LL.M. Minor Dissertation

Harmonisation of Data Protection Regimes in the Southern African Development Community: Considering the influence of the SADC Model Law on Data Protection and the European Union on data protection laws in SADC

By
Christoff Ferreira
(DPLCHR006)

Research dissertation presented for the approval of Senate in partial fulfilment of part of the requirements for the LL.M. specialized in International Trade Law for which the student is registered in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of LL.M. in International Trade Law dissertation, including those relating to length and plagiarism, as contained in the rules of this University and that this dissertation conforms to those regulations

Word Count: 23497

Supervisor: **Ms Robin Cupido**

February 2021

Acknowledgment

This thesis would not have been possible without the support of a number of people, in particular my family, friends and supervisor.

I would like to thank my supervisor, Ms Robin Cupido, for her consistent support and calm and positive demeanour throughout a challenging year. Without her guidance and insights, I would not have been able to produce this piece of work.

I would like to thank my friends and family for their continued support. To my Mother and Father, thank you for welcoming me back into your home, in the midst of the COVID 19 Pandemic.

Abstract

This minor-dissertation considers the issue of data protection coverage within the Southern African Development Community (SADC) and its importance to the Internet Telecommunications (ICT) sector in the various states of SADC but also its importance in providing protection to individuals in a region where internet penetration is increasing at a rapid pace.

SADC introduced the SADC Model Law with the assistance of the Support for Harmonisation of the ICT Policies in Sub-Saharan Africa (HIPSSA Project). This is meant to provide a model in terms of which states in SADC could introduce or improve their own data protection regimes. Nevertheless, this instrument has not been successful in changing data protection practices within SADC, with only one state introducing a draft Bill on the basis of the Model Law. Nonetheless, despite the apparent failure of the Model Law, there will still be a degree of harmonisation between the various data protection laws in the sub-region due to the influence of the European Union (EU)'s Data Protection Directive.

The approach taken is a comparative study which first considers the data protection laws of Mauritius and South Africa which have the two largest ICT sectors in SADC, the Zimbabwean draft Bill on Data Protection which was based on the SADC Model Law, and the Model Law itself. The purpose of this analysis is to determine whether a level of harmonisation has been achieved in SADC, despite the failure of the Model Law.

The next step was a comparative study between the Model Law and the European Union's Data Protection Directive 95/46/EC and the General Data Protection Directive (GDPR) 2016/679. The purpose of this was to track the development of data protection law in the European Union due to the impact which these laws had on data protection globally and to show differences between data protection regimes in SADC and the European Union.

The comparative study of laws in SADC illustrated that there is significant similarity between the laws considered, thereby proving that the Data Protection Directive played a more significant role in the harmonisation of data protection laws than the SADC Model Law. Nonetheless, the Model Law bared a significant resemblance to the other two existing data protection regimes. It also illustrated the weakness of the Model Law by demonstrating the lack of protection and shortcomings found in the Zimbabwean Bill based on the Model Law.

The comparative study between the regimes in the EU and the Model Law illustrates disparities in the level of protection found in the Current European regime, the GDPR and in SADC. The GDPR is stricter than the Model Law and has extra-territorial application with the potential to apply in SADC. Further, the Model Law is based upon the Directive, and is, thus, outdated and weaker.

The Model Law has, therefore, failed its stated goal of harmonising data protection laws in SADC yet there is still a degree of harmonisation due to the influence of the Data Protection Directive. The study showed the importance of having a strong data protection regime and also the shortcomings of existing regimes in SADC, when compared to the European Union.

Table of Contents

HARMONISATION OF DATA PROTECTION REGIMES IN SADC: THE SADC MODEL LAW ON DATA PROTECTION AND INFLUENCES OF THE EU.

1. INTRODUCTION

Fombad notes that it is important to consider the African continent in light of developments in technology and law, stating that it will be necessary to harmonize commercial laws to realise the continent's full potential.[1] The development of technology has led to the growth of ecommerce globally, and Africa's participation in ecommerce would lead to economic growth across the continent. [2] However, if African states wish to fully embrace the opportunities presented by ecommerce, there must be adequate regulation in place.[3]

One way to achieve such comprehensive regulation in the region is the harmonization of laws.[4] This can have the effect of eliminating legal obstacles and provides actors with certainty, which in turn promotes international trade and reduces transaction costs.[5] Efrat states that:

> The purpose of harmonised commercial law is to simplify the legal foundation of trade and to allow parties to save resources and to avoid controversy about the choice of law applicable to their transaction[6]

However, the growth of ecommerce has also changed the way in which commercial transactions take place, giving rise to new problems in international commercial law. [7] The United Nations Commission on International Trade Law ('UNCITRAL') recognised these problems and provided

[1] Charles Manga Fombad 'Some reflections on the prospects for the harmonization of international business laws in Africa: OHADA and beyond' (2013) 59 *Africa Today* 51 at 52.
[2] Nnaemeka Ewlukwa 'Is Africa ready for electronic commerce – a critical appraisal of the legal framework for ecommerce in Africa' (2011) 12 *European Journal of Law Reform* 550 at 551.
[3] ibid at 558.
[4] Ibid at 312; United Nations Commission on International Trade Law, Convention on Contracts for the International Sale of Goods (1980).
[5] David P Stewart 'Private international law, the rule of law, and economic development' (2011) 56 *Villanova Law Review* 607 at 608-9.
[6] Asi Efrat 'Promoting trade through private law: explaining international legal harmonisation' (2016) 11 *The Review of International Organisations* at 314
[7] DP Van der Merwe, A Roos & T Pistorius et al *Information and Communications Technology Law* 2 ed (2016) 149.

a Model Law on Electronic Commerce.[8] However, the UNCITRAL Model Law does not deal with what has become a key element of the digital economy: data protection.

The significant increase in internet usage in addition to the international nature of the internet has made the regulation of data privacy more important, especially in ecommerce where parties' personal information is used.[9]Data processors may not import or export data to and from jurisdictions without adequate protection, thereby hindering cross-border commercial activity.[10] States must thus have an adequate data protection regime in place.

The Southern African Development Community[11] ('SADC') has the potential to lead the drive for ecommerce on the continent yet it will face several challenges when transitioning towards life on the internet.[12] Regulators will be required to adopt innovative solutions to remain up to date with the latest technological developments.[13]

SADC has thus provided a Model Law on Data Protection that member states may use as a framework, should they wish to implement a data protection regime.[14] However, although the Model Law has been in existence since 2013, it has not made much progress in harmonising data protection laws within the sub-region.[15] This is because no SADC member state has implemented any data protection regime using the Model Law.

Rather, most SADC member states who have adopted data protection laws have done so based upon the European Union's ('EU') Data Protection Directive 95/46/EC directly.[16]

---

[8] Ibid at 154.
[9] United Nations Conference on Trade and Development *Data protection regulations and international data flows: implications for trade and development* (2016) at 1.
[10] Ibid.
[11] The member states of SADC are Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, the United Republic of Tanzania, Zambia and Zimbabwe.
[12] Lucienne Abrahams 'Regulatory imperatives for the future of SADC's "digital complexity ecosystem"' (2017) 20 *The African Journal of Information and Communication* 1 at 2.
[13] Ibid.
[14] Ewlukwa op cit at 566.
[15] Abrahams op cit at 18
[16] Alex B. Makulilo 'The context of data privacy in Africa' in Alex B. Makulilo (ed) *African Data Privacy Laws* (2016) 3 at 5.

The aim of this minor dissertation is thus to consider the reasons for the current failure of the Model Law and consider the consequences of this failure for consumers and for the facilitation of ecommerce within the sub-region. It will also consider the potential reasons why the identified SADC member states have chosen to follow the EU legislation as a guideline instead of the Model Law.

(a) Research questions

The question that this minor dissertation seeks to address is why the SADC Model law has failed to harmonise data protection laws in the sub-region since its inception. It will do so by questioning the following:

(i) How would the Model Law have been applied within SADC and to what extent would it have achieved harmonisation if its implementation were successful.
(ii) What is the current state of data protection within the sub-region.
(iii) Is the failure of the Model Law necessarily problematic considering national efforts to implement data protection laws.
(iv) What influence the EU Directive has had on the region, considering that most data protection regimes in SADC are based on it.
(v) What can SADC learn from the EU regarding data protection; and
(vi) Based on the analysis of the various data protection laws, what improvements and suggestions can be made for future attempts for harmonisation of data protection laws in SADC.

(b) Hypothesis

The hypothesis is that despite the SADC Model Law's failure to achieve harmonisation in the sub-region, most data protection regimes will still have a level of compatibility as most are based on the EU Directive, albeit coincidentally achieved.

(c) Literature review

(I) Electronic commerce and data protection

Although ecommerce across borders is beneficial, it is necessary to consider the use of consumer data in these types of transactions.[17] Sensitive consumer data is collected and analysed and data becomes a commodity that can be traded without the consumer's informed consent or knowledge.[18] This raises a number of privacy issues. Additionally, cross-border transactions are now easier as a result of the internet and pose another significant risk to the privacy of data subjects.[19] There is also the possibility of the processing of personal data for a purpose other than for which it was originally collected.[20]

Further, the internet is seen as 'national infrastructure, over which an increasing proportion of daily economic and social activity is carried out.'[21] Data protection laws, thus, provide the necessary safeguards for internet users. These laws are important to the facilitation of electronic commerce as they mitigate the risks of the exposure of personal data and provides for secure transactions online.[22] Additionally, data protection is necessary for the development of the internet itself as, without these rules, online consumers would have little trust in digital platforms.[23] Trust is critical to online businesses as it will affect the way the consumer interacts with the platform or whether the consumer will interact with the online platforms.[24]

UNCTAD has identified three categories that states fall into considering international data regulation. First, there are states with no data protection regimes at all,[25] which is problematic as it would limit such states' trade possibilities.[26] This would have big impact in the African context considering the continent's continued dependence on international trade. Second, there are states

[17] Van der Merwe et al op cit at 365.
[18] Morgan A. Corley 'The need for an international convention on data privacy: taking a cue from the CISG' (2016) 41 *Brooklyn Journal of International Law* 721 at 721-2.
[19] Julian Wagner 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) 8 *International Data Privacy Law* 318 at 318.
[20] Ibid at 319.
[21] Ibid.
[22] Ibid at 4.
[23] Ibid.
[24] M Dolores Gallego & Salvador Bueno 'Impact of B2C ecommerce codes of conduct on sales volume: lessons from the Spanish perspective' (2016) 31 *Journal of Business & industrial Marketing* 381 at 382.
[25] UNTAD op cit at 8. For example, Mozambique and Botswana.
[26] Ibid.

that have such legislation, but it is not comprehensive.[27] Third, there are some states where the data protection laws, although present, do not apply to certain sectors of the market,[28] limiting the scope of protection. There are African states in each of these categories, and it is clear that a more general data protection standard is needed. It is thus necessary to consider the level of data protection in SADC and assess the extent to which these rules provide protection to consumers in the sub-region.

(II) Data protection in SADC

The SADC Model Law on Data Protection provides that the harmonisation of the ICT sector is a necessary step towards trade liberalisation in the region.[29] In keeping with this aim of harmonization, the SADC Model Law on Data Protection (hereafter the Model Law) was drafted with the assistance of the International Telecommunications Union ('ITU'),[30] under the auspices of the Harmonisation of the ICT Policies in Sub-Saharan Africa ('HIPSSA') project.[31]

The Model Law seeks to provide states with a framework to use should they wish to implement their first data protection regimes.[32] It thus recommends a framework that can be transposed into national law by states as they see fit.[33] It should be emphasised that it is a soft law and that SADC member states are under no obligation to transpose it.[34] For example, South Africa has not changed its data protection laws to accommodate the Model Law and is unlikely to do so.[35] The South African Law Reform Commission had already started examining data protection in the late 2000s

[27] Ibid at 9; For example: Japan, Australia and Canada.
[28] Ibid; This will be the case where a company has applied to meet the provisions of the EU-US safe harbour requirements and is exempted from meeting some of the data protection requirements of EU law.
[29] Harmonization of ICT Policies in Sub-Saharan Africa *Data Protection: SADC Model Law* (2013) at iii.
[30] Caroline B. Ncube 'Data protection in Zimbabwe' in Alex B. Makulilo *African Data Privacy Laws* (2016) 99-116 at 111.
[31] Ibid.
[32] Ibid.
[33] Patricia Boshe 'Data privacy law reforms in Tanzania' in Alex B. Makulilo (ed) *African Data Privacy Laws* (2016) at 173.
[34] Alex B. Makulilo & Kuena Mophethe 'Privacy and Data Protection in Lesotho' in Alex B. Makulilo *(*ed) *African Data Privacy Laws* (2016) 337-348 at 339
[35] Ibid at 378.

and the first draft Bill for data protection in South Africa was introduced in 2009, four years before the SADC Model Law.[36]

Makulilo notes that a key motivator for African states to establish data protection regimes is the possibility of attracting foreign investment, especially from Europe.[37] Perhaps for this reason, the EU Data Protection Directive[38] has influenced the development of many data protection regimes i n Africa, which can be seen in national and regional policies.[39] Makulilo suggests that as most post-independence African states have retained their colonial legal system to some extent, the EU Directive is extremely compatible with African legal systems.[40] However, no African data protection regime has been deemed adequate by the European Commission to date, leading to questions about the extent of such compatibility.

Despite this influence of the EU Directive in Africa, it should be noted that, in the interim, in the EU the Directive has been replaced by the General Data Protection Regulation ('GDPR'),[41] which has an updated set of rules for data protection. This means that the African regimes are already behind the latest developments, and it is thus more important that the Model Law reflect current data protection standard if it is to be successful.

The use of the Model Law 'is seen as a way to promote common approaches to common problems, as well as a means to create similar regulatory environments, thereby encouraging investment, competitive regional markets and consumer access.'[42] The Model Law is thus a necessary step in creating a single digital economy within the region.[43] However, a concerted effort by all member states will be required to successfully harmonize the existing and non-existing data regimes in the region, which has not happened yet.

---

[36] Anneliese Roos 'Data Protection Law in South Africa' in Alex B. Makulilo *African Data Privacy Laws* (2016) 189-228 at 202.
[37] Alex Makulilo op cit at 18.
[38] 94/45/EC; Graham Greenleaf 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 *International Data Privacy Law* 68 at 77.
[39] Makulilo op cit at 19.
[40] Ibid.
[41] Paul De Hert & Vagelis Papakonstaninou 'The proposed data protection regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28 *Computer & Security Review* 130 at 130.
[42] Ibid at 16.
[43] Ibid.

For example, in Zimbabwe, following successive decades of political turbulence, the right to privacy is now enshrined within the state's Constitution.[44] The internet is used in the country by a broad range of actors from the state to businesses and private individuals and there is significant internet usage in the country.[45] During the HIPSSA project missions to Zimbabwe, training on data protection law; national assessment on data protection; and the Zimbabwe Data Protection Bill were covered yet the Government has yet to enact any laws.[46] Ncube argues that Zimbabwe should use the Model Law or the AU Convention on Cyber Security and Personal Data Protection Law to properly regulate data protection.[47]

Another SADC state which has lacking adequate data protection standards is the Seychelles.[48] Despite being a member of SADC, the country has not yet implemented national laws which reflect the Model Law.[49] The Seychelles has implemented their own Data Protection Act of 2003, but this is based upon the United Kingdom's Data Protection Act of 1984.[50] In the United Kingdom, this law was repealed as a result of the EU Directive on Data Protection and is clearly outdated.[51]

Mozambique is in a worse position than Zimbabwe and the Seychelles concerning data protection laws as the state has yet to implement any data protection regime.[52] This is despite the fact that the country has experienced changes to society as a result of technological advances.

Although the above three states have inadequate data protection laws, the situation is different and more promising in the other SADC member states with most states adopting laws that have been modelled on the EU Directive on Data Protection. Boshe provides that in Tanzania, data protection law reform is taking place with the Model Law being transposed into national law by the Draft

[44] Ncube op cit at 101.
[45] Ibid at 102.
[46] Ibid.
[47] Ibid at 113.
[48] Alex B. Makulilo 'Data Protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagascar' in Alex B. Makulilo *African Data Privacy Laws* (2016) 277 at 292.
[49] Ibid at 292.
[50] Ibid at 295.
[51] Ibid.
[52] João Luís Traça & Lidia Neves 'Data Protection in Mozambique: Inception Phase' in Alex B Makulilo *African Data Privacy Laws* (2016) 363-370 at 363

Privacy and Data Protection Bill.[53] Tanzania is a member of two regional economic communities, the East African Community ('EAC') and SADC. The EAC provides that member states should adopt several data protection principles whereas SADC provides the Model Law.[54] Tanzania decided to implement the Model Law. By participating in the HIPSSA project Tanzania received 'financial, technical and expert support from the International Telecommunications Union, the European Commission and the EU.'[55] This is a clear effort to promote the implementation of the SADC Model Law in Tanzania. Tanzania is one of the only SADC member states to start implementing the Model Law as it is. Many of the other member states chose to draw directly from the EU Directive on Data Protection instead.

South African law is not based upon the SADC Model Law but rather upon other comparable standards. For example, the Protection of Personal Information Act[56] is primarily based upon the Organization of Economic Cooperation and Development's ('OECD') Guidelines on Data Protection as well as the EU Directive.[57] The reason for the use of the EU Directive is the fact that the EU is the country's largest trading partner,[58] and thus it would be beneficial to follow similar data protection rules.

