MISA ZIMBABWE

Continuing and Emerging Issues for

Data Protection Authorities

in the Southern African Development Community

KONRAD ADENAUER STIFTUNG

CONTENTS

1 Executive Summary PAGE 2

2 Methodology & Limitations PAGE 3

3 Contextual Introduction PAGE 3

4 Issues Old and New

4.1 Unending Debate on Independence of Data Protection Authorities ..... PAGE 5

4.2 Protecting sensitive personal data: COVID-19 ..... PAGE 9

4.2.1 COVID Surveillance Infrastructure case of Zimbabwe ..... PAGE 10
4.2.2 COVID-19 data storage and destruction case of South Africa ..... PAGE 12

4.3 Automated data processing ..... PAGE 13

4.4 Breach notification or data leaks or security compromises ..... PAGE 15

4.5 Lawful transfer of data across borders ..... PAGE 18

4.5.1 Comparative data transfers provisions in SADC member states ..... PAGE 19
4.5.2 Designation of countries for cross border data transfers: Case of Botswana ..... PAGE 21

4.6 Digital identification systems (DIS) ..... PAGE 23

5 Concluding Observations PAGE 25

6 Recommendations PAGE 28

1. Executive Summary

Data protection has gained global importance, for various reasons. Data has been viewed as the new oil, though it is not oil, as it is non-rivalrous, and replenished unlike oil. Data has been seen as driver of economic growth, with its economic value estimated in billions, causing countries to rush towards a digital economy. Data has again been viewed as part of a fundamental right to privacy, though it is not the same as the right to privacy and albeit deserving protection as violations of personal data results in economic, social, emotional and discriminatory harms. This report does not debate or distinguish the value or importance of data but focuses on the increased efforts to protect data privacy within the Southern African Development Community (SADC) region, as a political and economic bloc.[1] This report contributes to the growing literature on data protection authorities (DPA) in Africa, focusing on countries in the Southern African Development Community (SADC). For purpose of this report only Eswatini, Zimbabwe, Botswana, Zambia, Lesotho, South Africa and Mauritius are referenced and reviewed.

As technology evolves, new challenges emerge, that data protection authorities are not sufficiently designed to resolve or address, and therefore their independence becomes irrelevant or insufficient, as the pressing matters are not entirely about independence, but technical, political and administrative. There are several challenges for data protection, and data protection authorities; these are automated data processing; cross border data transfers; handling of sensitive data including health related data from COVID-19; surveillance and smart cities; and data breaches. The report highlights some of the pressing needs for DPAs including financial support, administrative issues, and enforcement of decisions. The enforcement of data protection laws is dependent on the existence of a functioning data protection authority whether as a single institution or several institutions that might have shared mandates. While the absence of independent data protection authorities capable of enforcing data protection is usually the main issue of concern, there are other emerging aspects weakening the capacities of data protection authorities to advance data privacy and data protection as a fundamental right. This report makes further assertions that while independence of the data protection authority is essential, it cannot be the only issue undermining the effective protection of data privacy in the SADC region. The report makes specific recommendations to data protection authorities; legislature and civil society.

[1] *SADC has 16 Member States, namely Angola, Botswana, Comoros, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, and Zimbabwe.*

2. Methodology and limitations

The report uses a mixed methods approach of desk review and key informant interviews from specific countries as it relates to emerging and thematic issues that require the intervention of DPAs. The report builds on some of the extensive findings and recommendations from reports such as the Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of their Existence on the Continent (Paradigm 2021) and the Understanding the Challenges Data Protection Regulators Face: A Global Struggle Towards Implementation, Independence, & Enforcement Introduction (Internews 2022). In addition to desk review, the report utilised interview materials from a different key informant in the SADC region and beyond, who shared expert opinion on the state of data protection, challenges, and opportunities. The report does not conduct a full country investigation or complete analysis of all the laws concerned with data protection in each country.[2] The report revisits law provisions and contextual practices that affect DPA; cross border data transfers; automated processing; processing of sensitive personal data; and digital identities with an intention of highlighting the many emerging and continuing challenges.

3. Contextual introduction

Most African countries have adopted data protection laws.[3] And in the SADC region, the adoption of these laws was due to the partnership of SADC, the European Union (EU) and International Telecommunications Unions (ITU) through the Harmonisation Policies for the ICT Market in the African Caribbean and Pacific; for southern Africa, this project was called Support for Harmonization of ICT Policies in Sub-Sahara Africa (HIPSSA).[4] Through HIPSSA, a model data protection law was adopted which has informed most data protections laws in the SADC region. The SADC Model Law on Data protection is currently being revised by SADC, as it clearly has several shortcomings, one of which is that it is not binding on member states in comparison to other regions such as Economic Community of West African States (ECOWAS) established by the Treaty of Lagos on 28 May 1975 designed to promote regional cooperation and integration. ECOWAS adopted a binding Supplementary Act on personal data protection at the 37th session of

[2] *For different countries, there are specific and detailed analysis of each data protection law and in some instances, handbooks and guides for users and practitioners.*

[3] *According to UNCTAD as of 14 February 2021 of the 54 African countries 33 (61%) had legislation in place; 6 (11%) had draft Legislation: 10 (19%) no legislation and there was no data for 5 (9%). Of the 54 African countries of which in the SADC region of the 16 member states only 5 have pending drafts or are in the process of drafting laws. The majority of countries with data protection laws are therefore in the SADC region.*

[4] *Interview Nigeria respondent indicated that the DP laws are sometimes pursued for political interests and political points. Other countries might pass these laws but still concerned that they constrain their future interests.*

the authority of Heads of State and Government in Abuja.[5] SADC has maintained its model law, with implications for enforcement and regional integration, as a model law is not enforceable. Furthermore, at the continental level, the adoption of the African Union Convention on Cybersecurity and Data Protection, (the Malabo Convention) has not resulted enjoyed significant ratification by SADC countries.[6] The Malabo Convention faces delays in ratification, and in an interview one key informant observed that it's a combination of lack of interest and understanding of the opportunities being missed by countries in advancing the formation of a single digital market.[7]

As of 2023, at least 12 of the SADC countries had adopted a data protection law, and the remaining namely Namibia, Malawi, Democratic Republic of Congo had draft laws and Mozambique and Comoros were beginning drafting. More notable however is that all countries have constitutional provisions protecting the right to privacy and privacy of communications, with Mozambique, being more specific in that its constitution is the only one providing for data protection under article 71, and it further requires that there is a law that provides for access, generation, protection, and use of computerised personal data. This is significant.

The implementation of data protection laws has been driven by various factors including the demands for countries to be prepared for the information and data revolutions underway, to harnessing the economic dividends presented by data protection. The influence of the EU or economic interests cannot be overruled; however, the report does not detain itself on this issue, but the intention to understand the different old and contemporary challenges to data protection. The report looks at the following countries with data protection laws; Zimbabwe Cyber and Data Protection Act (CDPA) of 2021; Botswana Data Protection Act (BDPA) of 2018; Zambia Data Protection Act (ZDPA) of 2021; Mauritius Data Protection Act (MDPA) of 2017; Lesotho Data Protection Act (LDPA) of 2011; Eswatini Data Protection Act of 2022 (EDPA); South Africa: Protection of Personal Information Act (POPIA) of 2013.[8]

In addition to these data protection laws, some of the countries have retained statutes that either complement or constraint data protection. These laws include laws allowing for use of personal data for security purposes without sufficient oversight, the bulk interception and surveillance of communications,

[5] *A/SA.1/01/10 adopted in Abuja on the 16th day of February 2010.*

[6] *As of 14 February 2023, of the 16 SADC countries only 5 countries namely Zambia, Mozambique, Angola, Mauritius, and Namibia had ratified the Malabo Convention.*

[7] *Interview with SG, Nigeria, 24 January 2023.*

[8] *As most of the laws are all called Data Protection Acts, to distinguish them, each abbreviation of the Act in this paper is preceded by the initial of the country, as LDPA (Lesotho); ZDPA (Zambia); MDPA (Mauritius); BDPA (Botswana), with the exception of Zimbabwe and South Africa with different names.*

extreme hindrances on freedom of expression, and right to information which due consideration of the need to balance. Furthermore, the DP laws are not the only laws, but take account of other sector specific laws.[9] This is not an issue if there is coordination and complementary approaches, and if also the DPA is mandated to provide oversight on the actual protection of personal information that might be stipulated in for instance the Consumer Protection Act (consumer rights) or the Banking Act (financial information).

