-border transmission absence of an adequacy decision only on specific grounds namely where the data subject has consented to the transfer of their

285 Article 43(b)(ii) *Data Protection: SADC Model Law*.
286 Article 43(b)(iii) *Data Protection: SADC Model Law*.
287 Article 45(2)(a) *GDPR.*
288 *Ibid.*
289 Article 45(2)(b) *GDPR.*
290 Article 45(2)(c) *GDPR.*

data,[291] where the transfer is necessary for the performance of a contract between the data subject and the controller, or where the transfer is necessary for the precontractual measures taken pursuant to the data subject's request,[292] or is required in order to protect the interests of the data subject.[293] Furthermore, the data may be transferred where it is necessary for the conclusion or performance of a contract between the controller and a third party in the interests of the data subject,[294] or where the transfer is necessary or legally required to further public interest, or is in respect of legal claims.[295] Personal data may also be transferred to a third party country which does not ensure an adequate level of protection where the transfer is made from a register which is intended to provide information to the general public and is open to consultation to both the public and any person who can demonstrate a legitimate interest in the data.[296] Data transfers made pursuant to a register must be in accordance with and to the extent permitted by the underlying legislation including regulations.[297]

Whilst the SADC model law may appear to be flexible in permitting data transfers even in the absence of adequate levels of protection, the model law does not seem to explicitly require the processor to provide any appropriate safeguards to ensure effective measures are taken where data is transferred pursuant to the grounds outlined above. This may inadvertently compromise of personal data protection which may in turn hinder the transfer of personal data to countries which have adopted the model law in its current from. Whilst the GDPR also permits the cross-border transfer of data on the same grounds outlined above, the transfer is only permissible as an absolute derogation in the absence of an adequacy decision or appropriate safeguards.[298]

---

291 Article 45(1)(a) *Data Protection: SADC Model Law*.
292 Article 45(1)(b) *Data Protection: SADC Model Law.*
293 Article 45(1)(e) *Data Protection: SADC Model Law*.
294 Article 45(1)(c) *Data Protection: SADC Model Law*.
295 Article 45(1)(d) *Data Protection: SADC Model Law*.
296 Article 45(1)(f) *Data Protection: SADC Model Law.*
297 *Ibid.*
298 Article 49(1) *GDPR.*

4.3 Impact of divergent regulation on the digital economy

Personal data is generally regulated through national legislation, the application of which is confined to the territory of the particular country.[299] This has inevitably resulted in inconsistent levels of data protection[300] through a myriad of conflicting data protections laws as they are developed within different legal and socio-economic contexts.[301] This may it turn undermine the principle of judicial certainty and frustrate the data subject's right to judicial recourse.[302]

Furthermore, data subjects may be less inclined to adopt new technologies and use some of the emerging platforms if they have concerns regarding the protection of their personal data through effective implementation and enforcement of data protection laws.[303] This lack confidence may ultimately impact the growth rate of the digital economy in a particular country. Divergent data protection regulation therefore poses a significant challenge for global data flows.[304]

299 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 230.
300 Kong (2010) 21 *European Journal of International Law* 442.
301 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 240.
302 *Ibid.*
303 Buttarelli (2016) 6 *International Data Privacy Law* 77.
304 Kong (2010) 21 *European Journal of International Law* 442.

Chapter 5: Conclusion and recommendations

The preceding chapters outlined the evolution of the digital economy against the background of technological developments. The chapters assessed the data protection regulatory frameworks developed by the EU and SADC region respectively with a particular focus on cross-border data flows.

5.1 Global convergence of data protection regulation

Technology is not static and has continued to evolve at a rapid rate. Central to it is its ability to transmit information and for this reason it is also regarded as the cornerstone of the information society, the digital economy and the much talked about fourth industrial revolution.[305] The impact of technology is prevalent across all sectors of the economy, which further entrenches the pivotal role it plays in advancing socio-economic objectives, which are often translated into national policy and legislation.