Lesotho provides an interesting situation as its data protection regime is based upon several influences as opposed to a single source. The privacy principles adopted by Lesotho reveal connections to South African data protection law (as South Africa is Lesotho's main trading partner), to the SADC Model Law and to the EU Data Protection Directive.[59] Their law attempts to provide a legislative framework for data protection that is in line with international best

[53] Boshe op cit at 176.
[54] Ibid at 173.
[55] Ibid.
[56] 4 of 2013.
[57] Roos op cit at 201-2
[58] Hanno N. Olinger, Johannes J. Britz & Martin S. Olivier 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy Bill' (2007) 39 *The International Information and Library Review* 31 at 32.
[59] Makulilo op cit at 342.

practices.[60] Yet, the primary influence is South African law.[61] This is due to South Africa's impact on the economic growth of the sub-region.[62]

In Mauritius, the ICT sector is one of the pillars of its economy.[63] The country has consciously sought to legislate on data protection and electronic commerce to facilitate the growth of the sector.[64] However, despite being a member of SADC, Mauritius' national data protection laws do not reflect the Model Law.[65] The primary legislative means of data protection is the Data Protection Act of 2004, which has since been amended.[66] Amendments were made in order to keep the data protection regime up to date and were made with expert advice from the EU.[67] The primary reason for amendment was to meet the EU's adequacy requirements with a view to attract more foreign investment.[68]

Madagascar is also a SADC member state, yet its data protection laws are not representative of the SADC Model Law.[69] The Data Protection Act of 2015 provides the legislative framework for the protection of personal data and it too is based primarily on the EU Data Protection Directive.[70] The rationale for implementing the Act was to improve and modernise the economy.[71]

Angola's data protection regime draws mostly from the EU Data protection directive as well as from Portuguese law.[72]

---

[60] Ibid at 340
[61] Ibid at 342.
[62] Beverley Alice Townsend *Privacy and data protection in eHealth in Africa – an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health care in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking* (unpublished LLD thesis, University of Cape Town, 2017) at 85.
[63] Makulilo op cit at 278.
[64] Ibid.
[65] Ibid at 281.
[66] Ibid at 283.
[67] Drudeisha Madhub 'The pioneering journey of the Data Protection Commission of Mauritius' (2013) 3 *International Data Privacy Law* 239 at 240.
[68] Ibid.
[69] Makulilo op cit at 299.
[70] Ibid.
[71] Ibid.
[72] João Luís Traça & Francisca Correia 'Data Protection in Angola' in Alex B. Makulilo African Data Privacy Laws (2016) at 350.

From this we see that there is no uniform set of data protection rules that apply throught all of SA DC and some states where there is no data protection regime at all. However, all of these regimes share a common link: European principles of data protection.

(III) Data Protection in the EU

From the brief discussion above, it is evident that the EU Data Protection Directive is central to many data protection regimes outside of Europe.[73] The EU Directive was intended to implement the privacy principles of the OECD.[74] The General Data Protection Regulation (GDPR) has taken the place of the Directive and has further increased the standard of data protection in the EU.[75] The GDPR seeks to find a balance between the commercial need for data transfers and the protection of the right to privacy.[76] Despite the shift to the GDPR, the provisions concerning the export of data are similar to those of the Directive.[77] The transnational flow of data is now regulated by Articles 44 to 50.[78]

The GDPR's application extends beyond the jurisdiction of the EU. Where the Directive applied only to data processors within the EU, the GDPR applies to outside data processors, should they process the data of EU citizens.[79] Additionally, as with the Directive, the GDPR requires third countries to strengthen their data protection regimes.[80] The European Commission 'EC' has not yet indicated which African states meet the adequacy requirements in terms of the new GDPR,[81] something which will necessarily affect continued trade between the regions.

[73] Olinger et al op cit at 32.
[74] Tiwalade Adelola, Ray Dawson & Firat Batmaz 'Privacy and data protection in ecommerce in developing nations: evaluation of different data protection approaches' (2014) 5 *International Journal of Digital Society* 976 at 976.
[75] Ibid.
[76] Ibid at 320.
[77] Ibid at 319.
[78] Ibid at 320.
[79] Yves Poullet 'Is the General Data Protection Regulation the solution' (2018) 34 *Computer Law & Security Review* 773 at 774; Sahar Bhamimia 'The General Data Protection Regulation: the next generation of EU Data Protection' (2018) 18 *Legal Information Management* 21 at 24.
[80] Ibid.
[81] Santa Slokenberga, Jane Reichel & Rachel Niringiye et al. 'EU data transfer rules and African legal realities: is data exchange for biobank research realistic' (2019) 9 *International Data Privacy Law* at 36.

Interestingly, the debate concerning the importance of data protection has gone much further in Europe. There is a growing awareness of the economic value attached to personal data and the processing thereof.[82] Versaci considers the ongoing debate in the EU considering the Commission's proposal to introduce a 'Directive on contracts for the supply of digital content'.[83] The effect of this directive would be that digital contracts where the counter-performance is payable in money would be treated the same as those digital contracts where counter-performance is payable in personal data.[84] The author argues against the proposal of the Commission because of the discrepancies between the law of contract and data protection law.[85] First, the notion of counter performance is grounded within the law of contract and this concept is not necessarily compatible with data protection rules.[86] Secondly, and significantly within the EU, in the EU Charter of Fundamental Rights 2012/C 326/02 data protection is a fundamental right. The author, thus, argues that there cannot be a commodification of any fundamental right.[87]

This illustrates the importance of data protection in the EU. As data protection is protected as a fundamental right, it is likely that protection measures will be far more stringent. Additionally, it could explain the need for the adequacy standard and why Europe is involved in promoting data protection laws in Africa. It also illustrates that the debates concerning data protection at the policy level in Europe are at a completely different stage than they are in Africa. Where the state of economic development and technological infrastructure is completely different.

(IV) Conceptions of data protection

It is important to consider the differences in the conceptions of data protection. This is because cultural and socio-economic backgrounds play an important role in creating appropriate data protection laws.[88]

[82] Giuseppe Versaci 'Personal data and contract law: challenges and concerns about the economic exploitation of the right to data protection' (2018) 14 *European Review of Contract Law* at 376.
[83] Ibid at 377.
[84] Ibid at 378.
[85] Ibid.
[86] Ibid.
[87] Ibid at 379.
[88] Adelola op cit at 977.

In the EU, data protection laws must be understood in conjunction with the fundamental rights of privacy and the right to the protection of personal data.[89] The right to the protection of personal data is 'an enabling human right that renders a discrete contribution to the realization of a number of other rights and freedoms of the individual.'[90] Data protection allows for intervention in data processing and this protects the individual's right to autonomy and dignity.[91]

Another significant impact on the development of data protection law in Europe is the judgment in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12,[92] where the European Court of Justice ruled that the data subject's rights take preference over the commercial interests of the data processor.[93] This has resulted in a provision in the GDPR which ensures a 'right to be forgotten'.[94] Furthermore, European institutions are of the opinion that this right should be applied extraterritorially so as to provide protection to their citizens wherever their data is processed.[95]

The protection of personal data is thus an independent right and is not part of the right to privacy, albeit a related concept.[96] This right should be seen as an enabling right which allow for the complete protection of the right to dignity and personal autonomy.[97] Central to the development of this understanding of the right are the rights, often cited in European legal tradition, of personal autonomy and dignity.[98]

This conception of privacy and data protection can be contrasted against traditional African perceptions of the rights. Makulilo opines that privacy is an inherently western concept that derives

[89] Manon Oosteven & Kristina Irion 'The golden age of personal data: how to regulate an enabling fundamental right' in Mor Bakhoum, Beatriz Conde Gallego & Mark-Olver Mackenrodt et al (eds) *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (2018) 7-26 at 8.
[90] Ibid.
[91] Ibid.
[92] Case C-131/12.
[93] Giancarlo F. Frosio 'The right to be forgotten: much ado about nothing' (2017) 15 *Colorado Technology Law Journal* 307 at 307-8.
[94] Ibid.
[95] Ibid at 330.
[96] Oosteven & Irion op cit at 9.
[97] Ibid.
[98] Ibid at 13.

from autonomy.[99] It is because of individual autonomy that a person can claim his or her right to a private sphere.[100] However, outside of the western world, this approach differs.[101] It can be argued that in numerous African cultures, due to collectivism, group interests or the common good are given priority over the individual interest.[102] One can forward this argument by considering that there is no entrenched right to privacy in the African Charter of Human and Peoples Rights.[103] Some authors argue that pressure from the western world on African and non-western states to enact laws relating to privacy can be a form of cultural imperialism.[104]

Despite this, the fact remains that one of the key motivating factors for development in Africa is the need to participate in the digital economy.[105] African states have acknowledged the significance of electronic commerce and its ability to transform economies while providing adequate protection to consumers and should thus build regimes that promote trust.[106] In some African states there is a constitutional right to privacy accompanied with its own jurisprudence and discourse, yet this has not gone so far as to encapsulate data protection as a free-standing principle.[107]

It is thus apparent that Europe and Africa are at different stages of the development of their jurisprudence on data protection and privacy. Nonetheless, the European conception of data protection has had a profound impact on data protection laws in Africa, and this must be borne in mind when assessing the development of data protection in Africa.

(d) Importance of the study

[99] Alex B. Makulilo 'Myths and reality of harmonization of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* at 78.
[100] Ibid.
[101] Ibid.
[102] Kenneth Kaoma Mwenda 'Deconstructing the concept of human rights in Africa' (2000) 25 *Alternative Law Journal* 292 at 294.
[103] Makulilo op cit at 78.
[104] Ibid.
[105] ibid.
[106] Andrew Harris, Seymour Goodman & Patrick Traynor 'Privacy and security concerns associated with mobile money applications in Africa: Mobile Money Symposium 2013' (2013) 8 *Washington Journal of Law, Technology and Arts* 245 at 257-8.
[107] Makulilo op cit at 78.

The proposed topic of study will illustrate how the SADC Model Law has failed to harmonise laws in the sub-region, while highlighting the need for the harmonisation of data protection laws in order to facilitate the growth of the digital economy and for the protection of data subjects. A proper analysis of the shortcomings of the Model Law can provide guidance on how to remedy the gaps in data protection law in SADC and implement a successful harmonised data protection regime. The analysis of the national data protection laws of the member states will show whether harmonisation has been achieved within the sub-region, albeit unintentionally, as most data protection regimes are based on the EU Data Protection Directive. The study will also shed light on the EU's influence on the data protection laws in the SADC region. In doing so it will demonstrate that the context in which laws are implemented make a difference to whether these laws succeed.

(e) Research Methodology

This work will begin by examining the SADC Model Law, focusing on its aims and how such aims would be achieved. After consideration of the SADC Model Law, the attention will shift toward the national data protection laws of the SADC member states. These member states all fall into three categories: (i) those states that have begun reform of their data protection laws using the Model Law through the HIPSSA project; (ii) those states that have data protection laws based upon the EU Data Protection Directive; and (iii) those without any adequate data protection standards.

Due to the influence of the EU data protection regime in SADC the development of data protection in the European context will also be considered. Lastly, a comparative analysis will be conducted between the two sub-regions. In this instance, the impact of EU law in Africa will be considered as well as the differences in the methods of achieving harmonization.

(f) Limitations

The focus of this dissertation will be on data protection, ecommerce and the harmonisation of private law. The SADC Model Law on Data Protection and the EU Directive and Regulation will be considered. National laws will be considered to the extent of demonstrating fragmentation and discrepancies between the member states of SADC.

2. PURPOSE OF DATA PROTECTION

(a) Ecommerce and data protection in developing nations

To provide context for the operation of data protection regimes one must consider ICT, ecommerce and data protection, especially within developing nations. There is a debate concerning the lack of internet access in developing countries. Key issues in this debate include the high cost of introducing internet infrastructure and whether such infrastructure will positively impact development.[108] Moore's law provides that developments in ICT occur at a rapid pace with the result that ICT products become cheaper and accessible.[109]

This has caused an increase of internet penetration in the developing world due to the reduced costs of providing internet access. With easier means of internet access, more individuals can transact using the internet, mainly through mobile telephone technology.[110] Ecommerce has thus become a legitimate strategy for development and a means to increase the size of developing economies.[111]

However, despite the increase of internet access in developing countries there is a digital divide between developed and developing states.[112] The digital divide refers to the asymmetrical development of ICT in states, where the prevalence of the digital economy varies between different population groups.[113] Van Dijk provides another definition for the digital divide, namely that it is a 'division between people who have access and use of digital media and those who do not'.[114] The digital divide pertains to both internet access and internet literacy. Internet access is only part of bridging the digital divide.[115] This is because it is necessary to consider improving access to ICT, to increase engagement with ICT in order to prevent digital illiteracy and to improve the

[108] Andrea Goldstein & David O'Connor 'An introduction to the debate on electronic commerce and development' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) 8.
[109] Cyrus C.M. Mody *The Long Arm of Moore's Law: Microelectronics and American Science* (2016) at 7-8.
[110] Ibid at 14.
[111] Ibid at 9
[112] Gary Gereffi 'The evolution of global value chains in the internet era' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) at 19.
[113] Patrizia Fariselli 'Ecommerce for development: a general framework' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) at 37.
[114] Jan Van Dijk *The Digital Divide* (2020) 9.
[115] Stephen McNair 'The emerging policy agenda' in OECD *Learning to Bridge the Digital Divide* at 10.

competitiveness of the users of this technology.[116] Policies aimed at remedying the asymmetry of technological development should take into consideration the effect that the digital economy can have on development.[117] Policymakers should be aware of the need to build digital skills in addition to the provision of internet infrastructure as, in the twenty-first century, the ability to use technology properly will be the main factor that can close the gap of the digital divide.[118] Studies at the turn of the century noted that technological exports had becomes as important as manufacturing exports and that developing nations should invest in technology as a means of increasing gross domestic product through the digital economy[119]

The introduction of the digital economy has been shown to have a positive impact on both Business to Business (B2B) and Business to Consumer (B2C) contracts. The digital economy has also increased the amount of information that is available to contracting parties because it is now easier to share data.[120] However, this has introduced new dangers to consumers who interact with online platforms as they place their personal information at risk.[121]

To facilitate this transition, the appropriate framework should be in place.[122] At the core of the growth of the digital economy lies data. The greater the size of the digital economy, the greater the amount of data that is processed.[123] Lack of an adequate ICT framework can result in higher costs when conducting business online through the digital economy.[124] As such, a good starting point for developing countries would be to improve their ICT infrastructure and to increase the ICT skill levels.[125] A lack of legal regulation of the digital economy also leads to uncertainty which

[116] Ibid at 16 – 17.
[117] Op cit Fariselli at 35.
[118] Op cit Van Dijk at 61.
[119] Guillermo Kelley-Salinas 'Different Educational Inequalities: ICT an Option to Close the Gaps' in OECD *Learning to Bridge the Digital Divide* (2000) at 24.
[120]Op cit Fariselli at 36.
[121] Ibid at 37.
[122] Ibid.
[123] Ibid at 14.
[124] David O'Connor 'Ecommerce for development: between Scylla and Charybdis' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) at 55.
[125] Op cit Fariselli at 46

may prevent consumers from transacting online and prevent businesses from digitising their businesses.[126]

The level of trust that consumers have in an online vendor can also influence the success of the vendor's business.[127] The notion of perceived fairness is important. If an online platform provides a greater level of perceived fairness, then consumers will be more likely to conduct business using the platform.[128] If states implement adequate regulatory environments in which online vendors are obliged to operate, there will be an increase of trust online, encouraging ecommerce.[129]

Consent of the data subject is the cornerstone of most data protection regimes. When a data subject consents to give their data in exchange for use of an online platform, they consent to the analysis of their personal data and their behaviour online.[130] This observation is done mainly through corporations and is known as 'economic surveillance'.[131] Collected data is either used by the online platform, sold to advertisers or, in some instances, collected by state authorities for law enforcement purposes or to pursue a political agenda.[132]

The relationship between the online platform and the consumer or data subject is an ongoing one.[133] This has implications for consumer trust in the online space because the consumer is required, at the outset, to provide initial personal information and further information will be collected whenever the consumer interacts with the online platform.[134] The ongoing nature of this relationship can make it difficult to obtain consent for all future data collection,[135] and there is great potential for the consumer's information to be exploited. States should thus aim to have

---

[126] Deo John Nangela *The Adequacy of the Tanzanian Law on Ecommerce and E-contracting: Possible Solutions to be Found in International Models and South African Legislation* (unpublished PhD Thesis, University of Cape Town, 2011) at 6.
[127] Wei Sha 'The nomological network validity of perceived fairness in business-to-consumer ecommerce' (2014) 15 *Issues in Information Systems* 328 – 334.
[128] Ibid at 329.
[129] Simon Fraser 'Persistent barriers to ecommerce in developing countries: a longitudinal study of efforts by Caribbean companies' (2011) 19 *Journal of Global Information Management* at 33.
[130]Angela Daly *Private Power, Online Information Flows and EU Law: Mind the Gap* (2016) at 20.
[131] Ibid
[132] Ibid
[133] Erkki Patokorpi & Kai K. Kimppa 'Dynamics of the key elements of consumer trust building online' (2006) 4 *Information, Communications and Ethics in Society* at 19.
[134] Ibid
[135] Ibid

adequate data protection regulations in place for consumer protection to encourage the growth of the digital economy. It is also apparent that there is a need for the improvement of the digital economy in developing countries. Data protection in developing countries is thus a key part of the strategy for successfully transitioning to the digital economy.