4. Issues Old and New

The economic interests and rights aspects of data is premised as the reason for the adoption of data protection laws in most countries. Reading of preambles or statements of objects of the DP laws confirms this position. For instance, the LDPA objects is to "reconcile the fundamental and competing values of personal information privacy under this Act and sector specific legislation". A statement of objects and reason shared by the Lesotho Minister of Home Affairs accompanying the Bill noted that while "privacy of personal information must be guaranteed. On the other hand, free flow of information is a necessary feature of economic life. The Bill proposes provisions intended to balance protection of personal data rights against economic interests of the wider society". Similarly, the EDPA objects are for an "Act to provide for collection, processing, disclosure and protection of personal data; balancing of competing values of personal information privacy and sector specific laws and other related matters'. Zimbabwe's CDPA section 2 object are "to increase cybersecurity in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects".

These DP laws objectives demonstrate the complexity of managing the different data interests and rights, especially as it relates to public and private interests. The tension between these interests will increase with the technological evolution. With such changes, DPAs are required to adapt and meet the challenges. The laws might not be amended with each and every development, which is understandable, however if DPAs are not adaptive, then their function will be illusory and ineffective. Admittedly, amendments to some of the DP laws is also necessary to cure the fundamental shortcomings, and some of the amendments will be highlighted in the paper.

4.1 Unending debate on independence of data protection authorities

The independence of the DPA is essential to the effective protection of personal data for many reasons. First, the interest in personal data is from wide ranging of actors, domestic, and international. This means that a DPA must be capable

[9] *EDPA, and LDPA make explicit mention of other sector specific laws in their preambles/objects*

of tackling different kinds of data issues, breaches, provide guidance to controllers and data processors, who might include data brokers, social media companies, government agencies, among others. Being independent in this regard requires a high degree of financial and technical independence, and not being susceptible to political or economic influence.

Second, to achieve this level of independence, the appointment and constituting of the DPA must not only be independent, but it must be seen to be independent. Though most DP laws provide that the DPA must not be subject to the control or direction of any person, this statement is not convincing for various reasons. First, the budgets of most of these DPAs are decided by the executive through a minister. This is the case with South Africa's Information Regulator under the Protection of Personal Information Act (POPIA). In a recent move, South Africa's Parliament called for the IR to not rely on the policies and procedures of the Department of Justice and Constitutional Development (ministry of justice) as this showed lack of independence, as the IR must report and account directly to Parliament. In terms of financial independence, the IR is not recognised as a public entity or constitutional institution in terms of the Public Finance Management Act (PFMA)[10], which means it can only receive funding to perform its functions through the ministry of justice. Comparatively, the South African IR is perceived to be the most proximate of what constitutes an independent DPA in Southern Africa, but the role of central government or ministry is consistent with the required institutional independence and further the ministry of justice is a data controller and must be accountable to the IR on how it processes information. This current relationship does not augur for accountability. The financing of DPAs is similar to many of the countries under review.[11]

A number of African countries are not establishing new DPAs', existing communications commission or regulatory bodies are mandated to implement the DP law. Zimbabwe, CDPA section 5 designates an existing body, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) established under the Postal and Telecommunications Act (PTA) to be the data protection authority. The CDPA does not change the composition nor procedure to composition POTRAZ of which the Minister and President have significant influence on POTRAZ under PTA but will now supposedly not influence the direction of POTRAZ under the CDPA. Government authorities justified this

[10] *Other constitutional institutions recognised by PFMA includes the Public Protector; the Human Rights Commission; the Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities; the Commission for Gender Equality; the Independent Electoral Commission; the Independent Broadcasting Authority; the Financial and Fiscal Commission; the Commission on the Remuneration of Persons Holding Public Office; the Pan South African Language Board; the Municipal Demarcation Board.*

[11] *The financing is through line ministries such as Justice or Information or generally public service commission.*

decision on the basis to move with speed to enforcement and the cost factors.[12]

Eswatini adopted a similar approach in its 2022 DP law approving the Eswatini Communications Commission (ECC) to be the DPA. Section 5 of the EDPA designates the ECC established under the Eswatini Communications Commission Act (ECCA) as the DPA with the powers to enforce "administer this Act and protect the respective rights of information privacy provided for under this Act or any other law". This provision while clear, raises concerns on the administering of other laws on privacy, and this could be for instance the administration of the freedom of information law (if such exists), or a consumer protection law, or banking law if there rights of information privacy. The ECC is supposed to be independent and not under the direction of anyone, as provided under section 3(2) of the ECCA, which states that.

"Except as otherwise provided in this Act or any other written law, the Commission shall be independent in the performance of the functions of the Commission and shall not be subject to the direction or control of any person or authority".

The ECC is actually appointed by the Minister responsible for telecommunications in terms of in terms of section 6 of The Public Enterprises (Control and Monitoring) Act 1989. The same commission is responsible for regulating and coordinating matters of cybersecurity and enforcing security standards for critical infrastructure under the section 52 of the Computer crime and Cybercrime Act of 2022 as well as being the secretariat of the National Cybersecurity Advisory council, established under section 53 of the Computer crime and Cybercrime Act of 2022.

It must be pointed out that Zimbabwe takes a similar approach as have done a few other countries, namely Rwanda, Chad, and Ivory Coast. However, there are concerns with this institutional approach. First, while communication authorities are perceived to operate independently and without directions from anyone, some of the enabling statutes such as Postal and Telecommunications Act of Zimbabwe inserts clauses that deliberately reduce the independence or autonomy of the DPA. The Zimbabwe CDPA section 6(2) provides that the Authority (DPA-POTRAZ) shall no, in the lawful exercise of its functions under this Act (CDPA) be subject to direction or control of any person or authority, however in the same section, 6(1)(d) on functions of the Authority must submit to any court an administrative act inconsistent with CDPA in consultation with the minister responsible for information, publicity and broadcasting services. In consultation with is not interpreted in the Constitution, though there is definition of 'after consultation' whose consultation outcome is not binding, and therefore not obliged to follow.[13]

[12] *Interview with POTRAZ official suggesting that a separate DPA would have been costly and delayed, hence POTRAZ assumed this role, and might in future lead to the formation of separate and independent entity.*

[13] *Section 339 of the Constitution of Zimbabwe.*

The definition of in consultation means the opposite, that the person or authority concerned must follow the advice rendered. This interpretation if correct means that the DPA is actually not independent to carry out its tasks. The CDPA has other provisions in which directions may be given on the process of sensitive information affecting national security or interests of the state.[14] In addition to these provisions real concerns exist in respect of who do the DPA reports to. For Eswatini, the ECC submit reports to Parliament in terms of section 53 of the ECC, and under the EDPA functions of the ECC includes report with or without request to Parliament from time to time on any matter affecting protection of personal information. Zimbabwe's CDPA is silent on this, and in fact in the PTA, allows the minister to give policy directions to POTRAZ Board as the minister "considers to be necessary in the national interest" and the minister may direct board to reverse, suspend or rescind its decisions after consultation with the President.[15]

