12 Independence of data protection authorities in Africa: Trends and challenges

Lukman Adebisi Abdulrauf

Abstract

The significance of a dedicated institutional framework for monitoring and enforcing the right to data protection cannot be overemphasised. Among the catalogue of human rights, it is one of a few with such privilege. This is not surprising, but considering the complexity of data processing, this has increased the need for a specialist oversight body. Almost all international data privacy instruments (now) require countries to establish these agencies. They further require that these agencies, generally called data protection authorities (DPAs), be independent. The African Union Convention on Cybersecurity and Personal Data Protection, for example, not only requires member states to establish DPAs but must ensure that they are 'completely independent'. Despite the significance of 'independence' in data protection law, understanding what it entails and achieving it seems complex, especially for African states. Therefore, the objective of this chapter is to consider the journey so far in applying the concept of independence of DPAs in Africa. The interlinked questions that the chapter seeks to answer are: to what extent have international principles on independence been implemented in Africa, and what are the trends and challenges, so far, in the application of the concept of independence of DPAs?

1 Introduction

The importance of data protection authorities (DPAs) to the overall realisation of the data protection project cannot be overemphasised. This is the reason why almost all modern data protection instruments require the establishment of such bodies. These instruments also grant DPAs with far-reaching powers in the processing of personal information by both public and private entities. Because of the nature and sensitivity of these enormous tasks they must perform, DPAs are required to be completely independent. Independence, therefore, has become a very critical concept under data protection law.[1] Despite some initial doubts, the inextricable link between independence and the effectiveness of a DPA seems to have

1 FH Cate and others 'The intricacies of independence' (2012) 2 *International Data Privacy Law* 1.

been firmly established today.[2] Independence, therefore, is very important for the effectiveness of a DPA because the very nature of their functions sometimes requires them to stand up against the powers of private entities and the government.

Africa is witnessing a significant renaissance in privacy and data protection and, as aptly put by Greenleaf and Cottier, '[n]ow it is Africa that is leading [the] global expansion [in data privacy], with 12 countries since 2013 adopting new laws'.[3] Over the past few years, many African countries, indeed, have enacted data protection laws and established DPAs.[4] Some of these DPAs are now fully functional, sometimes making bold decisions.[5] However, the peculiar nature of the continent, which includes the fragility of its democracies and the far-reaching powers governments wield, means that independent regulatory agencies will face peculiar operational challenges. This is especially true for DPAs designed to make far-reaching decisions against the interests of the powerful. Many factors in Africa exist to always undermine their independence. In determining the extent of independence, the first place to look to is the statutes establishing the DPAs, which are the data protection laws of a country. Since international standards are now tilting towards detailed provisions, one can safely assume that the more detailed a statutory provision on independence, the better for independence. This, however, is not to undermine the peculiarities of individual countries, which calls for a contextual application of the concept. As rightly mentioned by Cate and others, 'independence may also be viewed differently in different legal cultures'.[6]

The objective of this chapter is to examine the experiences so far on the independence of DPAs in Africa with a view to showing trends and challenges. Specifically, the chapter questions the extent to which international legal standards on independence have been adopted (and

2 G Greenleaf 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer Law and Security Review* 3.

3 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' (2020) *University of New South Wales Law Research Series* 3, http://classic.austlii.edu.au/au/journals/UNSWLRS/2020/32.pdf (accessed 1 September 2021).

4 Out of the 55 African countries, 36 have enacted data protection laws. See Data Protection Africa 'Mapping 55 African countries | 36 data protection laws | 3 draft laws https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf (accessed 3 March 2024).

5 Greenleaf & Cottier (n 3)7. Fifteen Out of the 32 countries with data protection instruments are yet to establish/appoint DPAs.

6 Cate and others (n 1) 1.

implemented) in data privacy instruments and legislation in Africa. This study is timely for two reasons. First, there has been limited comparative study on the application of independence of DPAs over the years.[7] Thus, it is important to carry out such study for Africa considering the pace of reforms in data privacy around the continent. Second, the study of the application of independence in countries other than established democracies may, according to Tarosova, bring new perspectives to the issue.[8] Therefore, Africa is an interesting case study in view of the sweeping wave of democratisation and constitutional reforms on the continent.

For purposes of this study, the term 'DPAs' will generally be used to refer to those public (or corporate) bodies that are responsible for overseeing or enforcing data protection norms. Furthermore, while Francophone African countries have been active in respect of data protection, this study focuses mainly on Anglophone Africa.[9]

2 International influence on the conceptualisation of 'independence' of DPAs

The determination of the meaning of the concept of independence of a DPA in data protection law is crucial for its proper application/implementation. Ordinarily, the concept implies a state of 'not [being] subject to control by others' or 'not requiring or relying on something else'.[10] However, in law, this concept arguably has a narrower connotation, for it is not realistic in a constitutional democracy to have that sort of absolute independence as anticipated by its literal meaning. Generally, applying the concept of independence in law anticipates that certain public institutions should be able to carry out their statutory functions free from political influence or interference. It is a concept that originated in the United States, and its purpose is to insulate public bodies from political

7 Greenleaf (n 2) 4. The most comprehensive so far are the works of Greenleaf. See Greenleaf (n 2) 3-13. Regarding the Asian-pacific region, see also G Greenleaf 'Independence of data privacy authorities (Part II): Asian-pacific experience' (2012) 23 *Computer Law and Security Review* 121-128.

8 E Tarasova 'Data protection authorities in Central and Eastern Europe: Setting the research agenda' in P Jonason and others *The right of access to information and the right to privacy: A democratic balancing act* (2017) 144.

9 This is because of the challenge of translation of laws from Francophone countries. Even where these laws have been translated, such translations are not so reliable considering that they are not the official copies.