(b) The development of data protection principles

Currently, there is no over-arching international data protection regime and data protection laws are covered by national legislatures.[136] This should not necessarily be considered negative due to the varying degrees of privacy that exist in the social contexts of different nations.[137] However, the internet creates universal problems and it has thus been argued that it should be dealt with through the implementation of universal laws.[138] Weimann and Nagel highlight the case of Facebook and how it has successfully 'harmonised' data protection laws using a bottom-up approach through the platform's privacy policy.[139] Unfortunately for the authors, their article was published before the Cambridge Analytica scandal[140] which demonstrated online platforms' inability to use personal data in a responsible manner. Cambridge Analytica gained access to the personal data of millions of Americans and used this data to target voters based on their ideological profile. A consequence of the company's action is a loss of autonomy of the data subject,[141] as the company used data collection to target voters on a psychological level by targeting their 'ideological prejudices'.[142] This manipulation of users has had a negative impact on the trust between users and social media platforms and reinforces the need for adequate data protection by companies. The regulation of privacy and data protection should thus not be left to privately-owned online platforms, and it is clear that general standards of data protection should be implemented.

[136] Thomas Weimann & Daniel Nagel 'Agreeing on a definition for data protection in a globalized world' (2012) *IEEE Technology and Society Magazine* at 40.
[137] Ibid at 41.
[138] Ibid.
[139] Ibid.
[140] Julia Carrie Wong 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook' available at *https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook,* accessed on 22 May 2020.
[141] Ken Ward 'Social networks, the 2016 US presidential election and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioural microtargeting' (2018) 3 *Journal of Media Ethics* at 141
[142] Ibid.

An argument that is often made with respect to law and technology is that laws are outdated and lag behind technological developments.[143] The challenge of remaining up to date with technological developments is an ongoing one, yet law can only be made considering the facts available at the time. Laws can thus not always adequately regulate new technologies, but there is still an impact of law on the development of technology, which is often overlooked.[144] This is important in the context of data protection laws as these regimes impose a standard through the adoption of various principles. The development of data processing technology such as big data analytics should be informed by existing data protection principles.

The very first document introducing general data protection principles was the *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens*.[145] Significantly, this document introduced the rights of data subjects, which have since been replicated by the OECD and the EU.[146]

General data protection principles and the rights of the data subject can be seen in the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which lists the principles of data protection that states should apply in their own national laws.[147] These principles include the Collection Limitation principle[148]; the Data Quality Principle[149]; the Purpose Specification Principle[150]; the Use Limitation Principle[151]; the Security Safeguards[152]; and the

[143] Lyria Bennet Moses & Monika Zalneriute 'Law and technology in the dimension of time' in Sofia Ranchodás & Yaniv Roznai (eds) *Time, Law and Change: an Interdisciplinary Study* (2020) at 303.
[144] Ibid.
[145] U.S. Department of Health Education & Welfare *Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973)
[146] Roger Taylor 'No privacy without transparency' in Ronald Leenes, Rosamunde van Brakel & Serge Gurtwith et al (eds) *Data Protection and Privacy: The Age of Intelligent Machines* (2017) at 71.
[147] Part 2, Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.
[148] Paragraph 7: the collection of personal data can only occur if the data subject has consented to this collection and it is lawful.
[149] Paragraph 8: data collected should be 'relevant to the purposes for which [it] should be used' and that the accuracy of the data should also be ensured.
[150] Paragraph 9: the purpose for the collection of personal data should be provided at the latest, by when the data is collected and, further, that the data only be used for that purpose.
[151] Paragraph 10: 'Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9' unless the data subject has consented or there is legal authority permitting disclosure.
[152] Paragraph 11: reasonable security safeguards should be in place to protect the data.

Openness Principle.[153] These principles build on the fundamental principles of fair information practice found in the *Report*.

The OECD based their Guidelines on the *Report*,[154] and the EU Directive contains a similar set of principles.[155] The EU Directive was based on the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data came into force in 1985[156] as well as the OECD guidelines.[157] The purpose of the Data Protection Directive was to harmonise the laws of EU member states.[158] In the GDPR, these principles have been further developed to provide more comprehensive protection. A crucial part of these legal texts is that they provide for 'informational self-determination'.[159]

Corte notes that data protection can be considered *sui generis* because it is a fundamental right that is derived from legislation that initially regulated data processing.[160] The laws regulating the right preceded the existence of the fundamental right itself within the European context. Yet, this is not the case for all European legal systems.[161] This is because some countries within the EU still link the right to data protection to the right to privacy, such as in the Netherlands and Portugal, or to *das allgemeine Persönlichkeitsrecht*[162] in Germany. There is clearly a disparity between the interpretation and understanding of the right at the supranational and national levels.

[153] Paragraph 12: 'there should be a general policy of openness about developments, practices and policies with respect to personal data'.
[154] Op cit Taylor at 71
[155] Directive 95/46/EC.
[156] ETS No. 108.
[157] Michael D. Birnhack 'The EU Data Protection Directive: an engine of a global regime' (2008) 24 *Computer Law & Security Report* at 511.
[158] Rebecca Wong 'The Data Protection Directive 95/46/EC: idealisms and realisms' (2012) 26 *International Review of Law, Computers and Technology* at 230.
[159] Andrea Monti & Raymond Wacks 'Personal Information and data protection' in Andrea Monti & Raymond Wacks (eds) *Protecting Personal Information: The Right to Privacy Reconsidered* (2019) at 19.
[160] Ibid at 28.
[161] Douwe Korff *EC Study on Implementation of Data Protection Directive: comparative summary of national laws* (2002) at 8.
[162] This is a right enshrined in the German Constitution which provides for a right to respect an individual's personality; Ibid.

However, Corte emphasises the need for the right to data protection to be separated from the right to privacy.[163] Conflation between the two rights can create obstacles that may hinder the development of the right to personal data protection.

Corte also considers the development of data protection and the relation of data protection and privacy. A significant turning point was a decision by the German Constitutional Court in 1983 *Population Census Decision*.[164] This seminal decision provided the foundation for data protection as it is understood in Germany today.[165] The core concept on which the decision turned was 'informational self-determination', a right which data processing interfered with.[166] Informational self-determination refers to an individual's right to control the processing of their information.

The next development resulted from issues concerning the cross-border transfer of data. It was at this stage that the OECD and the Council of Europe turned their attention to data processing laws.[167] The first international treaty providing for data protection was the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[168] When it was introduced, data protection was still considered to be part of the right to privacy. It was only after further developments (such as the Data Protection Directive) that conceptions of data protection started to change. Data protection became a free-standing right in the Charter of Fundamental Rights of the EU.[169] The latest development of this right in the European context was the GDPR.[170]

From this discussion, it is evident that the development of data protection laws has occurred mostly in the European context. The EU Directive has been recognised as a 'prominent trendsetter for data protection norms'.[171] European data protection policy has thus had far reaching implications

[163] Op cit Corte at 28.
[164] BVerfG, 1 BvR 209/83, Judgement of 15 December 1983.
[165] Op cit Corte at 32.
[166] Ibid
[167] Ibid at 33.
[168] ETS 108
[169] 2012/C 326/02.
[170] Regulation (EU) 2016/679.
[171] Op cit Bygrave at 47.

on other states when implementing data protection laws, permeating into African data protection regimes through the influence of the EU Data Protection Directive.[172]

(c) Definitions

Before commencing a more detailed discussion on data protection, it is necessary to outline some of the key terminology used in data protection laws. For this purpose, the definitions found in the SADC Model Law, the GDPR and the domestic data protection regimes of South Africa, Mauritius and Zimbabwe will be considered. The definitions of data, data subject, processing, consent will be discussed.

(I) Data

'Data' is a core concept, and it is interesting that there are disparities between the definition in the different legal texts. In the SADC Model Law 'data' is broadly defined as 'all representations of information notwithstanding format or medium'[173] and contains a separate definition for 'sensitive data'. In the Protection of Personal Information Act 4 of 2013 ('POPI') there is no definition of 'data', only a definition of 'personal information'.[174] Under this definition, there are several sub-categories. Even though 'data' is not explicitly defined, the Act is applicable to the processing of personal information of the data subject and, thus, the definition of personal information explicitly refers to data. Mauritius passed the Data Protection Act 20 of 2017 which contains its own definition of 'data', defining personal data as 'any information relating to a data subject'.[175] The definitions also provide a list of special categories of personal data similar to those contained in POPI in South Africa.[176]

The Zimbabwean draft Bill[177] although drafted with the assistance of the HIPSSA does not resembles the SADC Model Law but rather POPI in that it provides a definition for personal

[172] Mauritius, Angola, Madagascar and Lesotho are some of the states within SADC that have data protection laws based on the EU directive.
[173] Part 1, Article 1 (3) *SADC Model Law* (2013)
[174] Section 1.
[175] Section 2
[176] Section 2 'Special categories of personal data'
[177] H.B 18, 2019.

information rather than data in Clause 3 on interpretation. Furthermore, the rules differ for the processing of non-sensitive data and sensitive data.[178] This shows that in drafting the Bill, it is clear that the Data Protection Law of Zimbabwe's neighbour and primary trading partner was also considered

The EU data protection regime includes definitions of 'personal data' in both the Directive and the GDPR. In the Directive, 'personal data' is defined as data that relates to a natural person who is identifiable with respect to several categories.[179] The GDPR extends this definition and includes genetic data, biometric data and data concerning health as subcategories of personal data.[180]

A notable difference between the African and European definitions of data is that the African regimes are more specific in listing certain categories of personal information. The definition of sub-categories does not, however, indicate that it is a closed list. In POPI it is explicitly stated that the list is 'not limited to' the specific sub-categories. In the Mauritian Act it is not explicitly mentioned that the list is not a closed one but in terms of sub-section (j) of the definition of special categories of personal data the Commissioner is allowed to determine personal data not listed as 'sensitive personal data'. In the Zimbabwean Bill, no wording similar to the South African and Mauritian data protection regimes can be found but 'data' itself is broadly defined[181] and it can thus be argued that this will prevent a narrow interpretation of data. Interestingly, the SADC Model Law contains no sub-categories of data, illustrating divergence between the Model Law and the national laws currently being implemented within the sub-region.

(II) Data Subject

The notion of 'data subject' is crucial as it refers to who will be protected by data protection regimes. In the SADC Model Law, a 'data subject' is defined as 'any individual who is the subject of the processing of personal data and who is identified or identifiable'.[182] The South African definition in POPI is similar yet it is worded with reference to personal information rather than

[178] Section 12 – 13.
[179] Article 2(a) 95/46/EC.
[180] Article 4 (1), (13), (14) & (15)
[181] Section 3.
[182] Article 1(8).

data,[183] as 'data' is not a concept explained in the Act.[184] In Mauritius, the definition of 'data subject' bears resemblance to the definition in the SADC Model Law, but expands on the notion of 'data' that identifies by listing, *inter alia*, ID numbers and location data. The definition in the Zimbabwean Bill is almost identical to that in the SADC Model Law.[185]

In both the EU Directive and the GDPR,[186] 'data subject' is defined in the definition of personal data,.[187] and is similar to the definition in the SADC Model Law. The European influence is thus clearly seen in the SADC Model Law's conception of a data subject.

(III) Processing

In the SADC Model Law, 'processing' is defined as a procedure through which data is used, either sorting, editing, compiling or erasing.[188] The definition of processing in POPI[189] and in the Mauritian Act[190] is similar to the definition in the SADC Model Law and the definition in the Zimbabwean Bill[191] is identical to the Model Law. One can find the same definition in the Directive[192] and the GDPR[193] and it is apparent that a relatively uniform definition exists across all the relevant laws.

(IV) Consent

It is necessary to consider the definition of 'consent' as it is the pre-requisite to any data processing. Without consent, there can be no legal data processing. In the Model Law, 'consent' refers to explicit consent by the data subject or their legal representation.[194] However, there is no reference to consent being unequivocal. 'Consent' in terms of POPI also refers to explicit consent yet it is

[183] Section 1.
[184] Section 1.
[185] Clause 3.
[186] Article 4 (1).
[187] Article 2 (a).
[188] Article 1 (15)
[189] Section 1.
[190] Section 2.
[191] Clause 3.
[192] Article 2 (e).
[193] Article 4 (2).
[194] Article 1 (2).

worded differently.[195] The Mauritian Act includes an additional requirement, namely that consent should be unambiguous.[196] The Zimbabwean draft Bill's definition is identical to the Model Law.[197]

In the Directive, explicit consent that is 'specific and informed' must be given by the data subject. The GDPR uses the same definition but the word 'unambiguous' is added, indicating a stricter approach than the Directive.[198] It would, thus, appear that the Mauritian Act draws on the GDPR in this instance.

The commonality in these definitions is the requirement for explicit consent by the data subject, setting a high standard for the conditions under which data can be used.

(V) Data processor and controller

In terms of the Model Law, 'Data Controller' is defined to include natural and juristic persons (whether private or public) that determine the purpose and procedure for the data processing a. It further provides that if data processing is done per each member state's legislation that the designated individual in the legislation is the Data Controller.[199] The data processor is defined to include natural and juristic persons (whether private or public) that are authorised and instructed to process the data on behalf of the Data Controller. In POPI, there are similar concepts, yet they are named the 'responsible party' (the Controller) and the 'operator' (the data processor).[200] There is, however, no reference to other legislation in POPI. The Mauritian Act defines 'Controller' and 'data processor' in a similar manner.[201]

Whilst the Zimbabwean draft Bill includes similar definitions, 'Data Controller' is defined with reference to the data authority. Data authority should be understood with reference to section 5 of

[195] Section 1
[196] Section 2.
[197] Clause 3.
[198] Article 4 (11).
[199] Article 1 (4).
[200] Section 1.
[201] Section 2.

the Postal and Telecommunications Act 4 of 2000. This provides that the data authority will be the Postal and Telecommunications Regulatory Authority Board, which is required to operate in accordance with the Act.[202]

The Directive's definition[203] of the Controller and data processor are almost identical to that in the Model Law and the GDPR.[204] The same concepts can thus be found in all the instruments considered albeit expressed in slightly different terms.

[202] Section 5.
[203] Article 2 (d) & (e).
[204] Article 4 (7) & (8).

3. COMPARATIVE STUDY OF LAWS IN SADC

(a) Introduction

This chapter will compare various data protection regimes in SADC to the Model Law. This serves to determine the extent of harmonisation of data protection laws between these states and the Model Law and the impact that the Model Law has had on these domestic laws. Before considering the provisions that each member state has in place, it is necessary to consider the context from which each legal regime arises.

The Model Law forms part of the HIPSSA.[205] The goal of the project is to promote and assist the development of ICT in each of the selected regions, to aid economic development and to ensure that local ICT standards are in line with global ICT standards.[206] The Model Law is one of many legal instruments that came from the HIPSSA project.[207]

The Model Law will first be compared to the South African data protection legislation, POPI,[208] as South Africa has the largest digital economy within SADC.[209] POPI is fully in force as of 1 July 2020.[210] POPI is the result of the *Privacy and Data Protection Discussion Paper* by the South African Law Reform Commission and is not a product of the Model Law.[211] The Commission considered two international instruments to be influential in the drafting process:[212] the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of

[205] International Telecommunications Union 'Support for the Establishment of Harmonized Policies for the ICT Market in the ACP States'https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx accessed 15 July 2020.
[206] Ibid.
[207] The SADC Model Law on e-transactions, SADC Model Law on cybercrime and the SADC guidelines are some SADC specific instruments that came about from the project; International Telecommunications Union 'Support for harmonization of the ICT Policies in Sub-Saharan Africa' available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx accessed 15 July 2020.
[208] Act 4 of 2013.
[209] United Nations Conference on Trade and Development *Digital Economy Report* (2019) at 75.
[210] Protection of Personal Information Act 'The Commencement Date of POPI' available at https://popia.co.za/ accessed on 22 July.
[211] South African Law Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).
[212] Ibid at V.

Personal Data[213] and the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[214]

The report considered cross-border information transfers and expressed the need for the South African data protection regime to comply with international standards.[215] The Commission also expressed that as 'the SADC region moves towards a trade bloc in 2008, South Africa's policies should be a guiding best practice for the region and capable of adaptation by our regional trading partners'.[216] Considering the Commission's report, it is interesting to note that the process surrounding the creation of a South African data protection regime stands somewhat in opposition to the Model Law. If POPI is described by its creators as a 'guiding best practice' there would appear to be an expectation that other states follow South Africa's regime rather than implementing SADC's Model Law. Nonetheless, one could argue that if the data protection regimes are compatible and they meet each other's adequacy standards then there has been harmonisation – not unification – in the region as all regimes are based on EU data protection laws.