In Botswana, the BDPA the commissioner and deputy appointed by the minister[16], and the commission may receive directions of a "general or a specific nature" from the minister regarding the exercise of its powers and functions.[17] Under its functions, section 5(2)(o), the commission shall perform any other functions that may be conferred it by the Minister. The BDPA requires that the directives or functions shall not be inconsistent with the Act or with Commissions obligations, and once given the Commission shall give effect to such direction. This provision is as problematic on many respects, as the Commission and Commissioners are not designed to object to any of the directions as the Minister gives. The directive might be incorrect, and the Commission has no power to object, and is operating under the Public Service Act provisions. Under section 5(2)(n), the Commission must record all directions given by the Minister during the course of the year, however this is not enough if not publicised or reported to Parliament. The Prime Minister on the advice of the Minister following public nominations appoints the data protection

[14] *Section 11(4) of Zimbabwe CDPA. See also the Interception of Communications Act section 7(1)(a)(ii) on renewal of interception warrants, noting that the "Minister in consultation with the Prosecutor General" may renew the interception warrant for a period not exceeding three months.*

[15] *Postal and Telecommunications Act sections 25(1) and 26(1).*

[16] *Botswana BDPA section 6(2). The commissioner then appoints other people to be part of the staff or commission.*

[17] *Botswana BDPA section 9.*

commission.[18] This process attempts to include public participation, but the final decision rests with the Prime Minister.

4.2 Protecting sensitive personal data: COVID-19

The first case of corona virus was reported in China in December 2019 amid state denials. On 11 March 2020, the world woke up to news of declaration of a global pandemic by the World Health Organisation (WHO) following an earlier declaration of COVID-19 as a Public Health Emergency of International Concern on 30 January 2020. According to the African Judges and Jurists Forum (AJJF), SADC member States undertook several measures including the setup of border and in-country testing centres; social distancing and cancellation of gatherings; adoption of self-isolation and mandatory quarantines.[19] Countries declared states of emergency or states of disaster. AJJF further reported that the declaration of national states of disasters were in Malawi, South Africa, and Zimbabwe; and states of emergencies were in Angola, Democratic Republic of Congo, Eswatini, Lesotho, Mozambique, and Namibia; while declarations of Public Health Emergencies were in Botswana, and Madagascar.[20]

The COVID-19 disaster declaration limited individual rights to decide on medical testing, and bodily integrity.[21] These emergency laws compelled compulsory testing[22], and authorised disclosure of COVID-19 status.[23] Of course, informed consent before any medical or scientific experiments, extraction or use of bodily tissue is required.[24] That said, consent remains a mystical, and is waived in public emergencies.[25] Medical professionals while bound to keep confidentiality of medical records and details, they are compelled to disclose COVID-19 status to authorities.[26] Unfortunately, as the pandemic necessitated, some countries like Zimbabwe resorted to deployment of non-medical personal to assist, with concerns of violation of patients

[18] *Lesotho, LDPA section 6 on Establishment of the Data Protection Commission.*

[19] *African Judges and Jurists Forum "Addressing the Impact of COVID-19 on Economic, Social and Cultural Rights in Southern Africa' A policy brief (June 2021).*

[20] *AJJF Policy Brief (2021).*

[21] *as protected under section 52(2)(c) of the Constitution of Zimbabwe for instance.*

[22] *See Zimbabwe Section 6 of the PHA COVID-19 Prevention and Containment Regulations provides for compulsory testing if one is suspected of having COVID-19. South Africa,*

[23] *Zimbabwe Statutory Instrument 77 of 2020 Public Health (COVID-19 Prevention and Containment) Regulations.*

[24] *UN General Assembly, Special Rapporteur on the Right of Everyone to the Enjoyment of the Highest Attainable Standard of Physical and Mental Health, A/HRC/22/53, 2013.*

[25] *Tschider 2019 96 Washington University Law Review 1505.*

[26] *McQuoid-Mason 2020 6 SAMJ 110.*

personal data.[27] [28] Data protection laws recognise such situations, but more importantly as Botswana law states any other person who is not a health professional collecting sensitive personal data must carry out those directions under the supervision of a health professional and a person who is directly authorised to perform such functions.[29] Many countries however subordinate these issues, when faced with public health crises but the balancing of rights is non-negotiable.[30] The public health interests limit the individual's decisional and informational privacy, as these rights become subservient to public welfare interests.[31]

To contain the spread of COVID-19, collection of sensitive personal data in form of health information increased, with the adoption of mobile applications, and contact notification procedures. According to International Centre for Not-for-Profit Law (ICNL), over 62 laws were adopted globally that violated the right to privacy through data collection, and Zimbabwe, South Africa, and other public health standard measures (PHSMs) requiring temperature readings and recording of personal mobile numbers for contact tracing, this information if cross-referenced with the mobile subscriber databases in most countries it, easily discloses health-related data.[32]

4.2.1 COVID Surveillance Infrastructure case of Zimbabwe

The COVID-19 pandemic had the most technologically advanced responses in human history and collected corpus amounts of personal data.[33] Countries adopted systematic and ongoing collection, collation, and analysis of sensitive personal data. The technology enabled surveillance assumed a positive societal value bringing efficiency and effective responses to the pandemic. However, there are significant concerns. The scale of surveillance and data collection was concerning as massive health-related data was processed in

[27] NewsDay 'Military nurses take over hospitals' https://www.newsday.co.zw/2020/11/military-nurses-take-over-hospitals/ (last accessed 10 April 2023)

[28] Article 9(3) of General Data Protection Regulation processing of health data for medical purposes under art 9 (2)(h) must be done by a professional who is bound by professional confidentiality.

[29] Botswana Data Protection Act section 23(2).

[30] Makwaiba BS "Tension between the individual's fundamental human rights and the protection of the public from infectious and formidable epidemic diseases" 2021 21 AHRLJ 311-334.

[31] Makwaiba (2021)

[32] Section 8 of Statutory Instrument 95 of 2014 Postal and Telecommunications (Subscriber Registration) Regulations, 2014. The Postal and Telecommunications Regulatory Authority (POTRAZ), established under Postal and Telecommunications Act (PTA) mandated compulsory registration of subscriber identity module (SIM) and establishing of a database.

[33] O Saki "A health pandemic not a data-pandemic: an analysis of Zimbabwe's data protection framework in response to COVID-19' paper unpublished (2022).

several countries.[34] The COVID-19 contact tracing applications carried a wide range of health-related data driven capabilities information sharing; self-testing; patients experiencing sharing; symptoms monitoring and contact tracing.

Zimbabwe adopted a ZimCOVID safe application for screening tool; general information on vaccination and testing centres information; and the short message service (SMS) based solution. The ZimCOVID application privacy policy stated that 'all data collected or shared (with you) is completely managed and stored by the ministry of health'. However, the actual type of information collected by the health ministry was not disclosed. On user registration, the application requested a mobile number.[35] For Zimbabwe, databases in the custody of public authorities are easily accessible.[36] And mobile network operators indiscriminately disseminated COVID-19 information.[37] The ZimCOVID application was able access to personal data on devices, and capable of modifying, deleting and reading the stored contents on device. The application was capable of preventing a mobile device from sleeping; can view network connections; and full network access.[38]

The collection of COVID-19 related medical data occurred before the passage of the CDPA, however other laws requiring the protection of personal data such as the Constitution, and the Public Health Act were in force. Due to the disaster declaration, public and private facilities were allowed to conduct tests in order to bolster government public health measures. As of 20 September 2021, Zimbabwe had officially approved 136 private testing facilities; 26 government laboratories; and 3 research, non-governmental facilities.[39] Retrospectively, the DPA, POTRAZ should consider procedures to address this, including asking data controllers to implement data destruction or data storage measures that safeguard privacy.