10 See *Merriam-Webster dictionary* online, https://www.merriam-webster.com/dictionary/independent (accessed 1 September 2021).

interference of political parties.[11] With advances in applying the doctrine of separation of powers, the concept of independence has been associated with the operation of certain public bodies.

While the first attempt to understand the concept of independence was made by scholars, international instruments, no doubt, have shaped the current understanding and application of the concept.[12] The first set of international data privacy instruments, the Organisation for Economic Cooperation and Development (OECD) Guidelines on Protection of Privacy and Transborder Flows of Personal Data 1980 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) 1981, did not provide for an institutional framework for the enforcement of data privacy norms. Thus, there was no question of the need for their independence. Subsequent instruments of these two international organisations, however, provided for such bodies. For example, the OECD Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy (2007) established a Privacy Enforcement Authority (PEA) but did not mention the need for its independence.[13] According to Greenleaf, the United Nations (UN) General Assembly Resolution on Personal Data (1990)[14] was the first international text to not only provide for establishing an enforcement authority but also require such authority to be independent. According to the Resolution, such authority 'shall offer guarantees of impartiality, independence *vis-à-vis* persons or agencies responsible for processing and establishing data, and technical competence'.[15] Apart from the non-binding nature of the Resolution, which limited its influence, this provision does not give clear guidance on what the concept entails. Nevertheless, at least, it opened the gates to the recognition of what would eventually become one of the most significant characteristics of a DPA.

The subsequent entry into force of the European Union (EU) Directive in 1995 concretised the requirement of independence of DPAs. Article 28 not only required state parties to establish DPAs, but that such authorities shall act with 'complete independence' in carrying out their functions. According to Greenleaf, '[b]y stating that all these functions must be exercised with "complete independence"' the Directive makes

11 O Lynskey 'The "Europeanisation" of data protection law' (2017) 19 *Cambridge Yearbook of European Legal Studies* 257.

12 See works such as that of D Flaherty *Protecting privacy in surveillance societies* (1987).

13 For a more elaborate narrative, see Greenleaf (n 2) 3-13.

14 Guidelines for the Regulation of Computerised Personal Data Files, adopted by General Assembly Resolution 45/95.

15 Point 8 of the Resolution.

quite a strong statement about what "independence" means'.[16] The EU Directive, however, does not give details on the components of 'complete independence'. What may be gleaned from a plain reading of the provision is only an emphasis on sufficient powers for a DPA to make bold decisions and the fact that such decisions may be appealed in court. The ability to make bold decisions arguably is only a manifestation of independence and not necessarily a factor for independence. The only other provision regarding independence is Recital 62, which really adds nothing new to article 28. To consolidate the provisions of the Directive, the Charter of Fundamental Rights of the European Union (2000) not only recognised the right to data protection as a *sui generis* right but also provided that the right shall be enforced by an 'independent authority'.[17] No further details were provided as to what this independence entails. In all, the EU Directive, with its globalising effect, subtly induced other jurisdictions, including those of African countries, to make provisions on independence, sometimes without understanding the implications of the concept.

Since the EU Directive, subsequent reforms of data protection frameworks, especially in Europe, have taken note of the importance of legal provisions on independence and attempted to put finer details to it. Two such reforms are worth noting. The first is the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 (Convention 108+),[18] which provides for complete independence.[19] Further, the Convention only referred to the fact that in performing their duties, the supervisory authorities 'shall not seek or accept instruction'.[20] It is unclear where such potential instruction that could impact 'independence' would be coming from, but it is plausible that the Convention envisages instructions from the government. Other provisions that relate to independence are the obligation upon state parties to provide sufficient resources for supervisory authorities to exercise their powers and that the decisions of supervisory authorities may be subject to appeals through the courts.[21] The second reform in data protection is the

16 Greenleaf (n 2) 6.

17 Charter of Fundamental Rights of the European Union 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (accessed 1 September 2021).

18 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (accessed 1 September 2021).

19 Convention 108+ art 15(5).

20 As above.

21 Convention 108+ arts 15(6) & (9).

coming of the EU General Data Protection Regulation (GDPR),[22] which Hoofnagle and others have rightly described as 'the most consequential regulatory development in information policy in a generation'.[23] So far, it contains the most detailed provision on independence. Article 52 of GDPR specifically provides for 'independence'. According to GDPR:[24]

(1) Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
(2) The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
(3) Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
(4) Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.
(5) Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
(6) Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

From the above provision, one may draw some preliminary conclusions as to what the critical components of an independent DPA are. These are the ability to exercise their powers and function independent of external interference; the ability to act without external instructions, rule against engaging in incompatible occupations during their term in office; adequate human, technical and financial resources and infrastructures; the ability to

22 Regulation (EU) 2016/670 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 1 September 2021).

23 CJ Hoofnagle and others 'The European Union general data protection regulation: What it is and what it means' (2019) 28 *Information and Communications Technology Law* 66.

24 GDPR (n 22) art 53.

choose and control its staff; a separate budget but subject to a financial control mechanism of the overall state or national budget. Article 52 may have incorporated some of the key elements of independence, but arguably it is not exhaustive. There are other important elements that complement independence, but which are only provided in other provisions of GDPR. For example, certain qualifications/qualities go with members of the supervisory authority, such as their mode of appointment, tenure, qualification, and method of removal. Indeed, achieving independence is dependent on a combination of complex factors, key among which attach to the holder(s) of the office of the DPA. Without those stipulations protecting the sanctity of the holder of the office, there is no way of achieving independence in practice. It probably is in recognition of this fact that GDPR goes a step further than all other international instruments by making detailed provisions in this regard.