Viewed in this light, it is also necessary to consider Mauritius' Data Protection Act ('the Act').[217] Mauritius is unique as it was one of the first SADC member states to implement a data protection regime. This regime was the Data Protection Act which was based primarily on the EU's Data Protection Directive.[218] The 2017 Mauritian Data Protection Act was adopted after changes were made to the European data protection regime with the implementation of the General Data Protection Regulation.[219] Over recent years, Mauritius' GDP has been increasing and a reason for this is growth in the ICT sector.[220] The sector is noted to have a 'strong enabling environment' by the African Development Bank.[221]

---

[213] ETS No. 108
[214] Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.
[215] Op cit South African Law Commission para 7.19
[216] Ibid.
[217] 20 of 2017.
[218] Satyanraj Ramdoo & Inza Dauharry 'Harmonising the GDPR in Mauritius' available at *https://www.africalegalnetwork.com/mauritius/news/harmonising-gdpr-mauritius/* accessed on 27 July 2020.
[219] Ibid.
[220] Ndoli Kalumiya 'Mauritius' in African Development Bank *2018 African Economic Outlook* (2018) at 2 – 3.
[221] Ibid at 9.

Lastly, the proposed data protection regime of Zimbabwe will be considered. Although the current Access to Information and Protection of Privacy Act provides regulation for public bodies and their use of personal data, this does not extend to private actors.[222] Perhaps because of this, Zimbabwe plans to introduce a new data protection regime through the Cyber Security and Data Protection Bill ('the Bill').[223] The Bill was drafted with assistance from the ITU through the HIPSSA project and the Bill should thus resemble the Model Law. However, several shortcomings in the Bill have already been highlighted.[224] In the law-making process there has been a lack of involvement of civil society and relevant stakeholders and the Data Protection Authority (established by the Bill) would be appointed by the executive branch,[225] which does not bode well for the independence of this body.[226] Additionally, regarding 'non-sensitive data' there are concerns that the term is too broadly worded with the implication being that explicit consent will not be required but can be implied by the data subject's conduct.[227] These shortcomings will be addressed in more detail in the comparative study below.

It is now necessary to consider the provisions of the Model Law and assess the extent to which they align with the selected domestic laws and to which they provide adequate protection to data subjects.

(b) Preamble, purpose and objective

(I) SADC Model Law

The Model Law's Preamble identifies key elements relating to the protection of data in SADC. It starts by noting that various international institutions and organisations recognise the protection of

[222] Op Cit Ncube 'Data Protection in Zimbabwe' at 106.
[223] H.B 18, 2019.
[224] Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe & International Human Rights Clinic at Harvard Law School et al *The Right to Privacy in Zimbabwe Stakeholder Report Universal Periodic Review 26th Session* (2016) at para 42; Additionally Privacy International has also criticised the Bill, Privacy International *Submission on the Cyber Security and Data Protection Bill 2019 to the Parliament of Zimbabwe* (202) available at https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf accessed 28 July 2020.
[225] Ibid.
[226] Ibid at 3.
[227] Ibid at 4.

data as a fundamental democratic value.[228] The rights of freedom of expression and freedom of association are specifically listed in the Preamble. This serves to address the possibility of any discrimination that may come from the processing of personal information, given that individuals' personal information could contain details about their political affiliations, race, gender or age.

The Preamble also highlights the content of the data protection principles derived from EU data protection law and the OECD Guidelines on Data Protection.[229] A principle that is explicitly mentioned in the Preamble is that of accountability.[230] This principle goes to the level of protection required for different types of data and rightly acknowledges that more sensitive data requires greater protection.

The Preamble further distinguishes between sensitive data and that which is not sensitive. Sensitive data refers to data which 'reveals a person's religious affiliation, ethnic origin and health' and can also include genetic information.[231] Sensitive data needs specific rules to ensure that this information is not unduly disclosed or leaked to the public. The Preamble also provides that individuals should have right of access to their personal information which results in a right of rectification and opposition.[232] There should be sanctions in place to render the law effective. The Model Law suggests sanctions ranging from an official warning[233] or notice of compliance,[234] failing which there may be fines[235] or a limitation of the processor's activities.[236]

There is explicit reference to globalisation and the impact of transnational data flows.[237] In this respect, the adequacy standard is relevant as states should only allow for a data transfer if the data

[228] Harmonization of ICT Policies in Sub-Saharan Africa *Data Protection: SADC Model Law* (2013), Preamble at 1.
[229] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108; Part 2, Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980; These principles include the Collection Limitation Principle, the Purpose Specification Principle, the Use Limitation Principle, the Openness Principle and the Data Quality Principle.
[230] Supra SADC Model Law, Preamble at 2.
[231] Ibid.
[232] Ibid.
[233] Article 9(1)(a).
[234] Article 9(1)(b).
[235] Article 9(2)(b).
[236] Article 9(2)(a)
[237] Model Law, Preamble at 2.

protection laws in the other state offer equivalent protection.[238] It is for this reason that the adoption of data protection laws at the regional level will be beneficial, as the object of the Model Law 'is to create a uniform system in a given area in order to create a safe environment for citizens'.[239]

The Preamble further provides that for a data protection regime to be successful, there must be a Protection Authority that ensures the enforcement of the law.[240] This Authority should be granted the power to interpret and provide clarification on certain provisions of the Model Law.

The Preamble concludes by stating that data protection regimes should be adapted to the specific circumstances in each 'region'.[241] It is likely that 'region' in this instance refers to each member state of SADC and not to the region of SADC itself. If the former were the case, then a model law would be an inappropriate legal mechanism to achieve the established goals due to the different socio-economic conditions found in each state. Thus, adopting a single uniform law in this instance could be ineffective, as the SADC Model Law could not be applied in the same way in each context. It is thus interesting to consider how the provisions of the Preamble find application in the selected member states' legislation.

(II) South Africa

The Preamble of POPI frames the Act in terms of Section 14 of the Constitution of the Republic of South Africa, 1996, which provides individuals with the right to privacy, including protection against the 'unlawful collection, retention, dissemination and use of personal information' and expressly stating that the State is required to promote this right.[242]

Like the SADC Model Law, the Preamble contains provisions outlining the importance of the protection of personal information with regards to human rights and democratic principles.[243] It

[238] Aysem Diker Vanberg & Maelya Maunick 'Data protection in the UK post-Brexit: the only certainty is uncertainty' 32 *International Review of Law, Computers & Technology* (2018) at 200.
[239] Ibid.
[240] Supra SADC Model Law, Preamble at 2.
[241] Ibid.
[242] Act 4 of 2013, Preamble.
[243] POPI Preamble, first and second sentence.

confirms the need to balance rights with the need for the free flow of information[244] and the harmonisation of laws.[245]

The main difference between POPI's preamble and that of the Model Law is that POPI seeks to give effect to the right to privacy which is guaranteed by South Africa's Constitution.[246] POPI's preamble is centered more narrowly around the right to privacy and how this right can attenuate data processing activities.

The Model Law considers a broader scope of rights which, in this context, will be infringed if the 'democratic value' of data protection is breached. The Model Law perceives data protection as an independent value whereas POPI considers data protection as an element of the right to privacy.

(III) Mauritius

Where the Model Law and POPI had substantial preambles, the Mauritian Data Protection Act's preamble is quite short in comparison, stating that its aim is:

> To provide for new legislation to strengthen the control and personal autonomy of data subjects over their personal data, in line with current relevant international standards, and for matters related thereto[247]

Although the goals of the different data protection regimes are similar, this is quite brief and captures the purpose of all data protection regimes rather than a regime specifically tailored to the Mauritian context.

There is, glaringly, no explicit reference to any rights which is significant as both the Model Law and POPI's preamble highlighted the importance of data protection in giving effect to various

[244] POPI preamble
[245] Third sentence, POPI preamble. See SADC Model Law Preamble at 2.
[246] Iain Currie & Johan de Waal *The Bill of Rights Handbook* 6ed (2016) at 303 – 304.
[247] Act 20 of 2017, Preamble.

human rights. However, certain rights can be implied as the data subject has control over their data.

(IV) Zimbabwe

In the Zimbabwean Bill, the Preamble provides that the proposed Act will provide data protection rules with respect to the rights enshrined in the Constitution of Zimbabwe[248] and it should create institutions that aim to ensure data protection and cyber security.[249] Further, it serves to 'create a technology driven business environment and encourage technological development.'[250] Lastly, the Preamble states the need to amend the existing criminal law to include cybercrime.[251]

The Bill's preamble is similar to both the Model Law and POPI, as it expressly refers to the protection of rights granted in the Zimbabwean Constitution. The inclusion of a clause stating the objective of the Bill shows the influence of POPI on Zimbabwe's drafting, as POPI contains such a provision. South Africa is one of Zimbabwe's largest trading partners and the South African data protection regime has influenced the content and structure of the Draft Bill.[252]

In comparing these preambles, the similarities and differences between the laws considered are already emerging. However, it is necessary to examine the specific provisions of the laws to determine the extent of harmonisation.

(c) Scope of application

The Model Law applies to any 'processing of personal data performed wholly or partly by automated means, and to the processing of personal data otherwise than by automated means which forms part of a filing system or is intended to form part of a filing system'.[253] Similar provisions can be found in POPI,[254] the Mauritian Act[255] and in the Zimbabwean Bill.[256]

[248] (No. 20) Act, 2013.
[249] Supra Zimbabwean Bill, Preamble.
[250] Ibid.
[251] Ibid.
[252] The explicit objective of the Bill is to stimulate confidence and trust in the ICT sector.
[253] Supra, Model Law Article 2(1).
[254] Supra POPI, Section 3(1)(a).
[255] Supra Mauritius Data Protection Act, Section 3(2).
[256] Supra Zimbabwean Bill, Clause 4(2)(a).

It applies both to data controllers that are established in the specific state and to those who are not permanently established in that state, but who conduct their processing operations in that state.[257] This only applies if the data is processed in the given state and not just transferred through the specific state.[258] Similarly, despite being worded differently, provisions defining the scope of to whom the law applies can be found in the other regimes.[259] The Model Law, the Mauritian Act and the Zimbabwean Bill all require the Data Controller to 'designate a representative' to defend against any legal actions taken against the Controller.[260]

Interestingly, POPI contains a provision that it will apply over other national laws setting conditions for processing, if these conditions are inconsistent with it. This will have a negative impact on harmonisation as South African law will always override a foreign law.[261] This is not stated in the other instruments, and it begs the question whether South Africa will ever be able to achieve uniformity in data protection.

Regarding the unique provisions of the Mauritian Law, the first provision regarding the application of the Act is that the State itself is bound by these provisions.[262] Yet, the Act does not apply is when information is exchanged between state actors and this information is 'need-to-know' [263] or if the processing is part of a 'purely personal or household activity'.[264] The exception concerning information that is 'need to know' is unique to the Mauritian Act. Regarding the Zimbabwean Bill, the proposed Act will also apply to instances where access to information is concerned, in addition to creating a broader data protection regime. The Bill applies to data processing. [265]

All the instruments thus seem to have a similar scope of application, although there are certain unique aspects.

[257] Supra Model Law Article 2.
[258] Article 2(2)(a).
[259] Supra POPI, Section 3(1)(b); Data Protection Act 4 of 2017 Section 3(5)(a) -(b); Clause 4(2)(b).
[260] Article 2(2)(b); Act 20 of 2017 Section 3(6); H.B 18, 2019 Clause 4(3).
[261] Supra POPI Section 3(2)(a).
[262] Section 3(1).
[263] Section 3(4)(a).
[264] Section 3(4)(b).
[265] Supra Zimbabwean Bill Clause 4(2)(a).

(d) Independent regulatory bodies

The Model Law provides for the establishment of a Data Protection Authority which is independent and performs an administrative function.[266] Part III also provides that the Authority is required to ensure that data Controllers comply with the Model Law and can investigate processing activities by demanding documentation.[267] It shall also provide its opinion on matters concerning the fundamental principles of data protections or on the Model Law or on statutes relating to the Model Law.[268] Powers uniquely granted by the Model Law are that the Authority may challenge legislative and administrative conduct and it may also pass resolutions relating to the model law.[269] The Authority may provide its opinion on data processing activities, be notified of such activities and may inform the judiciary of any offenses that it is aware of.[270] It can also create administrative sanctions,[271] an important regulatory function.

POPI also provides for the creation of an Information Regulator,[272] who has jurisdiction over the data processing activities in South Africa. This Regulator is required to act independently and in accordance with the Constitution[273] and the law.[274] Further, it will be held to account by the National Assembly.[275] The Information Regulator is granted a broad range of powers, duties, and functions, some of which are similar to the Model Law such as ensuring compliance and dealing with complaints relating to POPI.[276] It should determine the relevant codes of conduct that will guide individuals that wish to process information.[277] This should be distinguished from the Authority's power to pass resolutions in terms of the Model Law, showing its unique advisory role. It is required to 'provide education' on data processing, consult with parties interested in data

[266] Supra SADC Model Law Article 3. The Authority has 'oversight and control' over the Model Law and the rights of privacy relevant to the law (Art 3(1)) and the Authority shall consist of various actors from various spheres and provides for instances where substitutes on the Authority are required (Art 3(4) -(5)).
[267] Article 4.
[268] Article 4(1)(b)
[269] Article 4(1)(c) - (d).
[270] Article 5(1)(a) - (c).
[271] Article 5(2)
[272] Supra POPI Section 39.
[273] Section 39(b).
[274] Section 39(b) - (c).
[275] Section 39(d).
[276] Section 40(1)(b) & (d).
[277] Section 40(1)(f).

processing and ensure the facilitation of 'cross-border cooperation' along with other general responsibilities.[278]

In Mauritian law, the key institution established by the Mauritian Data Protection Act is the Data Protection Office which is required to act independently and impartially in terms of the Act.[279] The Data Protection Office is headed by the Data Protection Commissioner.[280] The Data Protection Commissioner is granted a similar set of powers and functions by the Act.[281] Unique to the Act is the requirement that the Commissioner must remain abreast with developments in data processing and it must consider unique risks posed by automated processing.[282] Another way in which the Mauritian Act stands out is that the Commissioner itself makes decisions, unlike in POPI or the Model Law where complaints are referred to the judiciary.[283] To date, the Commission has made 68 decisions regarding complaints relating to data protection.[284]

In Zimbabwe, the Bill provides for the existence of a Data Protection Authority. However, where the other regimes provided for the creation of a new and independent body, the existing Postal and Telecommunications Regulatory Authority will assume this role in Zimbabwe.[285] The functions of the Authority are like those of the bodies established above, as it is required to give effect to the Bill and ensure compliance with the legal regime.[286] However, it is not an independent body, which creates room for abuses of information gathered through data processing. This is markedly different to the general accepted practice in the other states, which is to have an independent body.

(e) Rules regulating the quality of data

Art. 11 of the Model Law provides the principles of data protection that the data Controller must adhere to. It requires that processing be done for a specific purpose in an adequate manner and that

[278] Section 40(1)(a), (c), (g) & (h).
[279] Supra Data Protection Act Section 4(2).
[280] Section (4)(3).
[281] Section 5.
[282] Section 5(h) - (i).
[283] Section 6(1)(b).
[284] Data Protection Office 'Decisions on' Compliance' http://dataprotection.govmu.org/English/Pages/Decisions-on-Complaints.aspx accessed 18 August 2020.
[285] Supra Zimbabwean Bill Clause 7.
[286] Clause 8

data collected should be kept up to date and kept only for long as is needed to achieve the stipulated purpose.[287]

The data controller is also required to adopt measures that will make data accessible 'regardless of the technology used', meaning that any updates must be taken into account when determining what measures must be used.[288] A similar provision is also seen in the Zimbabwean Bill.[289] It is a positive that the Model Law has acknowledged the development of ICT on the continent and plans for it. The Zimbabwean Bill's provisions are closely based on the Model Law in this instance.[290]

The Mauritian Act makes no explicit reference to the quality of data which is a principle that is found in both POPI and the Model Law. This is problematic as Mauritian processors are not obliged to ensure that the data, they have is accurate, which could lead to errors and the abuse of consumer information.

(f) General rules on the processing of personal data

(i) SADC Model Law

The general rules on the processing of data are different in each legal regime considered and are often found under different sections of the various laws. The Model Law provides for General Rules and the necessary, fair and lawful processing of data.[291] The rules ensure that a data Controller collects data for an explicit and legitimate purpose.[292] The Model Law, like the other regimes considered, draws a distinction between two different forms of data: Non-sensitive and sensitive data. The Model Law provides that consent can be withdrawn at any instance and no reasons for the withdrawal must be given and the withdrawal must be for free. [293] Art. 15(2)

[287] Supra Model Law Article 11(1)(a) - (c).
[288] Article 11(2)
[289] Supra Zimbabwean Bill Clause 9(2).
[290] Supra Model Law Article 9(1).
[291] Article 12
[292] Article 13(1).
[293] Article 15(1)(b).

provides a broad range of exceptions to the general rule in terms of which processing can occur without the data subject's consent, if it will be in the public interest, for example.[294]

(ii) South Africa

Chapter Three of POPI sets out the requirements that a processor must meet in order for the processing to be lawful, each of these requirements will be discussed to establish what POPI requires.[295] The accountability condition requires that the responsible party ensure compliance with the Act regarding the purpose of processing and processing itself.[296]

The processing limitation condition provides that processing should be done in a lawful and reasonable manner that will not infringe the data subject's privacy.[297] Generally, the consent of the data subject is required unless there is a law or legal obligation that states otherwise or if the processing will be in the interests of the public or a third party.[298] The responsible party bears the onus to show that the data subject consented.[299] The data subject has the right to withdraw their consent[300] and to object to the processing of their personal information.[301] Personal information shall be collected directly from the data subject,[302] unless it is an exceptional circumstance.