In most countries Zimbabwe included, all public facilities such as

[34] Foreign Affairs 'COVID-19 Isn't the Only Threat to Privacy' https://www.foreignaffairs.com/articles/2020-05-22/covid-19-isnt-only-threat-privacy (last accessed 11 April 2023)

[35] Reference to collection of personal data 'including but not limited to phone number' is purportedly for better application user experience, and that information is retained by the health ministry. https://dencroft.com/zimcovid-safe-app-policy (last accessed 11 April 2023)

[36] News Day https://www.newsday.co.zw/2018/07/zanu-pf-breaks-into-zec-database/.

[37] An urgent application was brought by Sikhumbuzo Mpofu against Econet Wireless network for unsolicited public notices on COVID-19, which Mr. Mpofu alleged were violating his rights including right to privacy.

[38] ZimCovidSafe Mobile Application Security Assessment Report. The assessment was conducted by a certified digital security expert on 10 September 2021.

[39] Health Professions Authority https://www.hpa.co.zw/admin/downloads/0-1632160057SARS-CoV-2%20REVISED%20LIST%20%20SEPTEMBER%202021.pdf (last accessed 12 November 2022)

supermarkets, banks, hotels were required to take temperature readings and record relevant personal information of clients.[40] For instance, Botswana required under Restrictions on Meetings, Societies, Gatherings that for purposes of contact tracing, a host must maintain a register containing the personal details and contact details of all persons accessing the premises. This information shall be open for inspection by the Director of Health Services for the purposes of contact tracing, and by law enforcement in the case of investigation of an offence under Emergency Powers.[41] The collection of personal data presented a huge risk to health-related data of consumers and the public as many of these public and private entities did not have the requisite training and infrastructure for confidentiality.[42] For Botswana and Zimbabwe the various statutory instruments declaring the pandemic, did not have any provisions of how the collected personal data was to be stored, and destroyed, and how DPAs or data controllers and processors were to conduct themselves.

4.2.2 COVID-19 data storage and destruction case of South Africa

Compared to Zimbabwe which had no DPA or DP law at the time of the declaration of COVID-19 disaster, South Africa had already enacted the Protection of Personal Information Act of 2013 (POPIA), with an independent and functional DPA, in this instance the Information Regulator (IR).[43] The IR oversight, appointment and removal is subjected to parliamentary processes.[44] As laws regulating the COVID-19 public health emergency are temporary, data protection mechanisms for health-related data need not be temporary. South Africa's data protection authority, IR issued guidelines articulating data processing parameters.[45] No other country in the SADC region had similar pronouncements. Even without data protection law or authorities, the ministries of health in all the countries acted as a sector specific public data controller responsible for other private and public data processors and must have issued health-related data processing guidelines concurrently with the public health standards and measures.

---

[40] This was done manually with basic thermometers, infrared temperature readings or mobile applications such as Quick Response (QR) codes or bar codes used to check in to venues, hospitals, public places.

[41] Botswana Government Gazette Directions for the Prevention of the Spread of COVID-19 – G.N. No. 301 of 2020; GN 302 of 2020; GN 303 of 2020

[42] A 9(3) of General Data Protection Regulation processing of health data for medical purposes under art 9 (2)(h) must be done by a professional who is bound by professional confidentiality.

[43] s39 establishment of IR; s41 appointment of IR under the Protection of Personal Information Act No. 4 of 2013.

[44] Section 40(1)(b)(iv); s41(2); s41(6) of Protection of Personal Information Act No. 4 of 2013.

[45] Guidance Note on the processing of personal information in the Management and Containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 of 2013.

South Africa introduced judicial oversight on the collection of personal health data under the COVID-19 application. The designated judge was supposed to receive weekly updates on the collection and usage of personal data and make directives for protection of privacy.46 In addition, the Disaster Management regulations that established a national COVID-19 Tracing Database containing the identification and contact information for all persons tested for COVID-19, and the details of known or suspected contacts of any person who tested positive for COVID-19, was supposed to destroyed within six weeks of the end of the State of Disaster. Furthermore, the database information must be anonymized, if to be retained for research purposes.

Despite the above clear framework, the IR as the data protection authority was unable to compel the National Department of Health (NDoH) to confirm that the information collected during the pandemic had been destroyed or archived with sufficient security measures confirmed by an expert third party information security firm. The NDOH was supposed to obtain a report from an information security firm confirming the measures undertaken, and this was also on recommendation of the designate judge. The NDOH defied a directive from the IR, compelling the escalation of the matter to the IR's Enforcement Committee issuing an enforcement notice equivalent to a court order.

4.3 Automated data processing

Through analysing personal data information technology has eased human roles in decision making accentuating risks of discrimination, bias and unfair decisions making to data subjects. The making of decisions that have an impact of significant nature or substantial effect from automated processes is not allowed in most DP laws, unless if there are exceptions, of a data subject allowing that, or appropriate measures are in place to protect data subject personal interests. The Zambian[47] and Mauritian[48] data protection laws, specifically define profiling as defined in the GDPR recital 71. The laws only differ on the use of personal aspects relating to a natural person (Zambia) and relating to an individual (Mauritius). The GDPR recital 71 define profiling means.

---

[46] Section 8(14) of the Disaster Management Act No. 57 of 2002 Regulations.

[47] ZDPA section 2, profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, including analysis or prediction of the data subject's aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

[48] Mauritian DPA section 2 means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements.

Section 62(1) of Zambia Data Protection Act and Mauritius Data Protection Act section 38(1) prohibits automated data processing which includes profiling that produces legal effects concerning data subject or significantly affects him or her.

The South African Law Reform Commission in its seminal report on Privacy and Data Protection described profiling in more helpful terms as where information which relates to an individual is structured in such a way that it can begin to answer questions about that person, so as to put his or her private behaviour under surveillance'. Further, profiling has two process components 1) profile generation and 2) profile application.[49] In most instances, profile generation is not harmful, as this is the case with most automated data processing systems. Profile generation becomes harmful when profile applied. Every bank has a customer profile, as part of Know Your Customer (KYC) based on personal data collected on a contractual basis for opening of bank accounts; customer banker relationship, but if the bank then uses that information to determine and decide the interests rates of a loan or to reject a loan application, this significantly affects the data subject. The bank must provide an explanation to the data subject, to remove concerns of bias. If the decision to reject a loan or high interest is communicated to a customer from an automated call centre, even with a human agent, this engagement might again be dictated by data produced assessment limiting the human agent to referencing computer generated responses. This human involvement is therefore immaterial and insufficient to provide justification and explanation.

These risks compels data controllers to seek authorisation or inform DPAs on automated data processing unless if exceptions applies. Under section 20(1) of Zimbabwe CDPA authorisation is especially required if there is a high risk of infringement of data subject rights and freedoms. Further, Zimbabwe CDPA section 23(1) mandates the DPA [Authority] to keep a register of all automatic processing operations. This register must be available for public inspection. The responsibility of the data controller in respect of automated data processing is to ensure that appropriate procedures for the profiling as well sufficient technical and organisational measures that reduce data inaccuracies, secure personal data, reduce and prevent, any bias or discrimination are in place.