It must be stated that some of the requirements mentioned for the first time in GDPR are not entirely new. After a comprehensive review of international sources before GDPR (especially various resolutions of DPA networks), Greenleaf identified five attributes of independence that are most common and seven others that are less common.[25] These are:

(1) the establishment by legislation rather than any executive order or delegate legislation (firm legal basis);
(2) the ability to investigate and report free of direction or permission from any other political or government authority;
(3) a fixed term of office (commissioners should be appointed on a full-time basis);
(4) removal from office only for defined reasons (inability, neglect of duty or serious misconduct) with procedural safeguards;
(5) powers and duties to report directly on issues to either the parliament and/or the public.

The seven less common attributes identified by Greenleaf are the following:

(1) immunity against personal lawsuits relating to the performance of official duties;
(2) appointment by the legislature rather than the executive;
(3) resources of the DPA determined independently of the executive;
(4) positive qualification requirements for members/commissioners;
(5) prohibition on commissioners undertaking other concurrent positions;
(6) prohibition of appointment of commissioners from specified backgrounds that could cause a conflict of interests;

25 Greenleaf (n 2) 11.

(7) DPA decisions being subject to a right of appeal (to court).

The above succinctly explains what independence involves. As shown, independence in data protection law entails much more than what is ordinarily conceived. In my view, the attributes of independence can be broadly categorised into four groups. These are the attributes that go with functions and powers; mode of appointment and tenure and qualification of the office holders; adequate resources; and accountability. The attributes that go with the functions and powers of the DPAs include a stipulation that the DPA must be established by legislation;[26] freedom to exercise their powers without interference;[27] and immunity from lawsuits. The second category is that which relates to the mode of appointment and tenure. These include the provisions on the mode of appointment;[28] terms of office;[29] mode of removal;[30] and qualification.[31] In the third category are those attributes regarding sufficient resources. In this regard, there are specifications that protect DPAs from any form of control in terms of resources (financial or personnel), which invariably means that they need to have sufficient resources.[32] Finally, accountability provisions enable the powers of DPAs to be kept in check. They include provisions subjecting their finances to budgetary control,[33] and the right of appeal to courts against their decisions.[34] Accountability and transparency provisions are particularly useful, although they appear to add nothing substantial to an understanding the concept. According to Kuner and others,

> the principle of independence is more complex than it may seem at first glance. While independence is indeed an indispensable requirement for the work of DPAs, complete and total independence is never possible, or even desirable, on the part of any public authority. Principles of accountability and transparency require that a supervisory authority be answerable for its

26 GDPR arts 54(1) & 51(1).

27 GDPR art 52(1).

28 GDPR art 53(1).

29 See generally GDPR art 54(1).

30 GDPR arts 53(3) & (4).

31 GDPR art 53(3); see also art 52(3) which speaks of members not engaging in an action that is incompatible with their duties or engage in any incompatible occupation. This, arguably, constitutes 'serious misconduct' and could be a ground for dismissal under art 53(3).

32 GDPR arts 52(4) & 52(5).

33 GDPR art 52(6).

34 GDPR art 58(4).

actions (eg, through the possibility of judicial review), and that it be subject to controls in order to ensure its integrity.[35]

Considering that GDPR has incorporated most of these attributes in the four groups, one would expect that this will be the next international standard against which independence in data protection regimes of countries will be assessed. Indeed, the potential global reach of GDPR is not to be taken for granted, especially in Africa.[36] The next important question arises as to how the concept of independence of DPAs, so far, has been understood and applied in Africa.

3 Independence of DPAs in Africa

The application of the concept of independence is not new to Africa. Over time, certain statutory bodies have been established in some countries whose sole purpose is to promote democracy, and it is usually the requirement of the law that they should function independently. For example, in South Africa, these bodies, generally called 'institutions supporting democracy', are constitutionally established and bestowed with powers to promote transparency and accountability in governance.[37] The establishment of such bodies with the requirement of independence also finds support at the regional level with the African Charter on Democracy, Elections and Governance (African Democracy Charter), which requires state parties 'to establish public institutions that promote and support democracy and constitutional order'.[38] Importantly, there is an obligation on state parties to constitutionally guarantee the independence and autonomy of these institutions.[39] Can DPAs be considered part of such institutions that aim to support democracy?

35 Cate (n 1) 1.

36 AB Makulilo 'The GDPR implications for data protection and privacy protection in Africa' (2017) 1 *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 12-19.

37 The Constitution of the Republic of South Africa, 1996 ch 9.

38 African Charter on Democracy, Elections and Governance art 15, https://au.int/sites/default/files/treaties/36384-treaty-african-charter-on-democracy-and-governance.pdf (accessed 1 September 2021).

39 African Democracy Charter art 15(2).

In this part, the approach towards the independence of DPAs at the regional-wide level will be considered before a review of the approach in selected African countries.

3.1 Regional context on independence of DPAs

Although regional data protection instruments, so far, have not had a significant influence on DPA regimes in Africa,[40] it is important to consider how the concept of independence is treated at the continental and regional levels. The foremost regional instrument on data protection, the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), provides in article 11 that each state party 'shall establish an authority in charge of protecting personal data' and such authority shall be 'an independent administrative authority'.[41] To further buttress the need for independence, the Convention provides that a member of the authority should not be member of the government or a business executive who owns shares in businesses in the ICT sector.[42] This is as far the Malabo Convention goes in providing for independence. The Personal Data Protection Guidelines 2018 (Guidelines)[43] made pursuant to this Convention also do not add much flesh to the concept. While it recognises independence as a vital element for building truast online, it merely provides that a DPA is not likely to succeed in data protection 'if it can be subjected to undue political, administrative or commercial pressure'.[44] The Guidelines mention some examples of factors that can affect independence, including where the staff of a DPA 'are subject to undue political, administrative or commercial pressure'; where it is starved of sufficient enforcement powers and resources or subject to commercial lobbying or vexatious litigation.[45] While these are mere examples, they provide an insight into what the Guidelines consider important to gain independence.