A prominent feature of the digital economy is that it is inherently transnational, as it is enabled by ubiquitous technology. Notwithstanding the globalisation of technology and data transfers, concerns regarding protection of personal data still predominantly addressed at a national level.[306] However, the territorial application of national legislation does not detract from the impact of what a country may deem as foreign legislation.

At the same time, there is a growing effort to strengthen integration of regional markets both abroad and with respect to the SADC region. The EU adopted the Digital Single Market Strategy in 2015 to *inter alia* further the objective of greater policy and regulatory coordination.[307] Importantly, the Digital Single Market Strategy pays particular attention to the importance of data as a catalyst for economic growth, and acknowledges the challenges posed by legislative barriers in the form of different rules of law adopted by the member states.[308]

---

305 Wolters (2017) 7 *International Data Privacy Law* 165.

306 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 230.

307 European Commission Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions - A Digital Single Market Strategy for Europe (2015) available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (accessed on 07-08-2020).

308 *Ibid.*

The EU recognises the need to continuously foster the development and adoption of common legal rules which are uniformly adopted throughout its territory, to promote *inter alia* judicial certainty and regulatory convergence.

The EU GDPR therefore acknowledges the significance of uniform levels of protection of personal data which have been developed within the broader context of preceding multilateral treaties, in particular the Treaty on the Functioning of the EU and the OECD Privacy Guidelines. The GDPR has also taken full cognisance of the leaps and bounds at which technology is developing, which continues to enable the dissemination of personal data at increasing rates and quantities. This is illustrated in its scope of application which establishes jurisdiction even where the data processor or data controller is not established in the EU or where the processing takes places outside of the EU territory, subject to the criteria provided in Article 3.

Similarly, SADC as a regional economic market has identified the importance of harmonising legal rules and adopting similar standards of protection. This is reflected in article 5(1) of the consolidated text of the SADC Treaty which includes the promotion of common political values and systems, through *inter alia* the harmonisation of political and socio-economic policies as one of SADC's objectives.[309] This objective is also articulated in the AU Convention of Cyber Security and Personal Data Protection which seeks to address the need to harmonized legislation in respect of cyber security and in particular personal data protection. The Agreement establishing the AfCFTA which came into force in 2019 also identifies non-tariff barriers to trade.[310] In order to achieve its objectives which include the establishment of a single market, the Agreement identifies the free trade areas of the respective regional economic community's including SADC, as the building blocks guided by best practices within these economic communities.[311]

These aforementioned policies are the pillars of the of respective members states' national legislation and their significance cannot be overstated. Notably, these multilateral instruments play a dual role of providing guidance to the individual member

309 Article 5(2)(a) *The Consolidated Treaty of the SADC*.
310 Article 4(a) *Agreement Establishing the AfCFTA.*
311 Article 5 *Agreement Establishing the AfCFTA.*

states whilst also standardising the laws within the region. It is therefore imperative that these instruments are on par with international best practice.

The EU GDPR provides advanced personal data protection in the digital age without derogating from well-established data protection principles by placing the data subject at the centre of the factors establishing jurisdiction.[312] Furthermore, the GDPR provides a comprehensive framework for cross-border data transfers by prescribing the applicable rules when personal data is transmitted outside EU territory in a descending order of importance.

Comparatively, the SADC Model law similarly adopts the data protection principles and also includes provisions on cross-border data transfers. Notwithstanding that the model law also provides for the transmission of personal data to a third country which has not adopted the model law or a similar regulatory framework, it does not adequately reinforce the importance of ensuring that all such data transfers are subject to adequate safeguards. The SADC model law purports to adopt the same approach as the GDPR by first assessing whether the third country provides an adequate level of protection, however, it does not provide sufficient guidance as to which entity shall be empowered to make this decision, whether it will be an independent data protection authority or a government department. Furthermore, the GDPR clearly provides that in the absence of an adequacy finding, transfers to third countries shall then only be permitted if there are appropriate safeguards provided by the data processor or controller.[313] The SADC model law on the other hand only imposes a similar duty only on the data controller and not the data processor.[314] Whilst it may be argued that this may be because the data processor processes personal data for and on behalf of the data controller,[315] they must both be identified as sharing the common responsibility of data protection.