[49] *South African Law Reform Commission Project 124 on Privacy and Data Protection (2009) 367- 368*

4.4 Breach notification or data leaks or security compromises

Data protection authorities are supposed to be notified of data breaches by data controllers. Under Zimbabwe's CDPA notification of security breach by the data controller must be notified to the DPA within 24 hours and similarly for Zambia,[50] which also expects data processors to notify data controllers within a reasonable time after noticing or discovering compromise. For Eswatini section 17, Lesotho section 23 and South Africa section 22 are similarly worded requiring that the notification should be as soon as reasonable possible after discovery without compromising legitimate law enforcement needs, and this notification includes to the data protection authority, and the data subject unless if identity cannot be established. Mauritius requires notification to be within 72 hours of data breach and the communication to the data subject must be without undue delay if there is a high risk to the rights and freedoms.[51] First, there are differences between the laws on how to handle notification of data compromises and breaches, including an assessment of whether risks are high for the data subject's rights and freedoms. This assessment must have established criteria to guide the data controller, and data processors, and developed by the data protection authorities. If there are standardised guidelines, the practices of DPAs in for instance when breaches occur across borders, the response protocols will be shared.

In the SADC region, only South African data controllers have disclosed security breaches.[52] This is not to suggest that there are no data breaches or compromises in other countries, it could be a number of reasons, including the secretive nature of the authorities, and also their complicit in some of the data breaches. In South Africa, the IR has been proactive in requesting data controllers to provide additional information whenever there is a data breach. For example, TransUnion Credit Bureau notified a security breach in March 2022, prompting the IR to request more details on 19 March 2022 of 'the date that the security compromise occurred, the cause of the security compromise, details of investigations into the security compromise, the extent and materiality of the security compromise, interim measures put in place to prevent a recurrence of the security compromise, and security measures that TransUnion Credit Bureau has put in place to prevent a recurrence of the security compromise'. [53] TransUnion Credit Bureau had indicated that 'at least three million customers

[50] ZDPA section 49(1) A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

[51] Mauritius Data Protection Act s 25 and 26.

[52] Mail and Guardian 'Five massive data breaches affecting South Africans' 19 June 2018 https://mg.co.za/article/2018-06-19-five-massive-data-breaches-affecting-south-africans/

[53] The Regulator instructs TransUnion to report in greater detail regarding their security compromise Media Statement, Information Regulator 19 March 2022

were impacted' despite the request for more details from the IR, the company was not cooperating, and another request for further particulars confirmed through a statement of 25 March 2022,

- Detailed description of the possible consequences of the security compromise and its impact on data subjects
- Advice and recommendations on the measures to be taken by the data subjects to mitigate the potential adverse effects of the security compromise.
- Description of the measures that TransUnion intends to take or has taken to address the security compromise".[54]

In addition to the above, the IR requested confirmation of a criminal report having been filed in terms of the Cybercrimes Act, Act No. 19 of 2020. The IR must be commended for taking a public stance on these matters, however there was no further disclosure of how the matter was resolved. The IR issued two statements or demands to TransUnion for specific action. Given the volumes, the 2022-2023 financial year the IR received eight-hundred and ninety-five (895) complaints and resolved six-hundred and sixteen (616) were resolved. This shows the importance of guidelines for the DPA on handling of complaints especially on breach notifications, and assessments guidelines.[55]

In Zimbabwe, every general election[56] period there are allegations of abuse of personal data through the sending of unsolicited campaign messages or the authorised disclosure of voter rolls in public domain. In 2018, the ruling party sent campaign messages to cell phone subscribers on Econet Wireless network, prompting citizens action and threats to take legal action against Econet and the Zimbabwe Electoral Commission (ZEC). The messages were personalised to the receiver, and therefore not bulk messages but direct and personalised campaigning. The messages was written in Shona translating to

"Cde [redacted], I am seeking your support [vote] to be President, Cde Mashavave for MP on elections to be held on 30 [July], ZANU PF values peace and progress"[57]

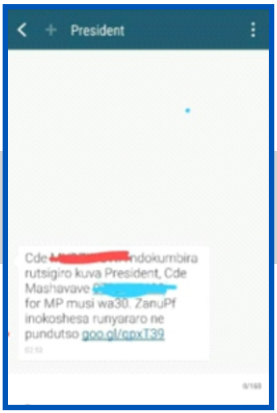
---

[54] The Regulator is dissatisfied with TransUnion's response, and it initiates an assessment on the security compromise. Media Statement Information Regulator, 25 March 2022.

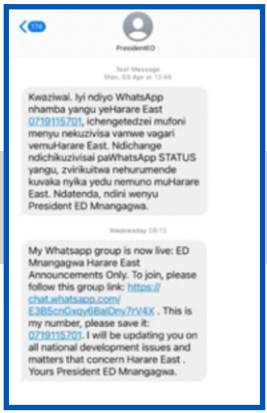
[55] Information Regulator shares outcomes of complaints investigated, and assessments conducted in relation to PAIA and POPOA Media Statement Information Regulator 5 April 2023

[56] Zimbabwe holds harmonised elections, which are presidency, parliament (house of assembly and senate), and local council (councillors).

[57] ZANU-PF Sending Personalised Messages To Individuals, Where Did They Get That Database? Electoral Commission And Econet Says Not From Them https://www.techzim.co.zw/2018/07/econet-denies-selling-customers-data-to-3rd-parties-refutes-zecs-allegations-so-who-sold-data-to-zanu-pf/ (accessed 14 April 2023)



Picture 1:
Screen shot (2018)
@TechZim



Picture 2:
Screen shot (2023)
@MISA Zimbabwe

On 12 April 2023, the Media Institute of Southern Africa (MISA) demanded POTRAZ, the dual data protection authority and telecommunications regulator to probe the flooding of unsolicited political short messages services by ZANU PF.[58] According to MISA, registered voters have started receiving messages on their mobile phones enticing individuals to President Emmerson Mnangagwa's WhatsApp group for specific constituency ahead of the 2023 general elections. No responses were received of MISA's complaints. There are few consistent patterns with these unsolicited and campaign messages. First, all of them are coming from the ruling party, ZANU PF. Second, the messages are not random by any imagination, as they are directed at a registered voter in constituency, and not just a mobile phone subscriber, this in 2018 included in the nominated House of Assembly candidate, and in 2023 only included a prospective ZANU PF presidential candidate.[59]

The 2023 messages further asks the data subject to subscribe for updates "on all national development issues and matters." While the sharing of national development issues or constituency issues is notable, this cannot be without an option to opt out from receiving the messages. In 2018, ZEC, network operators and POTRAZ distanced themselves from the messages, or and in 2023, POTRAZ ignored messages on how and why ZANU PF and President Mnangagwa acquired personal data. The denials and indifference from these 2018 and 2023 examples confirms that databases containing personal data in the custody of public and private bodies such as mobile network operators are easily accessed, and with impunity. This conclusion is damaging on Zimbabwe's DPA showing its political indifference to ZANU PF and government excesses, susceptibility to political manipulation, pursuit and safeguarding of elite interests, thereby general inability to provide adequate data protection and

[58] https://www.biometricupdate.com/202304/unsolicited-text-messages-to-zimbabwe-voters-raise-data-privacy-concerns (accessed 14 April 2023)

[59] The ZANU PF presidential candidate for 2023 had been confirmed in other different provincial meetings, and also when women, and youth assemblies met. Primary elections for house of assembly candidates were held in March-April 2023.

proof of ineffectiveness required for the free flow of data in country and across borders.

4.5 Lawful transfer of data across borders

Most instruments on data protection, either at national,[60] regional[61] or international[62] level has as one of its objectives the enhancing of cross border data transfers. The importance of cross border data flows increases with e-commerce and with globalisation seen as during the height of the pandemic as governments shared sensitive health data in an effort to combat the pandemic, while concurrently data subjects traded across borders, through online shopping. National laws have specific provisions allowing for cross border transfers. And as a matter of international practices, data flows are allowed in the under four specific instances. First, if there is consent, second if there is necessity (with or without consent), third where there are appropriate safeguards at data controller level (binding corporate rules or standard contract clauses) and fourth and last where there is an adequate decision that the country or international organisation is a safe data destination. The paper will not discuss the first three.