Yet another continental-wide instrument that provides for independence is the Declaration of Principles on Freedom of Expression and Access to Information, which was prepared pursuant to article 45(1)

40 See AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 19.

41 Malabo Convention art 11(1).

42 Malabo Convention art 11(6).

43 Personal Data Protection Guidelines for Africa (Guidelines) 9 May 2018 21, https://iapp.org/media/pdf/resource_center/data_protection_guidelines_for_africa.pdf (accessed 1 September 2021).

44 Guidelines (n 43) 16.

45 As above.

of the African Charter on Human and Peoples' Rights (African Charter) and adopted by the African Commission on Human and Peoples' in 2019.[46] In its provision on data protection, the Declaration urges states to establish independent entities for the protection of communications and personal information.[47] Furthermore, it provides that such entities should include human rights and privacy experts.[48] The general limitation of this instrument is that it actually seeks to foster the right to freedom of expression, and data protection is only incidental to it. Therefore, it may be presumed that where the right to freedom of expression and data privacy come in conflict, freedom of expression will prevail.

Unlike the Malabo Convention, the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection, one of the binding regional instruments on the continent, makes a more detailed provision on independence.[49] In providing that member states shall establish their own DPAs, the Supplementary Act stipulates that they shall be an 'independent administrative authority'.[50] It further provides for qualifications of the members, which shall be in law, information communication technology and any other relevant field.[51] Members, according to the Supplementary Act, shall be incompatible with membership of government, exercise of business executives and ownership of shares in business in the information technology (IT) sector.[52] It is also provided that members shall enjoy full immunity; however, the immunity is limited to 'opinions expressed in the exercise of, or during the tenure of their function'.[53]

The next important regional instrument is the Southern African Development Community (SADC) Model Law on Data Protection.[54] It provides for the establishment of an independent and administrative

46 African Commission on Human and Peoples' Rights Declaration of Principles on Freedom of Expression and Access to Information in Africa, https://www.achpr.org/legalinstruments/detail?id=69 (accessed 1 September 2021).

47 Declaration of Principles (n 46) Principle 42(8).

48 As above.

49 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf (accessed 1 September 2021).

50 Supplementary Act (n 49) art 14(2).

51 Supplementary Act (n 49) art 15.

52 Supplementary Act (n 49) art 16.

53 Supplementary Act (n 49) art 17.

54 Southern African Development Community (SADC) Model Law on Data Protection, https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf (accessed 1 September 2021).

authority which 'implies a decision-making power independent of any direct or indirect external influence on the Authority'.[55] Similarly, 'the members shall remain independent from the influence of instruction of any other public authority'.[56] The Model Law provides for the competences of the permanent members. They must be competent in 'personal data protection, privacy or communication and information technologies'.[57] Arguably, this is a more focused provision regarding competence acknowledging the fact that specific expertise is needed to run such an office. Furthermore, the SADC Model Law provides for the term of office[58] and the mode of removal of members of the DPA.[59] Finally, members of the DPA are granted immunity from views expressed in the execution of their duties.[60]

African regional instruments contain rather instructive provisions regarding independence, even though still incomparable to the detailed provisions of GDPR. For example, all these instruments fall short in making provisions on the mode of appointment and the need for adequate resources of DPAs. In view of the centrality of these elements to the realisation of independence, their omission indeed is a clear flaw at the regional level. In conclusion, most of the regional instruments are independent initiatives with little or no connection to one another. They have, so far, had minimum impact at the domestic level.

3.2 Overview of the legal framework on 'independence' in selected countries

As mentioned, Africa is gradually becoming home to one of the fastest-growing data privacy regimes in the world. Based on the latest comprehensive study on Africa, there so far are 36 countries with data privacy legal frameworks in place.[61] However, only about 16 of these have some sort of institutional framework for the enforcement of data privacy law. In this part I analyse the laws establishing some of the DPAs to show the nature and scope of the provisions on independence. To carry out this analysis, the approach of African countries in terms of statutory design can be broadly categorised into three (or four): the minimalist, moderate and robust. A fourth category is the extreme. Accordingly, regimes in the

55 SADC Model Law (n 54) sec 3.
56 SADC Model Law (n 54) sec 3(11).
57 SADC Model Law (n 54) sec 3(4).
58 SADC Model Law (n 54) sec 3(8).
59 SADC Model Law (n 54) sec 3(9).
60 SADC Model Law (n 54) sec 3(10).
61 Data Protection Africa (n 4).

robust category are countries with data privacy frameworks that provide for most of the international data privacy standards on independence contained in GDPR. The minimalist countries merely provide for independence without no elaboration of its basic attribute. The moderate falls in between both. At the extreme end are countries that do not even provide for independence at all or do not have a separate supervisory body for data protection.

South Africa arguably has the most elaborate incorporation of the international principles on independence in its Protection of Personal Information Act 2013 (POPIA).[62] Although POPIA was largely tailored along the lines of the EU Directive, it contains many modern principles of GDPR.[63] The Act establishes the Information Regulator (IR) to supervise data privacy and access to information.[64] POPIA was explicit where it provides that the IR shall be 'independent and is subject only to the Constitution and to the law'.[65] This indeed is one of the most instructive stipulations on the legal basis. POPIA also provides that the IR must 'be impartial and perform its functions and exercise its powers without fear, favour and prejudice'.[66] In terms of POPIA, the IR can receive and investigate complaints free from any sort of external influence.[67] Similarly, the Regulators are appointed by the President on the recommendation of the National Assembly. They are also appointed for a fixed term of not more than five years and may be eligible for reappointment.[68] According to POPIA, they 'must be appropriately qualified, fit and proper persons'.[69] POPIA provides clearly defined reasons for removal from office, which include misconduct, incapacity and incompetence.[70] It also stipulates the procedure for the removal, which must be based on a finding by a committee of the National Assembly and supported by a

62 Protection of Personal Information Act 4 of 2013 (POPIA), https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf (accessed 1 September 2021).