As at the time finalising this research paper, of the 16 SADC member states, 3 do not have any data protection legislation (Democratic Republic of Congo, Mozambique, and Comoros), and 7 only have draft legislation (Botswana, Malawi, Namibia,

312 Article 3 *GDPR.*
313 Article 46(1) *GDPR.*
314 Article 45(1) *Data Protection: SADC Model Law.*
315 Article 1(6) *Data Protection: SADC Model Law.*

Seychelles, Eswatini and Zimbabwe).[316] Within this context, it is conceivable that the SADC model law may be relied upon by any of the above-mentioned member states. It is all the more essential that as a model law, it be relevant and fit-for purpose.

5.2 Recommendations

The previous section highlighted the deficiencies of the SADC model law which have been further exacerbated by technological advancements. In order for the model law to remain relevant and promote the objective of harmonisation, the model law ought to be reviewed and updated.

Firstly, the scope of application needs to be data subject centric, even where the data controller or data processor is not physically present in the SADC member state or where the personal data is processed outside of the SADC member state provided there's a sufficient nexus between the activity of the data processor or data controller and the data subject residing in SADC member state, similar to the position adopted by the GDPR.[317] This will provide certainty on the applicable law and also provide the data subject with recourse should their personal data be misappropriated or not processed in accordance with the data protection principles. Furthermore, it will reinforce the data subject's rights where their personal data is transferred to third countries which have a different data protection regime.

Whilst some scholars have criticised that the unilateral expansion of the GDPR's jurisdiction may not always be appropriate in all circumstances and may inadvertently cause a network of conflicting applicable law, it has also been acknowledged that this can mitigated by identifying clear connecting factors.[318] The GDPR extends its jurisdiction in instances where the processing activities relate to the offering of goods or services to data subjects in the EU, or the monitoring of the data subject's behaviour where such behaviour takes place within the EU.[319] This approach implies that the

316 UNCATD Data Protection and Privacy Legislation Worldwide (undated) available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed 07-08-2020).

317 De Hert & Czerniawski (2016) 6 *International Data Privacy Law* 238.

318 *Ibid* 240.

319 Article 3(2) *GDPR.*

GDPR seeks to ensure adequate protection where EU data subjects are specifically targeted.[320]

Global data flows require that data protection be provided for through both national legislation and further advanced through co-operation between states and regions on the basis of similar principles. In the absence of a global law on data protection, the model law presents means through which greater co-ordination and harmonisation can be achieved within SADC, whilst also being cognisant of some of the unique developmental challenges facing the region. Data protection requires regional and multilateral collaborations on cross-border data protection and forums such as SADC can be instrumental in facilitating regulatory convergence.

320 Kong (2010) 21 *European Journal of International Law* 442.

Bibliography

Journal articles

Abrahams L “Regulatory imperatives for the future of SADC’s ‘digital complexity ecosystem’” (2017) 20 *The African Journal of Information and Communication* 1-29

Bu-Pasha S “Cross-border issues under EU data protection law with regards to personal data protection” (2017) 26 *Information & Communications Technology Law* 213 – 228

Bukht R & Heeks “Defining, Conceptualising and Measuring the Digital Economy” (2018) 13 *International Organisations Research Journal* 143-172

Buttarelli B “The EU GDPR as a clarion call for a new global digital standard” (2016) 6 *International Data Privacy Law* 77 – 78

De Hert P & Czerniawski M “Expanding the European data protection scope beyond territory: Article 13 of the General Data Protection Regulation in its wider context” (2016) 6 *International Data Privacy Law* 230 - 243

Hoofnagle C et al “The European Union general data protection regulation: what it is and what it means” (2019) 28 *Information & Communications Technology Law* 65 - 98

Jobodwana Z “Telecommunications Liberalisation in Africa: Proposed Regulatory Model for the SADC Region” (2009) 4 *Journal of Digital Forensics, Security and Law73 - 93*