The purpose specification condition requires that there be a 'specific, explicitly defined and lawful purpose' for the collection of personal information[303] and steps must be taken to inform the data subject of this purpose.[304] Personal information cannot be kept longer than necessary to achieve

[294] Article 15(1)(a) - (k). Examples of where the processing is in the interests of the data subject are article 15(1)(b) where the processing is to protect the interests of the data subject or article 15(1)(i) where it is required to make a medical diagnosis. Regarding processing based on law employment law (article 15(1)(a)) and social security laws are listed (article 15(1)(d), *inter alia*.
[295] Accountability; processing limitation; purpose specification; further processing limitation; information quality; openness; security safeguards; and data subject participation.
[296] Supra POPI Section 8.
[297] Section 9(a) - (b)
[298] Section 11(a) - (f).
[299] Section 11(2)(a)
[300] Section 11(2)(b)
[301] Section 11(3)
[302] Section 12(1).
[303] Section 13(1).
[304] Section 13(2).

the purpose.[305] If the responsible party initiates any further processing of the personal information, this can only be done if the requirements of purpose specification are met.[306]

The information quality condition requires the responsible party to take the requisite steps to ensure the accuracy of the personal information collected and to update the information.[307] The condition of openness requires the responsible party to keep a record of the processing[308] and should take steps to inform the data subject of which information is collected, the purpose for which it will be used and any other relevant information. [309]

The security safeguard condition requires the responsible party is required to 'secure the integrity and confidentiality of personal information' that it has collected.[310] The responsible party must take measures to prevent any harm by assessing risks and keeping safeguards up to date.[311] When doing so, the responsible party must be cognisant of accepted practices surrounding data protection.[312] The responsible party must contract with the operator to ensure the operator's compliance with the relevant security safeguards.[313]

Both the information regulator and the data subject should be notified as soon as reasonably possible of any breach.[314] The data subject is also granted a right to request and change any information the responsible party may have on them.[315]

POPI also addresses the processing of sensitive personal information with the processing of this type of information prohibited.[316] POPI sets out separate standards in this instance due to the

[305] Section 14.
[306] Section 15(1).
[307] Section 16(1).
[308] Section 17.
[309] Section 18(1)(a)
[310] Section 19(1).
[311] Section 19(1)(a) - (d).
[312] Section 19(3).
[313] Section 21(1)
[314] Section 22(1)(a) - (b).
[315] Section 23 – 24.
[316] Section 26. Special personal information is private information concerning the data subject's beliefs, racial profile, trade union member, political affiliation, health information and biometric information and information relating to accused criminal conduct of the data subject.

sensitive nature of the data in question. For example, processing is only allowed if the data subject has consented, or the processing is required in terms of a legal obligation or if there is compliance with the other rules of Part B.[317] Lastly, the exceptions in these circumstances are limited due to the sensitive nature of the data.[318]

One can clearly see the difference between the Model Law's general rules and the conditions for lawful processing set out in POPI. The conditions established by POPI are far broader providing more certainty for processors that need to comply with the conditions for processing, yet the Model Law deals with the same aspects in different parts of the instrument.

(iii) Mauritius

The Mauritian Act does not specify general rules for data processing. Instead, it focuses on the obligations that are to be placed on data Controllers and processors, the rights of the data subject and the instances in which an assessment must be done in order to determine the risk to data subjects through processing activities.[319] This leaves a gap in the law, and the Model Law could be used to provide guidance for future development.

(iv) Zimbabwe

Part V of the Draft Bill outlines the general rules applicable to data processing. Like the SADC Model Law and POPI, the Controller is required to ensure the necessity, lawfulness and fairness of the data processing.[320] Similarly, when data is collected for processing, it must be done for a 'specified, explicit and legitimate purpose' and relevant considerations, such as the data subject's reasonable expectation and the relevant legal provisions, should be considered.[321]

[317] S27(1).
[318] Section 36.
[319] Supra Data Protection Act Part IV – VI.
[320] Supra Zimbabwean Bill Clause 10.
[321] Clause 11(1).

Again, a distinction is drawn between sensitive and non-sensitive data. Sensitive data can only be processed if the data subject has consent.[322] Interestingly, for non-sensitive data, the consent of a data subject, if the data subject has full legal capacity, may be inferred.[323] Furthermore, these are instances where the consent of the data subject is not required such as where it will be used to prove an offence[324] or if the Controller is processing data in order to comply with an obligation imposed upon it by a law.[325]

The rules for sensitive information are far stricter and written consent may be required.[326] The data subject is also permitted to withdraw their consent.[327] In addition there are exceptions to this rule which are almost identical to those contained in the Model Law.[328]

However, a significant difference can be seen between Article 15*(2)(d)* of the Model Law and Clause 13*(2)(d)* of the Zimbabwean Bill. The Model Law provides an exception to the processing of sensitive information, if 'the processing is necessary to comply with social security laws.'[329] The provision reads the same as that in the Bill, but instead of allowing compliance with social security laws, it is for compliance with *national* security laws. The difference is significant and echoes, to a certain extent, the concerns raised above.[330]

(g) Duties of the Data Controller and Processor

(I) SADC Model Law

The duties of the Data Controller and processor are set out in Part VI of the Model Law. Like the openness condition in POPI, Art. 21 of the Model Law provides that the data subject should be informed of which data is collected and for which purpose.[331] The Controller should consider the

[322] Clause 12(1).
[323] Clause 12(2).
[324] Clause 12(3)(a).
[325] Clause 12(3)(b).
[326] Clause 13(1)(a).
[327] Clause 13(1)(b).
[328] Clause 13(2)(a) - (b).
[329] Article 15(2)(d).
[330] Op Cit *Zimbabwean Stakeholder's Report.*
[331] Article 21(1)(a)-(c).

circumstances surrounding the collection and provide information to the data subject to ensure that the processing is fair.[332] If the data is not collected by the Controller themselves, the same rules apply.[333]

Art. 24(1) establishes the requirement for ensuring that the data collected remains secure. This places an obligation on the Controller to ensure that the data collected is not negligently destroyed, lost, unlawfully processed, altered or accessed.[334] If the Controller appoints a data processor this must be done in terms of a legal instrument setting out the Controller's instructions and the controller must meet the standards established in art 24(1).[335] If the data processor experiences a data breach, it should inform the Data Controller of this breach and the Controller must then inform the Authority.[336]

There is an obligation on the Controller to notify the Authority of any processing. The Authority has the power to exempt certain categories from notification and designate categories of processing which require authorisation if they may impact the data subject's fundamental rights.[337] Art. 29 addresses processing and openness, stating that the Authority will have a register that is accessible to the public listing all processing operations.[338] It is explicitly stated that the Controller should be accountable to the principles established by the Model Law.[339] Additionally, the Controller must 'have the necessary internal mechanisms' that illustrate compliance with the principles established.[340]

(II) Mauritius

To be a data processor or Controller in Mauritius, registration with the Commissioner is a requirement.[341] Such registration can only take place once the individual provides certain

[332] Article 21(1)(e).
[333] Article 22.
[334] Article 24(1)(a)
[335] Article 23
[336] Article 24(2)
[337] Article 26(3) & Article 28.
[338] Article 29(1) - (2).
[339] Article 30(1)(a)
[340] Article 30(1)(b)
[341] Supra Data Protection Act Section 14.

information to the Commissioner, after which a registration certificate will be issued.[342] Data processing must be lawful, fair and transparent; it should be done for an explicit and limited purpose and kept for the duration of achieving that purpose; it should be accurate, and processing should respect the data subject's rights.[343] The Controller must also fulfil duties pertaining to the creation of policies and mechanisms illustrating compliance with the Act.[344] The Controller also bears the onus of showing the data subject's consent.[345] If there is any data breach, the Controller is required to inform the Commissioner and the data subject.[346] The Act also creates special categories of personal data for more sensitive information.[347] The Controller must ensure that there is adequate security surrounding the processing operation.[348] This includes preparing for any significant risks by means of an impact assessment.[349] The Act provides a list of processing operations likely to present a risk.[350]

(III) Zimbabwe

Part VI of the Draft Bill outlines the proposed duties of the data Controller and processor. If a Controller is collecting data directly or indirectly from the data subject, they are required to disclose certain information.[351] A data processor may only conduct processing operations if they have been granted the Authority to do so by a data Controller.[352] The Controller is, further, required to take appropriate steps to protect the data which they have collected.[353] The extent of the measures adopted should balance the costs of implementing the safeguards and the risk to the data

[342] Section 15(2)(a) -(h) & section 16.
[343] Article 21(a) - (f).
[344] Section 22. The mechanisms required are, *inter alia*, maintaining sufficient security measures and retaining a data processing record.
[345] Section 24(1).
[346] Section 25 - 26.
[347] Section 29(1)(d).
[348] Section 31.
[349] Section 34(1).
[350] Section 34(2)(a) - (c).
[351] Supra Zimbabwean Bill Clause 15(1) & 16(1).
[352] Clause 17.
[353] Clause 18(1).

subject's data.[354] If the Controller appoints a processor, this should be done using a legal instrument[355] ensuring that the processor makes sufficient guarantees to protect the data.[356]

If there is a security breach, the Controller is required to notify the Authority.[357] Significantly, there is no obligation to inform the data subject, yet this obligation exists in all the other laws considered. The Bill sets out other functions of the Authority such as establishing special categories of processing requiring consent, similar to the Model Law. The Authority is required to keep a register that details automated processing activities which should be accessible to the public.[358] The final duty of the Controller is that of accountability which requires compliance with the Bill and to have 'internal mechanisms' illustrating this.[359]

These provisions have been influenced by the SADC Model Law and provide comprehensive regulation of the data Controllers. This is a positive sign that the Model Law can be incorporated into member states' legislation successfully.

(IV) South Africa

There is no separate chapter placing obligations on the responsible party, as can be seen in the other jurisdictions discussed above. These obligations can, instead, be found in the conditions for lawful processing provided for under the general rules.

(h) Rights granted to the data subject

Part VII of the Model Law establishes the rights of the data subject, including the right of access, the right of rectification, deletion and temporary limitation of access and the right of objection. The right of access provides that a data subject, upon proof of their identity, has a right to the information concerning themselves.[360]

[354] Clause 17(2).
[355] Clause 18(5).
[356] Clause 18(4).
[357] Clause 19.
[358] Clause 23(1) - (3).
[359] Clause 24(1)(a) - (b).
[360] Supra Model Law Article 31(1)(a) - (d).

The right of rectification, deletion and temporary limitation of access allows the data subject to change, erase or limit the access of the Data Controller to their personal data if the personal data is inaccurate.[361]

The right of objection allows the data subject to object to the processing of any of their data.[362]
In terms of the South African data protection regime, the data subject is granted numerous rights by POPI. Data subjects have a right to have their information processed lawfully in terms of the conditions for lawful processing established in Chapter 3.[363] This includes the right to be notified that their personal information is being collected or has been accessed by an unauthorised individual.[364] The data subject can further request whether a responsible party has any of their personal information[365] and to request that this information be destroyed or corrected.[366] The data subject also has the right to object to the processing of their personal information,[367] including the collection of information for direct marketing.[368] The data subject can also request not to be subject to the automated processing of their information.[369] Lastly, the data subject can complain to the Regulator[370] and may initiate proceedings against individuals that interfered with their personal information.[371]

In Mauritius, the first right granted to data subjects in terms of the Act is the right of access.[372] If personal data is being processed, the Act sets out a list of which information the Controller should make available to the data subject in plain language.[373] The data subject also has a right to not be subject to automated processing[374] and a right to rectification.[375] The Controller is required to destroy any personal data if the purpose for processing has been achieved, if the data subject has

[361] Article 32
[362] Article 33.
[363] Supra POPI Section 5(1).
[364] Section 5(1)(a) - (b).
[365] Section 5(1)(b).
[366] Section 5(1)(c).
[367] Section 5(1)(d).
[368] Section 5(1)(e)-(f).
[369] Section 5(1)(g).
[370] Section 5(1)(g).
[371] Section 5(1)(i)
[372] Supra Data Protection Act Section 37.
[373] Section 37(2) - (3).
[374] Section 38(1).
[375] Section 39(1).

withdrawn consent or objects to the processing or if the processing is unlawful.[376] The data subject may also object to the processing of their personal data, including processing relating to direct marketing.[377]

In contrast to the number of rights conferred by the different regimes considered, the Zimbabwean Draft Bill provides the data subject with a single explicit right: the right to 'not be subject to a decision based solely on automated processing' that may result in legal consequences for them.[378] This does not apply where the data subject has provided their consent or if the processing is permitted by law.[379] There is a clear difference between the Bill and the other data protection regimes which provide data subjects with several explicit rights. This raises the question of whether the soft-law status of the Model Law limits its ability to provide substantial protection to data subjects.

(i) Requirements for transnational data transfer

Part XI of the Model Law contains the requirements for data transfer. A distinction is drawn between transborder flows of data to member states and non-member states.[380] If the transfer is to a member state that has adopted the Model Law, the recipient will be required to show that such transfer is in the public interest or that it will not prejudice the data subject's interests.[381]

Art. 44(1)(a) establishes an adequacy standard when transferring data to a non-member state. The main factor considered is 'adequacy of the level of protection' which is determined by assessing the context in which the transfer will take place, the type of data to be transferred, the purpose for which it is transferred and the rules regulating data protection in the recipient state.[382] The

[376] Section 39(2)(a) - (d).
[377] Section 40.
[378] Supra Zimbabwean Bill Clause 25(1).
[379] Clause 25(2).
[380] Supra Model Law Article 43 – 44.
[381] Article 43(1)(a) - (b).
[382] Article 44(1)(b)

Authority can establish categories of data which may not be transferred.[383] There are also exceptions where a data transfer can occur despite a lack of adequate protection.[384]

In South Africa, the rules relating to data transfer are contained in s72 of POPI. The provision is worded in the negative, stating that responsible parties may not initiate a data transfer unless certain conditions are met.[385] The requirements in this instance are conjunctive and are that: the party which will receive the data should be bound by 'law, binding corporate rules or [a] binding agreement' that ensures 'an adequate level of protection'.[386] The adequate level of protection should be 'substantially similar to the conditions for the lawful processing of personal information' including a provision regulating data transfers;[387] and the consent of the data subject will also be required.[388] The transfer should have a legal basis or be 'for the benefit of the data subject.'[389]

The requirements in Mauritian law are comparable to those found in both POPI and the Model Law. The Commissioner must be shown that safeguards protecting data exist and that the data subject has been made aware of the implications of the transfer and has consented and the transfer should be necessary.[390] Only the data relevant to the purpose will be transferred.[391] Lastly, the Commission can require a Controller or processor conducting a data transfer to show that the safeguards in place are effective, if they are not, the Commissioner can 'prohibit, suspend or subject the transfer to such conditions as he may determine'.[392]

In Zimbabwe, the data transfer provision establishes an adequacy standard.[393] These provisions are largely based on the provisions in the Model Law concerning data transfer to states outside of SADC.

[383] Article 44(2).
[384] Article 45.
[385] Supra POPI Section 72(1).
[386] Section 72(1)(a).
[387] Section 72(1)(a).
[388] Section 72(1)(b)
[389] Section 72(1)(
[390] Supra Data Protection Act Section 36(1)(a) - (c).
[391] Section 36(2).
[392] Section 36(4).
[393] Supra Zimbabwean Bill Clause 28.

(h) Concluding remarks

From the above, we see that the selected legal regimes are similar in their scope of application. Significant differences can mainly be seen in structure rather than substance. Another area of variation is the extent of the role which is played by the (independent) body required to regulate data processors in a specific jurisdiction. Broadly speaking, apart from Zimbabwe, data subjects are granted rights that they can exercise to retain their digital autonomy.

However, it should be noted that the similarities are not the result of the Model Law or the HIPSSA project. Mauritius and South Africa both implemented their data protection regimes independently of the Model Law and seem to have covered the same ground in their instruments. The Zimbabwean Bill still has serious shortcomings regarding the independence of the Authority and the lack of rights granted to data subjects. In this instance, the Bill differs the most from the Model Law with the lack of substantive protection provided to data subjects being a glaring shortcoming.

This notwithstanding, it can still be said that the regimes are harmonised to a certain extent. This is due to the standard established by the EU which most states seek to comply with. It is thus necessary to consider the two principal instruments in the EU, the Data Protection Directive and the GDPR to determine why they have had such an influence on data protection regimes in SADC.

4. DATA PROTECTION IN THE EU

(a) Relevance of the European Regime to SADC

The EU data protection regime is considered to be the most influential in the world,[394] Arguably because of the market power exerted by Europe globally in the sphere of data protection.[395] The result of this is that laws made unilaterally by the EU have an extra-territorial effect. Bradford refers to this as the so-called 'Brussels Effect' whereby the EU has the 'unilateral power to regulate global markets.[396] This extends beyond the sphere of data protection to other significant regulatory regimes such as competition law.[397] This results in the externalisation of European laws in other states, creating and setting a global standard.[398]

(b) The development of data protection in the EU and fundamental principles of EU law.