63 For more in-depth analysis of this, see A Roos 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African data privacy law: An evaluation of selected content principles' (2020) 53 *Comparative and International Law Journal of Southern Africa* 1-37.

64 POPIA, long title of the Act and sec 39.

65 POPIA sec 39(b).

66 POPIA sec 39(c).

67 POPIA sec 40(1)(d).

68 POPIA sec 41(2)(a).

69 POPIA sec 40(1)(b).

70 POPIA, sec 41(6).

resolution.[71] To further buttress its independence, it is explicitly provided that the IR is accountable to the National Assembly[72] and it can report directly to Parliament and the public.[73] Other provisions to guarantee its independence are the provision on immunity against personal lawsuits while performing its official duties; funds and resources of the Regulator being determined by Parliament independent of the executive;[74] and the prohibition on the appointment of regulators from certain backgrounds that could bring about a conflict of interest.[75]

While the South African POPIA arguably provides for most of the international principles on independence, there are certain provisions that could impact independence. For example, the Regulator appointed full-time cannot perform any other remunerative work during the period he/she holds office except with the prior written consent of the Minister.[76] This provision subjects the Regulator to the executive as the Minister, in this case, is the cabinet member responsible for the administration of justice, who is a core member of the executive. Another curious provision that could impact independence is the requirement that the Regulator must consult the Minister of Finance in the exercise of its powers of appointment of staff.[77] While this may be justified on grounds of budgetary and financial planning purposes, it could be a conduit for more executive control of the IR. Nevertheless, this provision is in accordance with GDPR, which anticipates that the DPAs must be subject to relevant budgetary control from the appropriate government ministry.[78] However, perhaps this should be done in such a way as not to affect its independence.

Kenya belongs to the moderate category in the treatment of independence in the Data Protection Act 2019. It provides that the Data Commissioner shall act independently in the exercise of its powers.[79] The Act contains at least many of the key components of GDPR. The office of the Data Commissioner is established by statute as a state office in accordance with the Kenyan Constitution.[80] It can receive and investigate

71 As above.

72 POPIA sec 39(d).

73 As above.

74 POPIA sec 52.

75 POPIA secs 41(1)(g) & 45.

76 POPIA sec 41(1)(e).

77 POPIA sec 47(5).

78 GDPR art 52(6).

79 Kenya Data Protection Act 24 2019 sec 8(3).

80 In accordance with sec 260(q) of the Constitution of Kenya 2010. See Kenya Data Protection Act sec 5.

complaints.[81] The Commissioner is appointed by the President with the approval of the National Assembly[82] for a fixed term of six years[83] and can only be removed from office on clearly defined grounds.[84] The challenge with respect to the grounds of removal is a lack of clarity with regard to terms such as 'incompetence' or gross misconduct. This, indeed, is a general challenge with even GDPR, and all will depend on a careful interpretation by the courts. The Commissioner enjoys immunity from personal lawsuits.[85] The major challenge to independence of the Commissioner is the fact of the prominent role the Public Service Commission plays in its administration, which ordinarily is a key executive body. In terms of the Act, the Public Service Commission plays a key role in the appointment of the Commissioner[86] and other member of staff of the Officer.[87]

Ghana's approach falls within the minimalist category regarding the substance and details on independence. The Ghanaian Data Protection Act 2012 is centred around the Data Protection Commission. It has the power to investigate any complaint in a manner it considers fair, anticipating some sort of independence.[88] Unlike the South African and Kenyan approaches, the Ghanaian regime has many provisions that question the requirement of independence. The Board is the primary policy-making arm of the Commission, and it comprises members who are part of the executive branch, such as representatives from the National Communications Authority and Ministry of Communications.[89] The President appoints the members of the Board without any form of consultation.[90] The same goes for the appointment of the Executive Director who is appointed solely by the President.[91] The Executive Director shall hold office 'on terms and conditions specified in the letter of appointment'.[92] More disturbing is the explicit provision on the ministerial directive which is to the effect that the Minister may give directives to the Board on matters of policy.[93] The

81 Kenya Data Protection Act sec 8(f).
82 Kenya Data Protection Act sec 6(3).
83 Kenya Data Protection Act sec 7(2).
84 Kenya Data Protection Act sec 11(d).
85 Kenya Data Protection Act sec 17.
86 Kenya Data Protection Act sec 6.
87 Kenya Data Protection Act sec 13.
88 Ghanaian Data Protection Act sec 3(c).
89 Ghanaian Data Protection Act sec 4(1).
90 Ghanaian Data Protection Act sec 4(2).
91 Ghanaian Data Protection Act sec 11(1).
92 Ghanaian Data Protection Act sec 11(2).
93 Ghanaian Data Protection Act sec 10.

executive also seems to be in control of the funds of the Commission in terms of the Act as sources of funds *inter alia* include 'money approved by the Minister responsible for Finance'.[94] Perhaps it is no coincidence that that law never made any specific mention 'independence' of the Commission.