Kong L “Data Protection and Transborder data flow in the European and Global Context” (2010) 21 *The European Journal of International Law* 441 - 456

Mattoo A & Meltzer J “International Data Flows and Privacy: The Conflict and Its Resolution” (2018) 21 *Journal of International Economic Law* 769 - 789

Roos A “Core principles of data protection law” (2006) 39 *The Comparative and International Law Journal of Southern Africa* 102 - 130

Wolters P “The security of personal data under the GDPR: a harmonized duty or a shared responsibility?” (2017) 7 *International Data Privacy Law* 165 - 178

Books

Blackman C & Srivastava L (eds) (2011) *Telecommunications Regulation Handbook Tenth anniversary* edition Washington DC: World Bank and the International Telecommunication Union

Buys R (ed) (2000) Cyberlaw @ SA: *The Law of the Internet in South Africa* Pretoria*:* Van Schaik Publishers

Calder A (2018) *EU GDPR: A Pocket Guide, School's Edition.* ITGP http://web.b.ebscohost.com.uplib.idm.oclc.org/ehost/detail/detail?vid=0&sid=49c4838f-5132-4943-ad70-938e7c185f7f%40pdc-v-sessmgr06&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=1901976&db=nlebk

ITGP PTIP (2017). EU General Data Protection Regulation (GDPR): *An implementation and compliance guide.* IT Governance Limited ProQuest Ebook Central https://ebookcentral-proquest-com.uplib.idm.oclc.org

Makulilo A (ed) (2016) *African data privacy laws* ProQuest Ebook Central https://ebookcentral-proquest-com.uplib.idm.oclc.org

Papadopoulos S & Snail S (2012) (eds) *Cyberlaw @ SA III: The law of the internet in South Africa* third edition Pretoria: Van Schaiks Publishers

Souter D (ed) (2009). *The APC ICT Policy Handbook* Association for Progressive Communications

Van der Merwe et al (2016) *Information and Communications Technology Law* second edition Lexis Nexis

Online sources

AU-EU (undated) Digital Economy Task Force available at https://www.africa-eu-partnership.org/sites/default/files/documents/finaldetfreportpdf.pdf (accessed 25-04-2020).

Chapman (2009) The history of the Internet in a Nutshell available at http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/ (accessed 25-04-2020)

European Commission (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions - A Digital Single Market Strategy for Europe available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (accessed on 07-08-2020)

EU (undated) EU Law available at https://europa.eu/european-union/law_en (accessed 28-05-2020).

ICC (undated) Our mission available at https://iccwbo.org/about-us/who-we-are/our-mission/ (accessed 25-04-2020).

ICC (undated) Trade in the Digital Economy: A primer on global data flows for policy makers available at https://cdn.iccwbo.org/content/uploads/sites/3/2016/09/Trade-in-the-digital-economy-A-primer-on-global-data-flows-for-policymakers.pdf (accessed on 10 April 2019)

Internet Society (2018) Personal Data Protection Guidelines for Africa available at https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed on 15 April 2019)

IMF (2018) Measuring the Digital Economy available at https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/04/03/022818-measuring-the-digital-economy (accessed 25-04-2020)

Internet World Stats (2020) Usage and Population Statistics available at https://www.internetworldstats.com/stats.htm (accessed 25-07-2020)

ITU (2013) Study on international internet connectivity in sub-Saharan Africa https://www.itu.int/en/ITU-D/Regulatory-Market/Documents/IIC_Africa_Final-en.pdf (accessed 25-04-2020)

ITU (undated) Overview of ITU's History available at https://www.itu.int/en/history/Pages/ITUsHistory.aspx (accessed 25-04-2020).

ITU (2019) Measuring digital development Facts and figures 2019 available at https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (accessed 25-04-2020)

ITU (undated) Support for Harmonization of ICT Policies in Sub-Sahara Africa Implementation strategy available at https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/HIPSSA_implementation_strategy_EN_090608.pdf (accessed 28-05-2020)

ITU (undated) Support for Harmonization of ICT Policies in Sub-Sahara Africa available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/hipssa/Pages/default.aspx (accessed 28-05-2020)

Mahler et al (2019) Internet Access in Sub-Saharan Africa http://documents.worldbank.org/curated/en/518261552658319590/pdf/Internet-Access-in-Sub-Saharan-Africa.pdf (accessed 25-04-2020).