The countries reviewed have a cascading and mixed approval regimes on cross border flows, starting from blanket prohibition of flows, to flows only allowed to a country with adequacy or similar or substantial protection standards, and that even if there are no country safeguards, individual proposed data controller adequate safeguards are sufficient. The argument is that it is not sufficient to delegate the adequacy satisfaction to a data controller whose actual effectiveness is dependent on other country level factors such as national security interests, data localisation practices, and general state of the rule of law. In other instances, transfer is not prohibited, but the law starts with approval based on consent, standard contracts, approval by relevant minister,[63] or data protection authority. This is true of Zambia's provision under section 71 of the ZDPA. Countries also have separate provisions on data transfer for SADC and non-SADC states. For instance, Eswatini law section 32(1) provides that 'SADC member states must have transposed the SADC data protection

[60] This is true of some national laws such as South Africa as POPIA preamble specifically includes "to regulate the flow of personal information across borders of the Republic". Other laws, Zimbabwe, Lesotho, Zambia, Mauritius, eSwatini, and Botswana are silent on this being an objective or purpose of the data protection law despite further providing for cross border data transfers.

[61] The GDPR article 1(1) this Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

[62] The Council of Europe Convention on the Processing of Personal Data (Convention 108+); the OECD Guidelines on Data Protection

[63] The provisions of approvals by relevant minister for data transfers can easily be abused especially for national security matters.

requirements…'. The SADC Data Protection Model Law providing for data protection guidelines in the region is not binding, but also not clear if there is a specific provision being referenced as partial transposition or the entire model law as complete transposition. Partial transposition could also be in reference to a specific section only on data transfers, or complete transposition which is substantially similar to the entire protection provided under the data protection law.

4.5.1 Comparative data transfers provisions in SADC member states

Country	Provision	Stipulation
Botswana	49(1)	Without prejudice to s48 [The transfer of personal data from Botswana to another country is prohibited] and subject to provisions of this Act, the transfer of personal data that is undergoing processing or intended processing, to a third country may only take place if the third country to which the data is transferred ensures an adequate level of protection.
Eswatini	32(1)	Personal information shall only be transferred to recipient in [SADC] Member State that has transposed the SADC data protection requirements-
	33(1)	Personal information shall only be transferred to recipients, other than member states of SADC…if an adequate level of protection is ensured in the country of recipient and data is transferred solely to permit processing otherwise authorised to be undertaken by the controller.
Lesotho	52	A data controller in Lesotho shall not transfer personal information about a data subject to a third party who is in a foreign country unless (a) the recipient of the information is subject to a law, code of conduct or contract which effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles under this Act; and (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country
Mauritius	36(1)	A controller or processor may transfer personal data to another country where (a) he or it has provided to the Commissioner proof of appropriate safeguards with respect to the protection of the personal data; (b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate safeguards (c) the transfer is necessary…(lists the necessary exceptions).
South Africa	72(1)	A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless, (a) the 3rd party who is the recipient of the information is subject to a law binding corporate rules or binding agreement which provide an adequate level of protection (1) effectively

		upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information…(ii) includes provisions that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country…
Zambia	70(1)	A data controller shall process and store personal data on a server or data centre located in the Republic.
	71 (1)	Personal data other than personal data categorised in accordance with section 70(2) may be transferred outside the Republic where (a) data subject has consented and (i) the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commission or (ii) the Minister has prescribed the transfers outside the Republic is permissible…
Zimbabwe	28(1)-(2)	1) Subject to the provisions of this Act, a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out. (2) The adequacy of the level of protection afforded by the third party or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third party or recipient international organisation, the laws relating to data protection in force in the third party or international organisation in question and the professional rules and security measures which are complied with in that third party or international organisation.

The above provisions show different approaches to handing of cross border transfers, ultimately however, the information flows as these laws have exceptions, for instance, Zimbabwe section 29 provides for "a transfer or a set of transfers of data to a country outside Zimbabwe which does not assure an adequate level of protection may take place in one of the following cases", and then lists about six conditions that are acceptable for information to be transferred even without adequate country protection. The laws all include framing of some level of "adequate level of protection" (Eswatini, Botswana, Zimbabwe, South Africa) or "appropriate safeguards (Mauritius). Eswatini supposes that transfers will be to SADC countries that have transposed the SADC Law, Lesotho and South Africa adds that the conditions must be 'substantially similar to the conditions for the lawful processing of personal information and includes provisions that are substantially similar to the sections' approving transfers.

There framing of the cross-border transfer provisions in these laws clearly shows that there are different levels of transposition of SADC laws, and different challenges with cross border transfers provisions. Some of laws have a specific provision allowing the minister, 'responsible' for the law to designate or indicate which transfers are permissible as is the case of Zambia under section 71(1)(ii) or to give directions to the implementation of data transfers provisions as is the case with Zimbabwe under section 28(4). While this role appears very administrative in nature, it can actually impact on the ability of the DPA to fully function due to executive interference. Zimbabwe has an even more widely framed provisions which states that.

"Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe".

The Cyber Security and Monitoring Centre is an entity established under the Interception of Communications Act64, administered by the President as no minister has been given authority to administer the Act and, this centre is a unit in the presidency.65 The monitoring centre is the sole facility for authorised interception and oversees the Interception of Communications Act and its enforcement. Other laws allow the data protection authority to decide and determine the nature of data to be transferred even to a country not designated as providing adequate protection.66

The designation of a country as a safe destination does not necessarily mean that the laws are identical to one another. At the very least the laws must be substantially similar. This is open to interpretation and can lead to very wide and different applications. For a regional community, inclusion and exclusion of other countries as safe destination creates discord in the development of a regional economic community. It can also be an extremely subjective interpretation and assessment if there is no shared criteria.

4.5.2 Designation of countries for cross border data transfers: Case of Botswana

Through Statutory Instrument 95 of 2022 and in terms of section 48(2) of the Botswana Data Protection Act. First, as a matter of law, data transfers are prohibited under section 48 which states that "the transfer of personal data from Botswana to another country is prohibited'.

---

64 Interception of Communications Act of 2007.

65 Statutory Instrument 212 of 2018 Assignment of Functions (His Excellency the President of the Republic of Zimbabwe) Notice, 2018. The Interception of Communications Act however can be assigned to Minister of Communications or any other Minister to whom the President may assign. As of writing this paper, the Act is assigned to the President, therefore technically and administratively, the President is responsible for Cyber Security and Monitoring Centre as the Act is reserved for his administration.

66 Eswatini EDPA section 33(4).

Section 48(2) goes on to state that "notwithstanding the generality under subsection (1), the Minister may by Order published in the Gazette, designate the transfer of personal data to any country listed in such order". Based on this provision the Minister issued a list of countries that were designated for transfer of personal data. What is not clear is whether the designation is based on some criteria or purely on the basis of the ministerial discretion. This is because section 49(1) states that.

"without prejudice to section 48, and subject to provisions of this Act, the transfer of personal data that is undergoing processing or intended processing, to a third country to which the data is transferred ensures an adequate level of protection."

The determination of adequacy is based on an assessment by the Commissioner in light of all surrounding circumstances, and transfer to a country not providing adequate protection is prohibited under section 49(4) however exceptions under section 49(5) provided such as performance of a contract, public interest, or vital interest of data subject, and alternatively the Commissioner can approve transfer to a country that does not ensure adequate level of security safeguards.