The Mauritius DPA is another regime that falls in the minimalist category. However, unlike the Ghanaian Data Protection Act, there is a clear stipulation on independence without the necessary details in its Data Protection Act 2017. The Act provides that '[t]he Office shall act with complete independence and impartiality and shall not be subject to the control or direction of any other person or authority'.[95] It also provides for the right of appeal to a tribunal from the decision of the Commissioner.[96] This is all it provides regarding independence, which is rather surprising considering that the Act is one of the most recent data protection laws on the continent. Makulilo was unequivocal with regard to the Mauritius Data Protection Act when he observed that

> [o]ne shortcoming of the Data Protection Act is that, it does not clearly state to whom the Data Protection Commissioner is accountable to. He is only required to lay an annual report of the activities of the DPO before the National Assembly. Arguably, this leaves a lot to be desired in terms of the security of tenure of the Commissioner and may compromise the principle of independence. The same is true with regard to the financial independence of the DPO. The Act does not state where the budget of the Office comes from and how its availability is guaranteed without putting the independence of this Office under the mercy of administrative authorities.[97]

Tunisia is also an interesting case where the Organic Act 2004-63 on the protection of personal data only recognises financial independence of the *Instance Nationale de Protection des Donn es Caract re Personnel* but still went on to provide that 'the budget of the office is attached to the Ministry of Human Rights'.[98] It also scantily prohibits the President and members of the *Instance* from holding any interest in organisations relating to personal data processing.[99]

94 Ghanaian Data Protection Act sec 14.

95 Mauritius Data Protection Act sec 4(2).

96 Mauritius Data Protection Act sec 51.

97 AB Makulilo 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25 *International Journal of Human Rights* 133-134.

98 Organic Act 2004-63 of 27 July 2004 on the Protection of Personal Data art 75.

99 Organic Act (n 98) art 78.

Uganda is an example of a country at the extreme end of the continuum. Its Data Protection and Privacy Act 2019, made no provision for independence. This is not surprising considering the controversial type of democratic regime that holds sway in the country. The only semblance of provision for independence is the requirement that on the personal character of the director, who shall be a 'person of high moral character, proven integrity and with relevant qualifications and experience'.[100] This stipulation, again, arguably is too vague. The Uganda Data Protection and Privacy Act also leaves a lot regarding the appointment of the National Data Protection Director, who is the head of the Personal Data Protection Office, to be determined by his/her instrument of appointment.[101] Indeed, such an 'instrument of appointment' can contain all sorts of conditions that will undoubtedly affect independence. Still in the category of recent laws that do not give credence to the requirement of independence is the Zimbabwean Data Protection Act, which never made any provisions regarding independence.[102] More surprising is the fact that it mandates data controllers to appoint data protection officers 'charged with ensuring, in an *independent manner,* compliance with the obligations' contained in the Act.[103] It is, therefore, strange that the Act requires independence for data protection officers of data controllers but not for the DPA.

From the above, it is clear that African countries need to do much more with regard to designing and implementing provisions on independence of DPAs. South Africa is one of the few countries with carefully-considered provisions, and it is hoped that this provision is sincerely implemented in practice.

4 Trends and challenges towards 'independence' of DPAs in Africa

The independence of a DPA, no doubt, is critical for the effective protection of the right to data privacy.[104] Data protection law, therefore, takes this requirement very seriously. The above analysis of the approach of African countries reveals that many countries have not paid close attention to the

100 Uganda Data Protection and Privacy Act 2019 sec 4(1).

101 See, e.g., Uganda Data Protection and Privacy Act 2019 secs 4(2) & (4).

102 Data Protection Act, No 5 2021, Available https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf (accessed 1 September 2021).

103 My emphasis. See sec 1, Zimbabwe Data Protection Act, 2021.

104 See T Davis 'Data protection in Africa: A look at OGP member progress' https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf (accessed 1 September 2021) 50.

technicality involved in the couching provisions on independence and its overall implication for independence in practice. In this regard, it is arguable that just the South African law makes a noteworthy provision on independence in terms of comprehensiveness. The point, however, must be re-emphasised that mere comprehensiveness of the provisions does not automatically translate into independence in practice. However, it is a first and, indeed, critical step towards attaining independence in practice especially for African countries. This part will now analyse some of the trends and challenges toward attaining the independence of DPAs in Africa. Since the experience of data protection on the continent is relatively nascent, the part will sometimes draw lessons from the experiences of other statutory bodies that are established to be independent in Africa.

Although the spread of data protection in Africa is rapid, there a general lack of appreciation of its intricacies.[105] The level of awareness of what is involved remains low and this could have a spiral effect on the extent of implementation.[106] Data protection is a technical aspect of law, and some level of expertise is needed to interact with this law. So far, while many African countries have adopted data protection legislations, many of these do so for purposes other than the realisation of human rights. For example, scholars have acknowledged the fact that the level of influence and the globalising effect of the EU regime is what has invariably forced many countries, especially in Africa, to adopt data protection laws.[107] If African countries do not appreciate the value of this subject, it will be difficult for them to sincerely establish supervisory agencies and grant them independent powers to function effectively. To justify this, it is easily noticeable on the continent that while many African countries have enacted data protection legislations, very few have established independent supervisory authorities and even fewer have these authorities already fully operational.[108]

105 See generally LA Abdulrauf 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms' (2021) 30 *Information and Communications Technology Law* 87-107.

106 See generally LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

107 Makulilo (n 40) 19.

108 T Ilorin 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solution' 1, https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf (accessed 1 September 2021).