During the 1970s and 80s data flows were of little significance, primarily being part of the internal workings of a company. Since then, ICT has developed to such an extent that individuals are exposed to data transfers in their everyday lives, which has had an adverse impact on their privacy.[399]

It became apparent that national rules alone would not suffice and that international regulation of data protection would be required.[400] The two sets of international rules introduced in the 1980s were the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[401] However, the Guidelines lacked legal force as the rules it contained

[394] Paul M Schwartz 'Global Data Privacy: The EU Way' (2019) 94 *New York University Law Review* at 772 – 773.
[395] Ibid.
[396] Anu Bradford 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* at 3.
[397] Ibid.
[398] Ibid.
[399] Ibid.
[400] Peter Blume 'An EEC Policy for Data Protection' (1992) 11 *Computer/Law Journal* at 403.
[401] Part 2, Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980; No. 108/1981.

could be varied by the states implementing them. The Convention also allowed states to vary its provisions but was not broadly ratified.[402]

The EC started considering the issue of more comprehensive data protection rules in 1990, with proposals on the directive being submitted in 1991 and 1992.[403] This coincides with the signing of the Maastricht Treaty or the Treaty on the EU.[404] Finally, in 1995 the Data Protection Directive was introduced. Along with the aim of providing adequate rules on transborder flows of data, the Directive also sought to harmonise data protection rules within the EU.[405] Harmonisation played a key role in achieving the aims established by the Directive.[406]Each state in the EU must thus adopt the same rules but the form of the rules can differ.[407] A unique aspect of the Directive is its 'long arm application', [408] as it provides that the Directive will apply to non-EU processors who are processing the data of EU citizens.[409] This has been criticised as regulatory overreach as the Directive forces compliance with the regime outside of the EU. However, there is no way to enforce this, which leaves the provision somewhat toothless.[410]

The Directive was considered a pioneer in the sphere of data protection when it was introduced in 1992. However, after nearly twenty years it was considered outdated and in 2012, the EC started working on its proposal for the GDPR.[411] The GDPR came into force in 2016 and was a response to an increase in the amount of processing due to increased ICT capabilities. It increased the level of privacy provided to individuals and it further harmonised data protection rules within the EU.[412]

---

[402] Fred H. Cate 'The EU Data Protection Directive, Information Privacy, and the Public Interest' (1994) 80 *Iowa Law Review* at 431.
[403] Thomas Hoeren 'Proposal for a Council Directive on Data Protection and Its Impact on German Industry' (1993) 1 *International Journal of Law and Information Technology* at 133.
[404] 11992M/TXT.
[405] David Bainbridge 'Processing Personal Data and the Data Protection Directive' (1997) 6 *Information & Communications Technology Law* at 18.
[406] Ibid; This is as the Directive serves to protect the right to privacy (considering data processing) and to reduce barriers to the flow of personal information within the EU.
[407] Ibid.
[408] Lokke Moerel 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 *International Data Privacy Laws* 28 – 29.
[409] Ibid.
[410] Ibid.
[411] Foivi Mouzakiti 'Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive' (2015) 1 *European Data Protection Law Review* at 39.
[412] Paul Voight & Axel von dem Bussche *The EU General Data Protection Regulation (GDPR): A Practical Guide* (2017) at 1.

It is important to consider both the GDPR and the Data Protection Directive as the latter is one of the most influential pieces of data protection legislation, having influenced many of the current data protection regimes in existence today.[413] One of these regimes is the SADC Model Law, which was introduced prior to the existence of the GDPR and is thus based on the provisions of the Directive. The Model Law bears resemblance to the other implemented data protection regimes in SADC and it is thus clear that the EU provisions have directly affected the development of data protection laws in Southern Africa.[414] Given this influence, it will be instructive to consider the provisions of the Directive and assess its impact in the SADC region.

(c) Preamble and purpose.

The Preamble of the Directive consists of more than 70 recitals outlining a broad purpose. It states that the Directive serves to forward the objectives of the EU by removing barriers, strengthening the unification project and assisting the functioning of the internal market by making the exchange of information easier.[415]The Directive should also provide for the protection of rights of individuals in the union, specifically the right to privacy.[416] It also introduces the principles of protection, imposing obligations on Data Controllers and processors and granting rights to data subjects.[417]

The processing of data is required to be lawful.[418] Consent is highlighted as an important component of the Directive and processing can only be conducted without consent if it is done to 'protect an interest which is essential for the data subject's life'.[419] Member states are allowed to process the data if it is in the public interest but must adopt safeguards to protect the privacy of the data subjects.[420]

[413] Op cit Birnhack at 512.
[414] Chapter 3
[415] Supra, Directive Preamble recital (1), (3), (4) & (5).
[416] Recital (10) – (11).
[417] Recital (25).
[418] Recital (28).
[419] Recital (30) – (31).
[420] Recital (34).

For data subjects to have a form of recourse, member states should grant the data subject a judicial remedy in the event that a Controller infringes the rights of the data subject.[421]

The Preamble also contains recitals pertaining to instances where third countries do not provide the same level of protection as in the EU. In terms of these, transfers to third countries can only be made if they meet the standards set out in the Directive. The Commission also has certain powers when determining the standard that third countries should comply with.[422]

By contrast, the GDPR's preamble has more than 170 recitals. The Regulation makes specific reference to relevant provisions of the Charter of Fundamental Rights of the EU and to the Treaty on the Functioning of the EU ('CFR').[423] It is recognised that there has been an increase in the amount of data that is transferred within the EU and globally.[424] It refers to the Directive and the fact that it has failed to prevent the fragmentation of laws, legal uncertainty and to raise awareness concerning the necessity of data protection.[425] Explicit reference is made to the 'existence of differences in the implementation and application of Directive 95/46/EC'.

Another crucial norm that has been introduced in the GDPR is that of 'technology neutrality',[426] which means that the GDPR should apply regardless of whether the data is processed by automated or manual means.[427] Further, it incentivises the 'pseudonymisation' of personal data, referring to the fact that data should not be attached to a specific data subject.[428] It also contains references to consent, obligations on the Controller and processor, the rights of the data subject and the exceptions to consent.[429] Crucially, the GDPR serves to give the data subject control over their data.[430] Further, there is a broader explanation of how the EU should consider data transfers to

[421] Recital (54).
[422] Recital (56), (57), (58), (59), (60) & (66).
[423] Recital (1).
[424] Recital (4) – (5).
[425] Supra, GDPR Recital (9).
[426] Recital (15).
[427] Ibid.
[428] Recital (28) – (29).
[429] Recital (42) – (64).
[430] Recital (68).

third countries, addressing some shortcomings in the Directive.[431] In doing so, a number of duties are placed upon the Commission.[432]

The Model Law's preamble is notably less detailed than that of both the Directive and the GDPR. Where the two latter instruments provide significant detail on the content of the laws, the Model Law's preamble only provides general context to the need for data protection in SADC and the importance of data protection regarding human rights.[433] Reference is made to the overarching need for the harmonisation of laws in the AU. The Model Law's preamble also refers to the need to consider existing legal frameworks, yet it does not detail exactly how the Model Law should interact with these other laws.[434] Rather, it provides that these tools should be 'good examples of present initiatives'.[435] This is problematic as the texts that the preamble refer to are Conventions and multilateral instruments which are legally binding while the Model Law is not. The Model Law only provides an example for states to base their data protection regimes on but does not force states to adopt it. Thus, there may be deviations in implementation, frustrating the goal of harmonization that the Model Law mentions.

(d) Scope of application

The Directive applies to the processing of data via automated, partially automated or non-automated systems, with the exception of activities relating to public security and the like.[436] The member states are deemed to have the ability to regulate the areas of 'public security, economic or financial interests and crime prevention'.[437]

As the Directive is a regional instrument there are provisions regarding the applicable national law. In this regard, the national provisions that a member state has adopted will apply if the processing is done 'in the context of the activities of an establishment of the Controller on the

[431] Recital (104).
[432] Recital (105) – (109).
[433] Supra, SADC Model Law Preamble at 1 – 2.
[434] Ibid.
[435] Ibid.
[436] Supra, Directive Article 3(1) – 3(2).
[437] Recital (43).

territory of the member state'.[438] The processing can therefore occur both inside and outside the EU and it will be covered by the Directive if it is related to the activities of an establishment in the EU.[439] The location of the processing is not important, but a territorial link is still established to the EU by virtue of the processing occurring in the activities of an establishment within the EU or by virtue of the processing equipment being located there.[440]

The scope of the GDPR is separated into the Material scope and the Territorial scope.[441] The material scope reflects the Directive in that it covers both automated and non-automated processing.[442] However, the GDPR excludes extra categories of data that fall outside of its scope.[443] This could be because the GDPR is a regulation and it must be incorporated into member state law as is, thus, greater exclusions are required to allow states to retain their regulatory power in certain areas.

The most significant difference is found in the provisions relating to the territorial scope. First, data processing of an establishment in the EU falls within the scope of the GDPR where processing occurs inside and outside the EU.[444] The GDPR also applies to the processing of personal data of data subjects in the EU by Controllers and processors outside of the EU if the processing is related to the provision of goods or services or if it monitors their behaviour.[445] These provisions provide for the extraterritorial application of the GDPR which confirms the principle of extra-territoriality in terms of the Directive.[446]

The SADC Model Law's material scope is the same as both the Directive and the GDPR. The Model Law refers to processing 'in the context of the effective and actual activities of any Controller permanently established' in the relevant territory,[447] which is more in line with the

[438] Article 4(1)(a)
[439] Op cit Moerel at 29.
[440] Op cit Moerel at 32.
[441] Supra, GDPR Article 2 – 3.
[442] Article 2(1).
[443] Article 2(2) – (4); *Inter alia,* these refer to household conduct or certain conduct on the part of member states
[444] Article 3(1).
[445] Article 3(2).
[446] Cedric Ryngaert & Mistale Taylor 'The GDPR as Global Data Protection Regulation?' (2020) 114 *AJIL Unbound* 6.
[447] Supra, Model Law Article 2(2)(a).

GDPR and current standards as it covers processing activities within the territory. Thus, despite being based on the Directive, the Model Law is up to date with modern standards in this respect.

However, in terms of these rules there can be no extra-territorial scope as foreign Controllers' activities only fall within the scope of the Model Law if they use processing equipment within the relevant territory.[448] This is problematic as foreign Controllers could process the data of SADC citizens without having to comply with the regime, leaving a gap in protection. This could be remedied by introducing a provision that specifically covers SADC citizens such as Art. 3(2) of the GDPR, but this may bring about issues of extra-territorial enforcement.

(e) Rules relating to the lawful processing of data

The Directive also outlines the conditions for the lawful processing of data,[449] known as the principles of data quality.[450] It sets out the criteria that must be met for data processing to be legitimate[451] and also creates a category for special data.[452] The processing of this type of data is prohibited and the Directive creates exceptions in terms of which it can be processed.[453] Significantly, the Directive gives member states the ability to determine their own exemptions relating to the public interest but there must be 'suitable safeguards' in place allowing the member states a certain degree of flexibility to pursue their own national policies.[454]
The GDPR also lists the principles of data processing and the conditions in terms of which processing will be lawful.[455] These are very similar to the Directive, including a category for special data.[456] Interestingly, the Directive contains a separate category for data relating to criminal

[448] Ibid.
[449] Supra, Directive Article 5.
[450] Ibid. These principles reflect the OECD *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980; Collection Limitation Principle, purpose specification principle, use limitation principle, openness principles and data quality principle.
[451] Supra, Directive Article 7(a) – (b). For example, the data subject must consent to the processing.
[452] Special data is defined in Article 8 as data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'.
[453] Article 8(1) – 8(2).
[454] Recital (34).
[455] Supra, GDPR Article 5 - 6.
[456] Article 9.

convictions.[457] This is because special authorisation is required to process this type of data,[458] indicating a need for further confidentiality.

The GDPR also sets out specific conditions for consent, increasing the threshold for valid consent in terms of the European data protection regime.[459] In setting out a more detailed standard for consent, the threshold which Controllers and processors must meet in order to process data was raised. This further solidifies consent as the primary condition for data processing.

The SADC Model Law contains the same principles as the European Regime; however, these principles are divided between provisions relating to the quality of data and the general rules of processing.[460] The Model Law also places an obligation on Data Controllers to ensure that the data should remain accessible even with technological advances.[461] This confirms that the instrument aims to aid future development and is forward looking.

(f) Data Subject

The Directive provides that member states must enact legislation requiring the data Controller (or their representative) to provide the data subject with certain information.[462] The identity of the Controller, the purpose of the processing and other information relating to who will be privy to the data and the data subjects' rights must be disclosed.[463] This places the data subject in a better position to make an informed decision regarding their personal information. This disclosure must occur at the time of data collection.[464]

The Directive also grants the data subject a right of access.[465] Part of this right entitles the data subject to require the 'rectification erasure or blocking' of processing if there is non-compliance

[457] Article 10.
[458] Ibid.
[459] Article 7.
[460] Supra, Model Law Article 11 – 13; Only the purpose specification principle, the data quality principle and the use limitation principle are explicitly set out.
[461] Article 11(2).
[462] Supra, Directive Article 10.
[463] Ibid.
[464] Article 11(1).
[465] Article 12(a).

with the Directive.[466] It is a contravention of the Directive to have incomplete or inaccurate data and this extends to any third parties that may process data on behalf of the Controller.[467]

The data subject also has a right to object to the processing of their data in instances where processing is done in the public interest or in the legitimate interests of the Controller or a third party.[468] The use of the words 'at least' indicates that these are minimum standards and that the relevant member state could set higher standards for when a data subject may object. The right to object also exists in instances where it is anticipated that the Controller will use the data for direct marketing.[469]

The data subject also has the right not to be subjected to the automated processing of decisions 'intended to evaluate' their conduct.[470] This is permitted if it is required for the performance of a contract to which the data subject has consented and there are sufficient safeguards to protect their interests or if it is permitted by law.[471]

The GDPR goes further than the Directive, including an entire chapter dedicated to the rights of the data subject. The data subject has the same rights as under the Directive with the addition of an obligation on the Controller to take steps to inform the data subject of their rights in a transparent manner.[472] The GDPR also includes the right to data portability. This right entitles the data subject to receive the data concerning them in an accessible manner and includes the right to give this data to another Controller.[473] This gives content to the right of access and allows the data subject to control their own personal data. In terms of the Directive, the data subject could only obtain access to categories of data relating to them and the communication of 'an intelligible form of data' being processed,[474]creating a more limited right. Unfortunately, the Model Law closely follows the Directive in this instance and does not include the additional rights found in the GDPR. As the

[466] Article 12(b).
[467] Article 12(b) – (c).
[468] Article 14(a).
[469] Article 14(b).
[470] Article 15(1).
[471] Article 15(2)(a) & (b).
[472] Supra, GDPR Article 12.
[473] Article 20(1).
[474] Supra, Directive, Article 12(a).

Directive does not provide the same extent of protection as the GDPR does, the level of protection in SADC is not as comprehensive as it can be, meaning that the Model Law is already out of step with the protections offered in Europe. A regime based on the Directive will clearly not meet the level of protection required by the GDPR, placing a greater burden on Controllers and processors to meet the level of protection required in terms of the GDPR due to a lack of protection afforded in legislation at the national level.

(g) Controller and processor

The Directive does not have a specific section dedicated to the Controller and the processor, as the obligations on these actors are found in other parts of the instrument. There are some provisions that deal directly with the Controller, namely those concerning confidentiality, security and the notification of processing activities.[475] The security requirement states that the Controller should take measures to prevent any unwarranted disclosure or destruction of the data[476] and must choose a processor that can guarantee a certain level of security.[477] There must be a defined legal relationship between the Controller and the processor, and the processor must follow the instructions of the Controller.[478]

The obligation of notification requires a Controller or their representative to inform the relevant supervising Authority prior to any partly or fully automated processing operations.[479] A great degree of discretion is granted to the member states in this instance. Member states may permit the simplification or exemption of notification in certain circumstances.[480] This may lead to uncertainty, for Controllers operating throughout the entire continent.

The GDPR, contrary to the Directive, contains a range of provisions relating directly to the Controller and the processor.[481] The Controller must take into account any risks associated with processing and weighing the severity considering the 'rights and freedoms' of natural persons.[482]

[475] Supra, Directive Article 16 – 18.
[476] Article 17(1).
[477] Article 17(2).
[478] Article 17(3).
[479] Article 18(1).
[480] Article 18(2) – (4).
[481] Supra, GDPR Chapter 4.
[482] Article 24(1)

To achieve this, the controller must conduct a risk assessment considering a number of factors.[483] If the risk assessment shows that there is a high risk, then the Controller must consult with the supervisory Authority[484] and take measures mitigating these risks.[485] The Controller is also required to implement a data protection policy and must comply with codes of conduct set out in Article 40.[486]

The GDPR also sets out provisions specifically relating to the legal relationship between the Controller and the processor.[487] For example, it provides that the processor's activities are limited by the instruction given by the Controller[488] and that the processor is bound by the relevant code of conduct.[489] This includes the same obligations as under the Directive and other obligations relating to the notification of processing and maintaining a processing record.[490] More detail is provided about the duties of the Controllers and processors, allowing for better co-operation and furthering the goals of harmonisation, which the Directive did not always succeed in doing.