The second observation is that the Ministerial Order designated 45 countries which are European Union and Council of Europe member states, and the UK, New Zealand, Israel, Japan, Isle of Man, Guernsey, Switzerland, Uruguay, Republic of Korea, Andorra, Argentina, the Faroe Islands, and Jersey. Only two African countries were listed South Africa, and Kenya with South Africa being the only SADC member state. There is only assumption of why these countries were listed, which is the adoption of the GDPR laws or its application for EU member states or the Council of Europe members to the Convention 108(+). South Africa and Kenya have adopted Protection of Personal Information Act, 2013 (POPIA) and Kenya Data Protection Act, 2019. The precedent set by Botswana creates challenges for data protection authorities at regional level and the development of a shared data economy and an integrated regional economic community:

- What are the reasons and grounds for the minister to designate other countries as destination and not, especially when leaving several other SADC and African states that already have data protection laws?
- What are the roles of DPAs is designing the assessment criteria to be followed for the designation of transfers to other countries, and does the ministerial designation constitute a confirmation of adequate protection.

The involvement of the executive in the implementation of the data protection law by the data protection authority which might be already compromised removes any doubt about the independence of the DPAs to supervise and enforce data protection law.

4.6 Digital identification systems (DIS)

According to the World Bank about 1.1 billion are without identification documents, with an estimated half being in Africa. The Sustainable Development Goal (SDG) 16.9 intends to ensure that everyone has legal identity including birth registration by 2030. To respond to this challenge, the World Bank launched an identification for development effort, though there are several challenges with the DIS. In most countries, there is a notable absence of comprehensive frameworks enforcing data subject rights and mitigating against abuse of persona data. Since DIS are based on large data sets and integrated systems, the abuse of data usually occurs through surveillance, profiling and attended discrimination. The combining of data sets, means data subjects have limited control and knowledge of how their information is being used, including inability to correct inaccurate data, and access personal data. In addition, due to the cross-border data transfers, DIS presents unique challenges of interoperability, enabling data subjects capacity to access services and enforce their rights across borders. This means that DPAs across regions, and borders must be capable of protecting transnational data subject rights. Furthermore, sufficient technical and organisational measures and safeguards are required to protect against unauthorised access. Data Protection Authorities must be involved and be aware of the many stages and steps of development of DIS. This means they have to be active or at the least aware of each data cycle point. From data capturing, DPA must enforce the principles of data collection such as purpose specification. On data hosting, credentials, and services, the DPA must be capable of enforcing the rights in the data protection law.

Globally, DIS has been touted as social protection solutions and access to services. For instance, in India the Aadhaar system is a 12 number identification issued to 1,3 billion people after collection of demographic and biometric information linked to personal data such as voter card, passport, driver's licence, bank account, utilities (electricity, gas) mobile phone, education and property. This integrated system presents major risks for data privacy even though it might be advancing other rights. [67] By their very nature, DIS are dependent on large data sets, within public and private sectors.

[67] The constitutionality of the Aadhaar system in protection of the right to privacy was challenged in Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others Writ Petition (Civil) No. 494 of 2012. The majority bench found Aadhaar to be constitutional with a few amendments. The court decided on the constitutionality by weighing privacy rights with other rights, finding that while privacy was important, the Aadhaar system advanced other rights such as dignity, and welfare, which were equally important.

[68] African countries are adopting digital identities systems as part of the development of digitialised services and a digital economy.

Zimbabwe has embarked on an integrated digital system project which according to the home affairs ministry will allow for issuance of 'national ID cards and biometric passports, register the birth of children, help security services monitor and track down criminals, and then also facilitate safe border crossings into the country'. [69] The integrated population registry system will connect major public data controllers such as the Zimbabwe Republic Police, Immigration, Registrar General, and Central Vehicle Registry and also it will connect to hospitals among others. This system according to the ministry will connect 'government ministries, departments, and agencies to enable them deliver different important services to Zimbabweans and other nationals living in the country'. First, there is no specific law articulating DIS in Zimbabwe as in many other African countries and the protection of digital identities is assumed to be included in data protection laws. Second, the creation of DIS falls within ministries such as home affairs and requires coordination with other ministries and departments.

In South Africa, a draft Official Identity Management Policy was published in 2020.[70] This draft shows the number of laws that are relevant for the creation of digital identities and the complexity which data authorities are required to navigate. These laws for South Africa include; Alteration of Sex Description and Sex Status Act 49 of 2003; Birth and Deaths Registration Act 51 of 1992; Citizenship Act 88 of 1995; Identification Act 68 of 1997; Immigration Act 13 of 2002; South African Passports and Travel Documents Act 4 of 1994; Refugee Act 130 of 1998; Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000; Electronic Communications and Transactions Act 25 of 2002; Promotion of Access to Information Act 2 of 2000; Promotion of Administrative Justice Act 3 of 2000; Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002; State Information Technology Agency Act 88 of 1998 among others. These laws are already authorising the collection of personal data, with public data controllers, and DIS will combine these data sets.

---

[68] Rubinstein SI 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 2 74.

[69] https://www.chronicle.co.zw/digital-integrated-system-to-revolutionise-access-to-government-services/ 6 April 2023.

[70] https://static.pmg.org.za/Draft_Official_Identity_Management_Policy_Version_with_Call_for_Comments.pdf (accessed 22 April 2023).

5. Concluding Observations

The paper has reinforced most pressing issues for data privacy and data protection authorities in Southern Africa. And as observed from literature and interviews, the laws and policies must be updated to answer to the many new emerging issues, not only issues such as big data, but as new issues will continue to emerge, and relevant laws will be required.[71] Again, the emerging issues might not be resolved by data protection laws only because data is implicated, this is the case with many of the emerging technologies such as the large language models (LLM) like ChatGPT. The existing challenges for data protection authorities means they are not singularly best placed to respond to these emerging issues, but they still have a critical role to play.

In most countries data protection authorities are faced with operational challenges including technical, financial and enforcement capabilities. These challenges in most instances stem in from the poor and weak enabling laws which do not provide sufficient independence to the DPAs. While the review and amendment of these laws is slow and impossible, Parliaments must insist on provision of adequate technical and financial resources to the DPAs. Furthermore, since most constitutions in SADC region provide for the right to privacy, which must be protected albeit limitations, DPAs must therefore report directly to Parliament as they are safeguarding constitutional rights; that is the right to privacy and right to data protection.[72]

The SADC has a non-binding model law on data protection, and as a region continues to lag behind in terms of developing an enforceable data protection regime. The model law has been under review, and one recommendation that must emerge from the review includes adopting a protocol on data protection in SADC, which includes a regional data protection authority, capable of assessing country laws for advancing an adequacy data region regime. The SADC Protocol on Data Protection must be automatically enforced by virtue of SADC membership and not open to ratification for existing members.[73] This will reduce the time required to enforce the protocol.[74] In addition, SADC must provide technical support to member states to allow for the alignment of laws with the new SADC Protocol on Data Protection.

The adoption of a SADC Protocol on Data Protection can be complimented by a more refreshed protocol on new technologies which seeks to create a robust policy framework that is more regulatory anticipatory than prescriptive. There are lessons from other economic blocs such as the EU touted as a leader in

[71] *Interview GS, 23 January 2023*

[72] *Only Mozambique includes data protection as a constitutional right.*

[73] *ECOWAS used an approach of a supplementary act to the ECOWAS Treaty removing the ratification requirement.*

[74] *These are lessons from the AU Malabo Convention which has taken long to be ratified and enter into force.*

technology regulatory practices and has seen a flurry of instruments in recent times, all aimed at addressing emerging challenges hence the EU Digital Services Act[75] or EU Artificial Intelligence Act[76] among others. These Acts will reinforce position of the EU as an influencer in regulatory processes and integrated economy driven by the protection of personal data from a human rights perspective and encouraging data sharing and cross border data transfers.