Apart from the lack of a sufficient understanding of the intricacies of privacy, which is manifested by the lack of political will to faithfully implement data protection standards, there also is the challenge of a shortfall in expertise to draft data protection laws. As earlier mentioned, data protection law is complex and there is a need for expertise. This expertise involved is not limited to a quality understanding of what the law involves, but also the ability to be able to track and transpose international development and standards in the law. In drafting the South African POPIA, the expert committee made an effort to track international development and ensure that this was reflected in the law. For example, the expert group carefully monitored the processes and discussions on GDPR even before it became fully operational.[109] Sufficient time was taken to develop a law that would stand the test of time. This is why the South African POPIA remains one of the continent's most detailed and carefully considered data protection instruments. Of course, this fact is vindicated by the nature and scope of the provisions on the independence of the Information Regulator considered above. The data protection laws of many other African countries contain very scanty provisions. This is even true for laws that were enacted after the entry into force of GDPR, such as the data protection law of Uganda. The Zimbabwe Data Protection Act is another example. In the Act, the powers of the Data Protection Authority are to be exercised by the Postal and Telecommunications Regulatory Authority.[110] It is difficult to speak of independence with this kind of arrangement, and such an approach speaks to the lack of a sufficient understanding of the intricacies of data protection.

A manifestation of the lack of expertise that may impact provisions establishing DPAs in Africa is the trend towards appointing the heads or members of the supervisory authority just from any legal background and sometimes from the civil/public service without necessarily having expertise in data protection. As was mentioned in the previous part, the qualifications of members of the supervisory authority form part of independence. GDPR requires that 'each member shall have the qualifications, experience and skills, *in particular in the area of the protection of personal data*'.[111] In South Africa, the requirement of POPIA is that members of the Information Regulator 'must be appropriately qualified, fit and proper persons', which is understood, among others, as being experienced as a practising advocate or attorney or a professor of law at

109 See P Stein 'South Africa's EU-style Data Protection Law' (November 2012) *Without Prejudice* 48, https://journals.co.za/doi/pdf/10.10520/EJC128763 (accessed 1 September 2021).

110 Zimbabwe Data Protection Act, 2021.

111 GDPR art 53(2) (emphasis added).

a university.[112] Similarly, the Mauritius Data Protection Act provides that to qualify as a commissioner, the person must be a lawyer with at least five years' standing at the bar.[113] It is submitted that these backgrounds (or even a background in law specifically) do not necessarily make them experienced in data protection, which, as was earlier noted, is a technical field requiring specific expertise. The approach of the Kenyan DPA seems to be preferable because it provides that the Data Commissioner should hold a university degree in data science, law, information technology or any other related field.[114] Although a law degree is required, it mentions other specialisations showing the technical and specialist experience. Though this may sound slightly ambitious, it is important that members of the DPA at least have some experience in data protection in addition to a legal background.

Obviously, the way in which provisions establishing DPAs are drafted goes a long way towards providing a platform for independence. A mere superficial provision does no good to the realisation of independence and could be a significant obstacle to achieving independence. In my view, this shows the extent of seriousness toward data protection on the continent. It must again be emphasised that the implementation and enforcement of these laws are another issue. Therefore, no matter how detailed a provision is on independence, the absence of political will to ensure its faithful implementation will always constitute a formidable challenge. Here, the disconnection between *de facto* and *de jure* independence is evident. Commentators have argued that legislations sometimes establish DPAs and claim they are independent, but such independence is only on paper.[115] Indeed, Africa is seen as a region with rules and no real policing.

Yet another factor which may be a challenge to realising independence of DPAs in Africa is the general distrust by the African political class towards independent regulatory authorities. Though not supported by firm empirical evidence, these politicians make every effort to frustrate such bodies as shown in the experience with similar bodies like electoral commissions and anti-corruption agencies.[116] This is especially true for countries with questionable democratic credentials, as even the judiciaries

112 POPIA sec 41.

113 Mauritius Data Protection Act sec 4(4).

114 Kenya Data Protection Act sec 7.

115 Davis (n 104) 50.

116 See generally CM Fombad 'The role of hybrid institutions of accountability in the separation of power scheme in Africa' in CM Fombad (ed) *Separation of powers in African constitutionalism* (2016) 325-344.

in such countries struggle to maintain their independence. This view was expressed Kuda Hove in a recent study that:

> [t]here's this general distrust in having independent institutions in Africa. There is that distrust in having independent institutions in Africa. There is that distrust [that] if we grant them true autonomy, if we give then independence, they might turn against us in the future, that's sort of the feeling that governments have. So, to manage that fear, governments will then undermine their independence.[117]

A manifestation of this distrust is that while some countries have established DPAs, they still ensure that they are made an integral part of a government ministry. The Ghana Data Protection Commission is one of many examples. With such an arrangement, there is no way that the DPA can achieve independence. Another infamous example is that of Uganda. The Data Protection and Privacy Act clearly provides that the personal data protection office shall be 'under the Authority which shall directly report to the Board'.[118] The Authority in this case is the National Information Technology Authority which is a key executive body. This used to be the case in Nigeria until 2023, when the Data Protection Act was enacted. The Nigerian Data Protection Regulation (NDPR), which was made by the National Information Technology Development Agency (NITDA) was implemented by NITDA (and subsequently the Nigeria Data Protection Bureau) which is one of the key agencies of government established under the Ministry of Communications and Digital Economy.[119] The idea that data protection is just a mechanism toward advancing technology in a country and, therefore, subsuming the mandate of the supervisory agency under a government ministry is no good for the realisation of independence. Without structural independence, achieving independence of DPAs will only continue to remain a mirage. GDPR was unequivocal in this respect where it provides that the supervisory authorities must 'remain free from external influence, whether direct or indirect, *and shall neither seek nor take instruction from anybody'*.[120]

The broad functions DPAs are expected to perform mean they need adequate resources. Independence also means that DPAs have sufficient manpower and financial resources. This a big challenge that many DPAs are facing in Africa. For example, in a recent status report before the National Assembly, the Information Regulator of South Africa complained

117 As above.

118 Uganda Data Protection and Privacy Act sec 4(1).

119 'Mandate', https://nitda.gov.ng/mandate/ (accessed 1 September 2021).