McKinsey Global Institute (2017) The ascendancy of international data flows available at https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows (accessed 25-04-2020).

Odedra (1993) Sub-Saharan Africa: A Technological Desert http://www3.cis.gsu.edu/dtruex/courses/IB8710/Articles/Odedra-SubSahara-CACM1993.pdf (accessed 25-04-2020)

OECD (undated) About the OECD available at https://www.oecd.org/about/ (accessed 25-04-2020)

OECD (2016) Harnessing the digital economy for developing countries available at https://www.oecd-ilibrary.org/development/harnessing-the-digital-economy-for-developing-countries_4adffb24-en (accessed 25-04-2020).

OECD (2018) The Digital Economy, Multinational Enterprises And International Investment Policy available at http://www.oecd.org/investment/investment-policy/The-

digital-economy-multinational-enterprises-and-international-investment-policy.pdf (accessed 25-04-2020)

OECD (2011) Thirty Years After The OECD Privacy Guidelines available at http://www.oecd.org/sti/ieconomy/49710223.pdf (accessed 3-07-2020).

Research ICT Africa (2018) Measurement of the digital economy available at https://researchictafrica.net/wp/wp-content/uploads/2018/12/2018_Measurement-of-the-digital-economy_Africa-E-Week.pdf (accessed 25-04-2020)

Research ICT Africa (2019) SADC Parliamentary Forum Session IV: Harnessing the opportunities of the digital economy in SADC available at https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_SADC-Parliemantary-Forum.pdf (accessed on 30-05-2020).

SADC (2012) History and Treaty available at https://www.sadc.int/about-sadc/overview/history-and-treaty/ (accessed 28-05-2020)

Tralac (2018) Economic Partnership Agreement between the European Union and Southern African Development Community Group https://www.tralac.org/documents/resources/faqs/2049-sadc-eu-epa-faqs-july-2018/file.html (accessed on 15 April 2019)

UNCTAD (undated) About UNCTAD available at https://unctad.org/en/Pages/aboutus.aspx (accessed 25-04-2020)

UNCTAD (2019) Digital Economy Report 2019 Value creation and capture: implications for developing countries available at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf (accessed 25-04-2020)

UNECA (undated) What is Digital Identity, Digital Trade and Digital Economy for Africa? available at https://www.uneca.org/dite-africa/pages/what-digital-identity-digital-trade-and-digital-economy-africa (accessed 25-04-2020)

UNCATD (undated) Data Protection and Privacy Legislation Worldwide available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed 07-08-2020)

WTO (undated) What is the WTO? available at https://www.wto.org/english/thewto_e/thewto_e.htm (accessed 25-04-2020)

WTO (2018) World Trade Report The future of world trade: How digital technologies are transforming global commerce (2018) available at https://www.wto.org/english/res_e/publications_e/wtr18_e.htm (accessed 25-04-2020)

WTO (2011) Regional Integration in Africa available at https://www.wto.org/english/res_e/reser_e/ersd201114_e.pdf (accessed 28-05-2020).

South African Legislation

Electronic Communications and Transactions Act, 25 of 2002

International instruments

AU Convention on cyber security and personal data protection, (2014). Retrieved from https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

AU Agreement establishing the African Continental Free Trade Area, (undated). Retrieved from https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf

EU Charter of Fundamental Rights of the EU (2012). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

EU Consolidated version of the treaty on the functioning of the European Union (2012). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

EU Regulation (EU) 2016/679 of the European Parliament and of the Council 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). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

SADC Data Protection: SADC Model law (2013). Retrieved from https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

SADC *Declaration on Information and Communication Technology* (2001). Retrieved from http://www.sadc.int/documents-publications/show/830

Foreign case law

Case C-582/14 – Patrick Breyer v Bundesrepublik Deutschland.