Cross border data transfers are increasing with the development of integrated and digital single markets (DSM). The regulatory environment is not responding with speed to enable an African or Southern African digital single market (DSM) that protects personal data across borders. A fragmented regional legal regime complicates regional market integration and undermines the usefulness of data transfers in a digital economy. The rapid ratification of trade agreements such as the African Continental Free Trade Agreement (AFCTA) demonstrates the importance of free movement of goods and persons, and data across borders. And in this regard, data protection authorities are essential to realisation of DSM not only from a trade perspective but enforcing the multidimensional aspect of data privacy, easily ignored trade conversations. The use of binding corporate rules (BCR) and standard contract clauses (SCR) mentioned in most data protection laws, is a short-term and very transactional in nature. However, as countries are moving to adopt digital identity systems or more robust digital economies, BCRs and SCRs are insufficient, as country risk are wider than single company or transaction certification. Holistic data protection based on adequacy determination and certification is ideal in advancing regional integration.

The cost of data breaches on companies is huge, and unfortunately the cost of individual privacy is hardly calculated. Absence of a culture of transparency and accountability, especially among public data controller means that, data breaches in African countries are not public. A few private data controllers have disclosed breaches in South Africa, but in other countries there is denial or total secrecy which feeds into the non-transparent conduct on many private data controllers. In addition, there is a general contempt and disregard for non-Western authorities especially by global technology private companies. The instruments at the disposal of global south, especially African DPAs is limited. The perceived or real limited economic and market interests in African

[75] Digital Services Act came into force on 16 November 2022. The DSA protects users and contest removal of content by platforms, provides for dispute resolution mechanisms, transparent terms and conditions for platforms; stronger obligations for large online platforms to assess and mitigate risks, protections for minors, bans on targeted adverts on online platforms directed at minors or using sensitive personal data among others.

[76] European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (accessed 23 April 2023)

countries by these private companies further reduces the opportunities for enforcement and limited jurisdiction.[77] Despite what is limited economic returns of African markets, this will change with Africa constituting the largest young population and many market opportunities.

Private companies are protective of their collected personal data for profit purposes, and this creates market distortions and unfair competition. Again, there are valid grounds that if this information is shared it constitutes misuse contrary to data principles, yet it is not stopping these companies from profiteering from the same personal data. These are valid reasons requiring the development of data trust sharing principles, which reduces the risk to the individual data subject, increases trust and transparency on data handling. Such rules however cannot be developed at country level at the very minimum they need to be developed a regional level to capitalise on combined market share and political influence.

As the value of personal and non-personal data has enormous social and economic potential, the current frameworks in many countries are insufficient to safely extract this value. The development of DIS will result in increased data sharing among public and private data controllers, and the massive personal data reuse to build the integrated systems. Ordinarily, the reuse of data for other purposes other than originally collected or without additional consent, or in the absence of a legitimate public interest is a violation. With digital identities, a more holistic and robust data governance framework is required, at the very minimum the various laws and policies must unequivocally address inclusion to respond to existing inequalities, incorporate robust and secure system design, and governance systems focused on building trust protecting privacy and user rights.[78] While these principles provide for an enabling policy framework, a regional cross-sectoral instrument such as the EU Data Governance Act is necessary. Such an instrument will regulate data reuse, increase secure and trustworthy data sharing, regulate the many data intermediaries and encourage data sharing for public purposes. The adoption of data governance act does not remove the need for robust data protection protocol at the SADC level.

---

[77] There are cases pending in African courts now against platforms companies like Facebook, in Kenya on Content Moderators Labour Rights, https://www.foxglove.org.uk/2023/03/24/facebook-sama-layoffs-redundancy-nairobi/ on in Ethiopia on the alleged complicit of Facebook in failing to remove materials that incited harm and violence in the Tigray conflict https://www.dw.com/en/facebook-owner-meta-sued-for-inciting-hatred-in-ethiopia/a-64085804 (accessed 23 April 2023).

[78] World Bank Principles on Identification for Sustainable Development: Towards the Digital Age (2017). Governments are adopting principles to address digital identities such as the UK government Identity Assurance principles which articulate about 9 principles essential for the establishment of secure DIS. These principles resonate with data privacy principles but are nuanced to digital identities. They are user control; transparency; multiplicity; data minimisation; data quality; service-user access and portability; governance/certification; problem resolution; and exceptional circumstances. https://www.gov.uk/government/consultations/draft-identity-assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles#commentary-on-the-context-of-the-principles (accessed 23 April 2023).

More than half of the SADC countries have adopted data protection laws. This is a progressive development. It creates an opportunity for development of regional network of African data protection authorities. At the global level, there is the Global Privacy Forum that brings together DPAs.[79] In Southern Africa, only South Africa and Mauritius are listed as Global Privacy Forum as accredited members as of April 2023.[80] As some DPAs in Southern Africa have dual roles like Zimbabwe and Eswatini, who are telecommunications regulators, they are already members of other networks in the region such as Communications Regulators Association Southern Africa (CRASA)[81], this could be a platform that can be activated to consider challenges of DPAs and dual roles. The institutionalisation of a regional network of DPAs could enhance collaboration, and coordination on transnational issues such as data transfers, enforcement of data subject rights, data sharing practices and data intermediaries.[82] Critical role of this network includes developing and designing regional guidelines on data transfers for instance and responding to newer challenges on data protection. In addition, a more coordinated platform for sharing lessons and opportunities is necessary, that in future could be the African or SADC data protection authority, with full regulatory and enforcement powers.

6.Recommendations

6.1 Public engagement and awareness

At a country level, DPAs must engage in public awareness and education. There are examples of Zimbabwe, South Africa DPAs engaging citizens on data privacy matters, however this might not be sufficient considering the capacity constraints faced by these institutions. In partnership with civil society, consumer interests groups such as consumer associations, the DPAs must produce public engagement materials and agendas simplified to explain the many technical aspects of data protection, and the data subject rights.

[79] From their website the Global Privacy Assembly first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The Assembly has been the premier global forum for data protection and privacy authorities for more than four decades. The Assembly seeks to provide leadership at international level in data protection and privacy. It does this by connecting the efforts of more than 130 data protection and privacy authorities from across the globe.

[80] https://globalprivacyassembly.org/participation-in-the-assembly/list-of-accredited-members/ (accessed 23 April 2023).

[81] 13 member states of SADC are part of CRASA with the exception of Seychelles, Mauritius and Comoros.

[82] The African Digital Rights Hub has been instrumental in providing a platform for African DPAs to meet during Africa Data Protection Summits. This needs to be institutionalised within African institutions such as SADC or the African Union.

6.2 Production of guidelines through consultation process

Data controllers and processors in most countries are deprived of sufficient guidance on critical matters. The DPAs must organise sector specific forums, which will enhance design and development of guidelines, such as for the banking, insurance, medical, and non-profit sector among others. More technical guidelines such as authorisation of processing of sensitive data or data transfers can be developed with DPAs leading. Most of the laws already provide for sector lead efforts in designing codes of conducts, however this has not commenced in most countries, or at the very least there is no publicly available information.

6.3 Coordination of multiple bodies and multiple laws

The DPAs are in some instances tasked with implementing two laws such as South Africa's Information Regulator overseeing PAIA and POPI concurrently, or Zimbabwe established as communicators authority with more than 15 other assignments, and additional tasks under the CDPA. Further, in most countries, other laws exist which are protecting data and might not necessarily be under the purview of the DPA. To exercise sufficient oversight of all these laws, DPAs must develop internal coordination protocols and processes with other bodies to allow for effective privacy protection, including how disputes, and complaints are resolved.

6.4 Regional platforms for coordination and lessons sharing.

SADC as bloc is one of the least integrated economic blocs and also one of the youngest comparatively. The adoption of a data protection protocol is necessary. This protocol must be forward looking and anticipatory of other and emerging challenges to reduce the review and revisions that slow down regional protocol development. The protocol must incorporate a regional data protection authority for development regional guidelines and cooperation.

MISA ZIMBABWE

KONRAD ADENAUER STIFTUNG