The Model Law follows the Directive to a great extent but provides for the duties of the processor and the Controller in a manner similar to that seen in the GDPR.[491] This could be due to the fact that the Model Law was introduced in 2013, only a few years before the GDPR, and data protection norms had already changed a lot from when the Directive was introduced in 1992. The Model Law also includes the requirement of openness which reflects the need to comply with the Model Law and establish internal mechanisms ensuring compliance.[492] This bears resemblance to the accountability principle found in the GDPR and is an encouraging sign that the Model Law is not completely out of sync with international norms.

[483] Article 35.
[484] Article 36.
[485] Ibid.
[486] Article 24(2) – (3); The same obligations are found in the GDPR in Article 23 along with the requirement that the any individual processing must have the authority to do so.
[487] Article 28(1) – (3); The processor can only act on the mandate of the controller and there must be a contractual relationship between the two actors.
[488] Article 29.
[489] Article 28(6).
[490] Article 30 – 34.
[491] Supra, Model Law Part VI.
[492] Article 29 – 30.

(h) Supervisory capacity

The Directive requires that the supervisory Authority conduct an examination of the risks presented by processing operations before they commence.,[493] Member states may also pass legislation that can assist in determining the risks present.[494]

Member states must also provide for the publication of ongoing processing operations, to be kept in a register by the supervisory Authority.[495] This registry will contain the same information which the data subject receives from the Controller.[496] In both the GDPR and the Model Law these requirements are set out in the duties of the Controller.

For the supervisory Authority to be able to enforce the regime, it has the power to issue administrative remedies and persons must be granted a right to a judicial remedy for breaches of data protection law.[497]

The GDPR provides more definition of the powers and purpose of the supervisory Authority.[498] The supervisory body is required to protect the rights and freedoms of natural persons in the context of processing and to enhance the flow of information in the EU.[499] Related to this is the need to 'contribute to the consistent application' of the regulation.[500] Each supervisory body is independent and has the competence to exercise the tasks and powers assigned to it by the regulation.[501] The supervisory Authority can regulate the conduct of Controllers and processors through investigative, corrective and advisory powers.[502]

[493] Article 20(1) – (2).
[494] Article 20(30).
[495] Article 21(1) – (2).
[496] Article 21(3).
[497] Article 22.
[498] Supra, GDPR Chapter 6.
[499] Article 51(1).
[500] Article 51(2).
[501] Article 52 – 56.
[502] Article 58(1) – (3).

The provisions of the Model Law follow a similar pattern to the GDPR, yet the rules are not as detailed.[503] The Model Law divides the powers and duties of the Data Protection Authority.[504] A greater deal of attention is given to the provisions regulating the appointment of the Authority.[505]

Similar provisions also exist regarding remedies. The Authority is empowered to use a number of judicial sanctions to ensure compliance with the Model Law.[506] However, a crucial difference exists between the Directive and the SADC regime. In the Directive, the judicial remedy exists independently from the administrative sanctions that can be exercised.[507] The way that member states implemented this was that the data subject could approach different bodies for different remedies.[508] Therefore, depending on the remedy which the data subject sought, they could approach either the Authority or the Courts.[509] Research showed that in the EU, data subjects faced with an infringement of their rights were more likely to go the Authority.[510]

In terms of the Model Law, an individual seeking recourse must first exhaust all the remedies available before seeking recourse at the courts.[511] This forces the data subject to first approach the Authority in the event of a dispute. Based on the experiences of the EU, this is not problematic as most data subjects approached the Authority. Yet, there is still a limitation of the remedies that a data subject can rely on.

Ultimately, whether a data subject can successfully make a claim in terms of the Model Law will depend on the efficacy of the Authority.

(i) Data Transfer

[503] Supra, Model Law Part III.
[504] Article 4 & 5.
[505] Article 3.
[506] Article 9.
[507] Supra Directive Article 22 & GDPR Article 78 & 79.
[508] European Agency for Fundamental Rights *Access to data protection remedies in EU Member States* (2013) at 20.
[509] Ibid 32.
[510] Ibid 31.
[511] Supra, Model Law Article 39 – 40.

The Directive provides that there can only be a transfer of data if a third country provides adequate protection.[512] A number of factors are used to assess this, such as the nature of the data, the purpose of the processing, the rules of law in force and any professional rules.[513] If a third country does not have provide adequate protection, then the Commission should inform the member states and vice versa.[514] Further, steps should be taken to prevent a transfer to that third state.[515]

The Directive provides derogations from these rules by setting out the circumstances in which a transfer can occur to a third country not providing adequate protection.[516] There are a number of disjunctive grounds in terms of which a transfer can occur.[517] Further, a transfer is permitted if the Controller 'adduces adequate safeguards' to protect the rights and freedoms of the data subject.[518]

The GDPR's provisions are similar to the Directive yet they expand on certain rules. The 'general principle for transfers' are set out, establishing a concrete norm.[519] Second, when the EC makes the adequacy decision it will consider a stricter range of factors than in the Directive.[520] This is unsurprising as the GDPR serves to provide greater protection to data subjects by ensuring compliance with the standards it deems appropriate.[521] There is also the introduction of an obligation on the EC and the supervisory authorities to forward international cooperation, provide assistance internationally to third countries, to engage with relevant stakeholders in the international sphere and to promote the exchange of legislation relating to data protection.[522]

It is apparent that the GDPR strengthens the European transfer system by introducing stricter measures and a stricter standard for compliance. Accordingly, the obligation to foster international cooperation and assistance is beneficial as many regimes are based on the Directive and not on the

[512] Supra, Directive Article 25(1).
[513] Article 25(2).
[514] Article 25(3).
[515] Article 25(4).
[516] Article 26(1).
[517] Ibid.
[518] Article 26(2).
[519] Supra, GDPR Article 44.
[520] Article 45.
[521] Recital (101) – (104).
[522] Article 50(1).

GDPR and this can assist other states in bringing their data protection regimes in line with the GDPR.

There is, thus, the strange situation where the Model Law has an adequacy standard based on the Directive.[523] As the GDPR is stricter than the Model Law, it is likely that GDPR will meet this standard allowing for transfers from SADC to the EU. However, the Model Law, based on an out dated and weaker regime, will not be deemed adequate in the EU.

However, the Model Law's existing transfer rules are still of some significance for SADC and can still play an important role in creating a safe environment for data transfers within the region. As there is a lower transfer threshold for transfer to states that have implemented the Model Law, this could incentivise its adoption.[524] Further, it may even encourage states to adopt their own data protection regimes as there must still be an adequate level of protection which as beneficial as a stricter standard to comply with will result in greater protections to data subjects.[525]

(j) Concluding remarks

While the introduction of the Directive established a good starting point for data protection regulation within the Union, it had its own shortcomings surrounding its application and fragmentation. The GDPR remedied these issues, updated the Directive and elaborated on some key provisions like the duties of the Controller and processor. It also provided a far more detailed scheme for transborder data flows. The GDPR introduces more principles into the legal regime such as that of transparency concerning processing activities and data transfer and is thus one of the most comprehensive data protection regimes to currently exist.

Unfortunately, the Model Law bears a closer resemblance to the Directive than to the GDPR, meaning that many of its provisions are already outdated, despite it being a relatively recent instrument. However, there have been some important developments, such as the imposition of the obligations of transparency and accountability on the processor, that set the Model Law apart from

[523] Article 43
[524] Article 43(1)(a).
[525] Article 44(1).

the Directive. Despite this, it is apparent that no states from SADC, or Africa, are deemed to provide adequate protection.

Unfortunately, the comparison of the different regimes also revealed that states which adopt the Model Law will be at a disadvantage. Although a data protection regime has been introduced in SADC, a closer investigation has shown that it will not be as comprehensive as the regime in Europe, affecting data subjects, data processors and Controllers. It is easier for processors and Controllers to gain access to personal data in SADC than it is for SADC based Controllers to gain access to the EU. This is because the SADC based Controllers are only mandated to comply with their national regime. Should they wish to process data in the EU, they will be required to comply with the much stricter standard of the GDPR, which will increase their operational costs.

Additionally, one can ask what the point would be of implementing the SADC Model Law if it is outdated. For example, Mauritius, when updating its data protection regime in 2018 did so on the basis of bringing its provisions in line with the GDPR, completely bypassing the Model Law.

Thus, it is clear that there are a number of shortcomings with the SADC Model Law, and its future efficacy must be questioned.

5. CONCLUSION

The central theme of this work is the assertion that the SADC Model Law would fail to harmonise the data protection laws within the region, but that, despite this failure, there is still a degree of harmonisation between the laws due to the strong influence of the EU Directive in Africa. This is supported by an analysis of the relevant laws and other academic literature considering data protection in Africa.[526] This dissertation takes the existing literature a step further by considering the provisions of the SADC Model Law in specific detail and to compare it to data protection laws that are currently operative within the sub-region. Furthermore, comparing the SADC Model Law to the European regimes illustrates the extensive influence of the EU on data protection regimes in SADC, highlighting the shortcomings of the Model Law. By doing so, it has been shown why the Model Law is not necessarily the best instrument for the harmonisation of data protection law in the SADC region and why it needs to be revised and updated if it is to find effective application.

The comparative study undertaken here confirms the importance of having an effective data protection regime to promote cross-border trade and foreign investment in Africa, which is needed for the continent's continued economic development. Such a regime will also play a key role in allowing the ICT sector to develop and flourish. In turn, a flourishing ICT sector plays an important role in bridging the digital divide and must thus be nurtured. Additionally, the importance of harmonisation cannot be understated as it allows for transborder data flows to be established, which is crucial in a globalised world.

(a) Reflection on comparative study

Regarding how the Model Law was implemented and the state of data protection within the sub-region, research indicated that there were data protection laws already being applied in SADC but most of them were inadequate. The Model Law was introduced to address this problem, but it is a soft law and, thus, SADC member states are under no obligation to implement it. So far, only Tanzania and Zimbabwe have started to implement the Model Law with the 2018 Zimbabwean Data Protection bill being the only realisation of the Model Law in a domestic context so far. Yet,

[526] Alex B. Makulilo *Data Privacy Laws in Africa* (2016).

this is only a bill and no domestic law based on the Model Law has come into force. This illustrates that the first several years of the Model Law have been unsuccessful, and it has failed to achieve its stated aim of providing assistance in the establishment of data protection regimes in the region.

To consider the extent of harmonisation within the sub-region, the data protection laws of Mauritius and South Africa were considered. These two legal systems were selected as they are the most established data protection regimes in SADC and both states have comparatively large ICT sectors. Both states' data protection regimes were primarily based on the European regime and are not based on the Model Law. In fact, the South African Law Reform Commission suggested that South Africa should set the standard for data protection within SADC because of the leading role the country plays within the regional organisation. The comparative study highlighted some elements of the Zimbabwean data protection regime that resembled POPI rather than the Model Law such as the purpose clause, showing that the Model Law is not necessarily the only source that can be considered when introducing new data protection regimes.[527]

Despite the failure of the Model Law to play an important role in harmonisation, the laws considered still displayed some form of harmonisation in that each of the laws shared the same elements and similar legal definitions. The most notable differences can be found in the Zimbabwean Draft Bill which deviates more from the Model Law than POPI and the Mauritian Act. The Bill has been shown to have numerous issues concerning the independence of the Data Protection Authority and the wording of certain provisions relating to consent and the processing of data for national security laws where the other regimes all refer to social security laws.[528] The Bill also provides less rights to the data subject than the other regimes.[529] This is especially problematic when viewed in light of Zimbabwe's history of human rights violations.[530]

Thus, the Model Law has failed to harmonise laws in the region. Further, its soft law status has led to the discrepancies in the Zimbabwean Bill allowing for serious shortcomings as stated above.

[527] Supra, Zimbabwean Bill Clause 2
[528] Clause 13(2)(d) as compared with Article 15(2)(d) of the Model Law.
[529] Supra, Part VII of Zimbabwean Bill; Section 5(1) POPI; Section 37 – 40 Mauritian Act; Article 31 – 33 Model Law.
[530] Op cit, *Right to Privacy in Zimbabwe.*

Nevertheless, the hypothesis is confirmed in that there is still a degree of harmonisation due to the EU's influence in data protection law.

The influence of European law on the SADC member states' data protection regimes was also examined above.[531] Interestingly, each of the identified regimes is based on a European instrument, either the EU Directive or the GDPR. For this reason, the Model Law was compared to the relevant EU data protection instruments. The GDPR was focused on to determine the current state of development of data protection in the EU.[532] This is due to the significant influence which the EU has in the sphere of data protection and the fact that the GDPR can have extra-territorial effect, meaning that potential trade partners would have to have similar provisions.

In conducting the comparative study, it became clear that the Model Law is weaker than the current EU data protection rules in a number of areas, one example of this weakness is its inability to have extraterritorial application.[533] By extension, the other legal regimes considered in SADC are most likely outdated as well because they bear a close resemblance to the Model Law, which in turn resembles the now-outdated EU Directive. The only state that has updated its laws after the introduction of the GDPR is Mauritius, and still its Act is not as comprehensive as the GDPR.

The result of these discrepancies is that data protection regimes in SADC will not meet the EC's adequacy standard as it is far stricter than that in SADC.[534] As such, processors wishing to transfer data to Africa will have to take extra steps to ensure protection of this information, thereby increasing costs. In contrast to this, processors transferring from SADC to the EU will incur greater costs as the GDPR is stricter than most of the regimes considered. The disparities between the regimes clearly creates a power imbalance between the EU and SADC member states of a neo-colonial nature. Despite the introduction of data protection measures in SADC, which is encouraging, the content of these measures is already largely outdated, meaning that African states will be left behind. It also has the effect that there can be no processing of EU data within SADC

[531] Op cit Ramdo & Dauharry; Ncube in *African Data Privacy Laws*; SALC *Privacy and Data Protection.*
[532] Supra GDPR recital (4) – (5).
[533] The main issue is that the Model law reflects the Data Protection Directive which is outdated and not as comprehensive as the GDPR.
[534] Supra, GDPR Article 44.

because these states will never meet the strict adequacy standard. This restriction to data could possibly hinder the development of the digital economy in SADC.

Whether SADC can learn from the EU in this instance is a complicated matter. First, the context in both regions is completely different. The EU has one of the largest digital economies in the world with the implication that most member states have well established ICT sectors. This is not the case for SADC, where the goal is not to further integrate digital economies but rather to create an environment in which member states can develop their own digital economies. This is most evident if one considers the preambles of the different instruments, where specific reference is made to EU integration in the Directive and the GDPR.

There are also significant differences between the European understanding of privacy and data protection and SADC's more fractured approach where each state has a different understanding of privacy. This conceptual difference is highlighted by the separate right to data protection found exclusively in Europe.[535] By enshrining data protection as a separate right to the right to privacy, it illustrates how seriously data protection is taken in the EU and one can ask whether the same level of protection in SADC will ever be achieved without the Eurocentric conceptions of privacy and data protection.

Despite these differences, SADC and SADC member states have still adopted data protection laws that reflect the norms found in the EU. On some level, this is a positive development as these states are considering their need for data protection and have begun to build a data protection regime and the development of their ICT sectors. It is also noteworthy that most of the laws are based on the same European standards, meaning that intra-SADC data transfers should not be problematic, which could possibly lead to the growth of the digital economy in the region. There is also nothing preventing states in the sub-region from developing their own data protection laws (as Mauritius has done) to bring them in line with the newer European standard, which should allow for more uniformity with foreign trade partners based in the EU.

[535] Supra, TFEU Article 16.

Furthermore, a number of the laws considered in SADC place an obligation on the various data protection Authority to remain abreast with the latest developments in data protection and to inform government of these changes.[536] Some SADC states' data protection laws expressly include an obligation to cooperate internationally regarding data protection laws.[537] Provided that these obligations are complied with, SADC member states can further harmonise and update their rules which can lead to a more integrated digital economy in SADC. Thus, there is room for the growth of the digital economy and ICT sector in SADC which would be especially beneficial if it meant moving away from a reliance on the European Standard and European data flows. However, it will require a great deal of political will and cooperation.

(b) Recommendations

First, despite the degree of harmonisation between existing regimes, SADC member states should cooperate to further align existing data protection regimes and to assist other states in SADC to introduce their own data protection laws where none currently exist.[538]

Second, states should comply with the norms established in their data protection laws as this can assist the development of their own data protection laws and the data protection laws of other states. For example, POPI places an obligation on its Authority to facilitate cross-border cooperation 'by participating in any initiative that is aimed at such cooperation'.[539] Compliance with the data protection laws and participation in related initiatives would also include the obligation to educate members of the public about data protection, which is an important part of bridging the digital divide and aiding economic development.[540]

Third, in order to achieve successful harmonisation, there should be a greater dialogue between states pertaining to data protection laws. The current level of harmonisation has not been achieved

[536] Supra, Mauritian Act Section 5; Zimbabwean Bill Clause 8.
[537] Supra, POPI Section 40.
[538] For example, Mozambique.
[539] POPI, S40(h).
[540] Op cit Fariselli at 37. The digital divide does not only deal with the technological infrastructure but also with the ability of citizens to be adept in their use of the internet. Thus, states should educate their citizens to enable them to make better use of technology.

as a result of communication between states but rather because all laws are based on the same source material. By not having a shared data protection agenda, SADC member states will struggle to align their data protection laws. The result is inconsistencies in laws and the expansion of the digital divide within SADC. Thus, the introduction of a dialogue on shared data protection laws and norms, can improve the level of data protection to data subjects in SADC but also allow for a greater degree of harmonisation.

Fourth, although the adoption of a data protection regime similar to the EU's is beneficial as it grants protection to data subjects, States should be aware of the developmental context. There are elements in the laws considered that are aware of this such as the obligation on processors to ensure that data remains accessible despite any technological developments yet, most of the data protection laws are simply a transplant of a regime that exists in a different context. One can ask whether data protection regimes can be designed in a way that is more friendly towards developing nations, a weighty question that bears future investigation.

BIBLIOGRAPHY

Primary Sources

Conventions

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108.

Charter of Fundamental Rights of the European Union 2012/C 326/02.

UNTITRAL Convention on Contracts for the International Sale of Goods (1980)

WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

GATT 1994: General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994).

GATS: General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994).

TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994).

DSU, Dispute Settlement Rules: Understanding on Rules and Procedures Governing the Settlement of Disputes, Marrakesh Agreement Establishing the World Trade Organization, Annex 2, 1869 U.N.T.S. 401, 33 I.L.M. 1226 (1994).

Court Cases

Population Census Decision BVerfG, 1 BvR 209/83, Judgement of 15 December 1983.

Model Laws

SADC Model Law on Data Protection (2013)

UNCITRAL Model Law on Electronic Commerce (1996)

Regional Laws

African Charter on Human and Peoples Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982)

European Union Charter of Fundamental Rights 2012/C 326/02

EU Directive 95/46/EC

General Data Protection Regulation 2016/679

National Laws

Access of Information and Protection of Privacy Act 27 of 2007 (Zimbabwe)

Data Protection Act of 2003 (Seychelles)

Data Protection Act of 2004 (Mauritius)

Data Protection Act of 2015 (Madagascar)

Protection of Personal Information Act 4 of 2013 (South Africa)

Secondary Sources

Abrahams, Lucienne 'Regulatory imperatives for the future of SADC's "digital complexity ecosystem"' (2017) 20 *The African Journal of Information and Communication* 1 – 29.

Adelola, Tiwalade, Ray Dawson & Firat Batmaz 'Privacy and data protection in e-commerce in developing nations: evaluation of different data protection approaches' (2014) 5 *International Journal of Digital Society* 976 – 985.

Amiri, Shahram & Joseph M. Woodside 'Emerging markets: the impact of ICT on the Economy and society' (2017) 19 *Digital Policy, Regulation and Governance* 383 – 396.

Bainbridge, David 'Processing Personal Data and the Data Protection Directive' (1997) 6 *Information and Communications Technology Law* 17.

Bennet Moses, Lyria & Monika Zalneriute 'Law and technology in the dimension of time' in Sofia Ranchodás & Yaniv Roznai (eds) *Time, Law and Change: an Interdisciplinary Study* (2020) Hart Publishing, UK.

Bhamimia, Sahar 'The General Data Protection Regulation: the next generation of EU Data Protection' (2018) 18 *Legal Information Management* 21 – 28.

Blume, Peter 'An EEC Policy for Data Protection' (1992) 11 *Computer/Law Journal* 399.

Birnhack, Michael D. 'The EU Data Protection Directive: an engine of a global regime' (2008) 24 *Computer Law & Security Report* 508.

Boshe, Patricia 'Data privacy law reforms in Tanzania' in Alex B. Makulilo (ed) A*frican Data Privacy Laws* (2016) Springer, Electronic.

Bradford, Anu 'The Brussels Effect' (2012) 107 *Northerwestern Law Review* 1.

Bygrave, Lee A. 'International agreements to protect personal data' in James B. Rule (ed) *Global Privacy Protection the First Generation* (2008) Edward Elgar, Cheltenham, UK.

Cate, Fred H 'The EU Data Protection Directive, Information Privacy, and the Public Interest' (1994) 80 *Iowa Law Review* 431.

Corley, Morgan A 'The need for an international convention on data privacy: taking a cue from the CISG' (2016) 41 *Brooklyn Journal of International Law* 721 – 779.

Corte, Lorenzo Dalla 'A right to rule: on the substance and essence of the fundamental right to personal data protection' in Dara Hallinan, Ronald Leenes & Serge Gutwirth et al (eds) *Data Protection and Privacy: Data Protection and Democracy* (2020) Hart Publishing, UK.

Currie, Iain & Johan de Waal *The Bill of Rights Handbook* 6ed (2016) Juta & Co, Cape Town.

Daly, Angela *Private Power, Online Information Flows and EU Law: Mind the Gap* (2016) Hart Publishing: Oxford, England.

Data Protection Office 'Decisions on' Compliance' http://dataprotection.govmu.org/English/Pages/Decisions-on-Complaints.aspx accessed 18 August 2020.

De Hert, Paul & Vagelis Papakonstaninou 'The proposed data protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28 *Computer & Security Review* 130 – 142.

Efrat, Asi 'Promoting trade through private law: explaining international legal harmonization' (2016) 11 *The Review of International Organizations* 311 – 336.

Ewlukwa, Nnaemeka 'Is Africa ready for electronic commerce – a critical appraisal of the legal framework for ecommerce in Africa' (2011) 12 *European Journal of Law Reform* 550.

Fariselli, Patrizia 'E-commerce for development: a general framework' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) Organization for Economic Cooperation and Development, Paris.

Fombad, Charles Manga 'Some reflections on the prospects for the harmonization of international business laws in Africa: OHADA and beyond' (2013) 59 *Africa Today* 51.

Frosio, Giancarlo F. 'The right to be forgotten: much ado about nothing' (2017) 15 *Colorado Technology Law Journal* 307 – 336.

Goldstein, Andrea & David O'Connor 'An introduction to the devate on electronic commerce and development' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) Organization for Economic Cooperation and Development, Paris.

Gereffi, Gary 'The evolution of global value chains in the internet era' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) Organization for Economic Cooperation and Development, Paris.

Faria, Jose Angelo Estrella 'Legal harmonization through Model Laws: the experience of the United Nations Commission on International Trade Law' available at https://www.justice.gov.za/alraesa/conferences/2005sa/papers/s5_faria2.pdf accessed 15 July 2020.

Fraser, Simon 'Persistent barriers to e-commerce in developing countries: a longitudinal study of efforts by Caribbean companies' (2011) 19 *Journal of Global Information Management* 30.

Greenleaf, Graham & Marie Georges 'African regional privacy instruments: their effects on harmonization' (2014) 132 *Privacy Laws and Business International Report* 19 – 21.

Greenleaf, Graham 'The Influence of European data privacy standards outside Europe: implications for globalization of Convention 108' (2012) 2 *International Data Privacy Law* 68 – 92.

Harmonization of ICT Policies in Sub-Saharan Africa *Data Protection: SADC Model Law* (2013) International Telecommunications Union, Electronic.

Harris, Andrew, Seymour Goodman & Patrick Traynor 'Privacy and security concerns associated with mobile money applications in Africa: Mobile Money Symposium 2013' (2013 8 *Washington Journal of Law, Technology and Arts* 245 – 263.

Heawood, Jonathan 'Pseudo-public political speech: Democratic implications of the Cambridge Analytica Scandal' (2018) 23 *Information Polity* 429.

Hoeren, Thomas 'Proposal for a Council Directive on Data Protection and Its Impact on German Industry' (1993) 1 *International Journal of Law and Information Technology* 129.

International Telecommunications Union *HIPSSA – ICT Regulatory Harmonization: A Comparative Study of Regional Initiatives* (2009) International Telecommunications Union, Electronic.

International Telecommunications Union 'Support for the Establishment of Harmonized Policies for the ICT Market in the ACP States'https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

accessed 15 July 2020.

Kalumiva, Ndoli 'Mauritius' in African Development Bank *2018 African Economic Outlook* (2018) African Development Bank, Electronic.

Kelley-Salinas, Guillermo 'Different Educational Inequalities: ICT an Option to Close the Gaps' n Organisation of Economic Cooperation and Development *Learning to Bridge the Digital Divide* (2000) Publishing, OECD & Centre for Research and Innovation, Paris.

Korff, Douwe *EC Study on Implementation of Data Protection Directive: comparative summary of national laws* (2002) Human Rights Centre University of Essex, Colchester.

Lee, Suk-Joo, Cheolhwi Ahn & Kelly Minjung Song et al. 'Trust and distrust in e-commerce' (2018) 10 *Sustainability* 1015 – 1034.

Lohsse, Sebastian, Reiner Schulze & Dirk Staudenmayer 'Trading data in the digital economy: legal concepts and tools' in Reiner Schulze & Dirk Staudenmayer (eds) Trading *Data in the Digital Economy: Münster Colloquia on EU Law and the Digital Economy* (2017) Hart Publishing, Oxford.

Madhub, Drudeisha 'The pioneering journey of the Data Protection Commission of Mauritius' (2013) 3 *International Data Privacy Law* 239 – 243.

Makulilo, Alex B. 'Data protection of the Indian Ocean Islands: Mauritius, Seychelles, Madagascar' in Alex B. Makulilo *African Data Privacy Laws* (2016) Springer, Electronic.

Makulilo, Alex B 'Myth and reality of harmonization of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78 – 89.

Makulilo, Alex Boniface 'Data protection regimes in Africa: too far from the European " adequacy" standard' (2013) 3 *International Data Privacy Law* 42.

Makulilo, Alex & Kuena Mophethe 'Privacy and Data Protection in Lesotho' in Alex B. Makulilo *(*ed) *African Data Privacy Laws* (2016) Springer, Electronic.

Makulilo, Alex 'The context of data privacy in Africa' in Alex B Makulilo (ed) A*frican Data Privacy Laws* (2016) Springer, Electronic.

McNair, Stephen 'The emerging policy agenda' in Organisation of Economic Cooperation and Development *Learning to Bridge the Digital Divide* (2000) Publishing, OECD & Centre for Research and Innovation, Paris.

Mody, Cyrus C.M. *The Long Arm of Moore's Law: Microelectronics and American Science* (2016) MIT Publishing, Cambridge Massachusetts.

Moerel, Lokke 'The long arm of EU Data Protection Law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 *International Data Privacy Laws* 23.

Monti, Andrea & Raymond Wacks 'Personal information and data protection' in Andrea Monti & Raymond Wacks (eds) *Protecting Personal Information: The Right to Privacy Reconsidered* (2019) Hart Publishing, UK.

Mouzakiti, Foivi 'Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive' (2015 1 *European Data Protection Law Review* 39.

Mwenda, Kenneth Kaoma 'Deconstructing the concept of human rights in Africa' (2000) 25 *Alternative Law Journal* 292 – 295.

Nangela, Deo John *The Adequacy of the Tanzanian Law on E-commerce and E-contracting: Possible Solutions to be Found in International Models and South African Legislation* (unpublished PhD Thesis, University of Cape Town, 2011)

Ncube, Caroline B. 'Data Protection in Zimbabwe' in Alex B. Makulilo *African Data Privacy Laws* (2016) Springer, Electronic.

Ndossy, Kevin Godfrey *Mobile Cellular Communications and its Effect on Personal Data Protection in Tanzania* (Unpublished LLM thesis, University of Oslo, 2014).

O'Connor, David 'E-commerce for development: between Scylla and Charybdis' in Andrea Goldstein & David O'Connor (eds) *Electronic Commerce for Development* (2002) Organization for Economic Cooperation and Development, Paris.

Oosteven, Manon & Kristina Irion 'The golden age of personal data: how to regulate an enabling fundamental right' in Mor Bakhoum, Beatriz Conde Gallego & Mark-Olver Mackenrodt et al (eds) P*ersonal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (2018) Springer, Berlin Heidelberg.

Olinger, Hanno N. Johannes J. Britz & Martin S. Olivier 'Wester privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy Bill' (2007) 39

The International Information and Library Review 31 – 43.

Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data* (1980).

Patokorpi, Erkki & Kai K. Kimppa 'Dynamics of the key elements of consumer trust building online' (2006) 4 *Information, Communication and Ethics in Society* 17 – 26.

Poullet, Yves 'Is the General Data Protection Regulation the solution' (2018) 34 *Computer Law & Security Review* 773 – 778.

Privacy International *Submission on the Cyber Security and Data Protection Bill 2019 to the Parliament of Zimbabwe* (202) available at *https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf*

accessed 28 July 2020.

Ramdoo, Satyanraj & Inza Dauharry 'Harmonising the GDPR in Mauritius' available at *https://www.africalegalnetwork.com/mauritius/news/harmonising-gdpr-mauritius/* accessed on \ 27 July 2020.

Roos, Anneliese 'Data Protection Law in South Africa in Alex B. Makulilo *African Data Privacy Laws* (2016) Springer, electronic.

Ryngaert, Cedric & Mistale Taylor 'The GDPR as Global Data Protection Regulation?' (2020) 114 *AJIL Unbound* 6.

Schwartz, Paul M 'Global Data Privacy: The Eu Way' 2019 (94) *New York University Law Review* 771.

Sha, Wei 'The nomological network validity of perceived fairness in business-to-consumer ecommerce' (2014) 5 *Issues in Information Systems* 328 – 334.

Slokenberga, Santa, Jane Reichel & Rachel Niringiye et al. 'EU data transfer rules and African legal realities: is data exchange for biobank research realistic' (2019) 9 *International Data Privacy Law* 30 – 48.

South African Law Commission Discussion Paper 109 (Project 124) *Privacy and Data Protection* (2005).

Stewart, David P 'Private international law, the rule of law, and economic development' (2011) 56 *Villanova Law Review* 607 – 630.

Taylor, Roger 'No privacy without transparency' in Ronald Leenes, Rosamunde van Brakel & Serge Gurtwith et al (eds) *Data Protection and Privacy: the Age of Intelligent Machines* (2017) Hart Publishing, UK.

Tikkinen-Piri, Christina, Anna Rohunen & Jouni Markulla 'EU General Data Protection Regulation: changes and implications for personal data collecting companies' (2018) 34 *Computer Law & Security Review* 134 – 153.

Townsend, Beverley Alice *Privacy and data protection in eHealth in Africa – an assessment of the regulatory frameworks that govern privacy and data protection in the effective implementation of electronic health care in Africa: is there a need for reform and greater regional collaboration in regulatory policymaking* (unpublished LLD thesis, University of Cape Town, 2017).

Traça, João Luís & Francisca Correia 'Data Protection in Angola' in Alex B. Makulilo African Data Privacy Laws (2016) Springer, Electronic.

Traça, João Luís & Lidia Neves 'Data Protection in Mozambique: Inception Phase' in Alex B Makulilo *African Data Privacy Laws* (2016) Springer, Electronic.

United Nations Conference on Trade and Development *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (2016) United Nations, Geneva & New York

United Nations Conference on Trade and Development *Digital Economy Report* (2019) United Nations, Geneva & New York.

United States Department of Health, Education & Welfare *Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973) Department of Health, Education & Welfare, Washington D.C.

Van der Merwe, DP; A Roos & T Pistorius et al *Information and Communications Technology Law* 2 ed (2016) Lexis Nexis, South Africa.

Van Dijk, Jan *The Digital Divide* (2020) Polity, Cambridge England.

Vanberg, Asyem Diker & Maelya Maunick 'Data protection in the UK post-Brexit: the only certainty is uncertainty' (2018) 32 *International Review of Law, Computers & Tchnology* 190.

Versaci, Giuseppe 'Personal data and contract law: challenges and concerns about the economic exploitation of the right to data protection' (2018) 14 *European Review of Contract Law*

374 – 392.

Voight, Paul & Axel von Dem Bussche *The EU General Data Protection Regulation (GDPR): a Practical Guide* (2017) Sprininger International Publishing, Online.

Von Grafenstein *The Principle of Purpose Limitation in Data Protection Laws: the Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation* (2018) Nomos Verlagsgesellschaft mbH, Baden-Baden Germany.

Wagner, Julian 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' (2018) 8 *International Data Privacy Law* 318 –337.

Ward, Ken 'Social networks, the 2016 US presidential election and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioural microtargeting' (2018) 3 *Journal of Media Ethics* 133.

Weimann, Thomas & Daniel Nagel 'Agreeing on a definition for data protection in a globalized world' (2012) *IEEE Technology and Society Magazine* 39 – 42.

Wong, Julia Carrie 'The Cambridge Analytica scandal changed the world – but it didn't change Facebook' available at *https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook,* accessed on 22 May 2020.

Wong, Rebecca 'The Data Protection Directive 95/46/EC: idealisms and realisms' (2012) 26 *International Review of Law, Computers and Technology* 229.

Wright, Scott A. & Guang-Xin Xie 'Perceived privacy violation: exploring the malleability of privacy expectations' (2019) 156 *Journal of Business Ethics* 123.

Zimbabwe Human Rights NGO Forum, the Digital Society of Zimbabwe, Privacy International & International Human Rights Clinic at Harvard Law School et al *The Right to Privacy in Zimbabwe Stakeholder Report Universal Periodic Review 26th Session* (2016).