120 GDPR art 52(2).

of limited funds. In fact, she further complained of lack of a permanent office space.[121] Similarly, it was reported that in the 2018/2019 financial year, the South African Information Regulator had to work with a budget of R27 Million, which was the same amount expected in the next financial year when the Regulator is supposed to be fully operational.[122] Besides, the Regulator must also combine the task of overseeing the enforcement of the POPIA with the Protection of Access to Information Act.[123] According to Adam and Adeleke, this is a 'woefully low budget' compared to similar independent institutions such as the South African Human Rights Commission.[124] The Mauritius Data Protection Commissioner also made a similar remark regarding insufficient human resources, which could impede the effective enforcement of the Data Protection Act. According to the Data Protection Commissioner, 'one longstanding problem faced by this office is the severe insufficiency of human resources, which inevitably hampers the efficiency of service delivery'.[125] This comment was made in the 2018 report. Unfortunately, this situation remained the same as reported in 2019. According to the Data Protection Commissioner, '[o]ur last annual report 2018 showed how this office struggled to meet service delivery due to a severe shortage of human resources. In 2019, the situation worsened since our workforce was reduced by two for better career options.'[126]

Financial independence, no doubt, is key to achieving real independence. In Africa, governments have used control over finances to undermine the independence of statutory bodies, and this situation cannot be totally ruled out with regard to DPAs. In this regard, subsuming DPAs into ministries will pose a challenge to financial independence. According to Gbenga Sesan, '[i]f you get your money directly from the

121 SA Human Rights Commission Annual Report; Information Regulator Status Report, https://pmg.org.za/committee-meeting/25227/ (accessed 1 September 2021).

122 R Adams & F Adeleke 'Protecting information rights in South Africa: The strategic oversight roles of the South African Human Rights Commission and the Information Regulator' (2020) 10 *International Data Privacy Law* 157, citing Dommisse Attorneys 'POPI News: Appointment of the Information Regulator' 7 November 2016, http://dommisseattorneys.co.za/blog/popi-news-appointment-information-regulator/ (accessed 1 September 2021).

123 As above.

124 As above.

125 Makulilo (n 97) 18, citing Data Protection Office Annual Report 2018.

126 Data Protection Office Annual Report 2019 9, https://dataprotection.govmu.org/AnnualReports/DPO%20Annual%20Report%202019.pdf (accessed 1 September 2021).

national budget, you have more power. If you get your money from the ministry, you have no power.'[127]

The absence of a specific data protection supervisory body at the regional level may also have direct or indirect implications for the establishment and guarantee of independent DPAs. Looking at the structure that exists in the EU, it will be seen that the role of the supervisory agency at the regional level, the European Union Data Protection Supervisor (EDPS),[128] is significant in pushing for independence at the domestic level.[129] Similarly, the newly established European Union Data Board (EUDB) is responsible for regional harmonisation and has proactively led DPAs in the EU toward effective data protection enforcement.[130] The office of the supervisor has been proactive in ensuring that member states fulfil their obligations under GDPR. There are numerous cases initiated or supported by the EDPS member states for not complying with provisions on independence. For example, in cases such as *Commission v Hungary*[131] and *(Grand Chamber) European Commission v Republic of Austria*,[132] member states were brought

127 Quoted from Davis (n 104) 53.

128 EDPS 'About us', https://edps.europa.eu/about/about-us_en (accessed 1 September 2021).

129 L Jančiūtė 'European Data Protection Board: A nascent EU agency or an "intergovernmental club"?' (2020) 10 *International Data Privacy Law* 57-75.

130 See A Giurgiu & TA Larsen 'Roles and powers of national data protection authorities' (2016) 2 *European Data Protection Law* Review 342-352. See also EDPB 'Who we are', https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en (accessed 1 September 2021).

131 Case C-288/12 *Commission v Hungary* ECLI:EU:C:2014:237 8 April 2014, also available online at European Union Data Protection Supervisor (EDPS). In brief, the decision of the Court with regard to independence was that 'by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data, Hungary has failed to fulfil its obligations under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data'.

132 See Case C-614/10, CJEU (Grand Chamber) *European Commission v Republic of Austria*, 16 October 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62010CJ0614&from=EN (accessed 1 September 2021). Briefly, the Court was of the view that by failing to take all measures necessary to ensure that the legislation in force in Austria meets the requirements of independence with regard to the Data Protection Commission, more specifically by making a regulatory framework that makes the Data Protection Authority integrally linked to the Federal Chancellery, the Republic of Austria has failed in its obligations under art 28(1) of the EU Directive which requires 'complete independence' of DPA. For a more in-depth analysis of this decision, see A Balthasar 'Complete independence of national data protection supervisory authorities – Second try: Comments on the judgement of the CJEU of 16 October 2012, C-614/10 (*European Commission v Austria*), with due regard to its previous judgment of 9 March 2010, C-518/07 (*European Commission v Germany*)' (2020) 9 *Utrecht Law Review* 26-38.

before the Court of Justice of the EU for failure to comply with the requirement of independence. Although the nature of supranationalism that exists under the African Union (AU) is incomparable to that of the EU, a regional data protection body will go a long way towards assisting state parties. While the AU Commission is making some effort to be this regional body,[133] such effort cannot be compared to having a body that focuses on data protection alone.

Still within the regional context, networks of data protection authorities have been instructive in expanding the understanding of independence. They do this by having certain accreditation requirements for DPAs of member states. While there is one such network in Africa, the Network of African Data Protection Authorities, it appears that they have not developed an accreditation criterion. The website of the network merely provides that its membership is limited to 'data protection authorities in states which have adopted legislation on privacy and data protection'.[134]

It needs not be gainsaid that achieving independence in typical African countries will be a struggle for several reasons. Even in Europe where the concept seems to have developed, it constantly is under threat.[135] However, African countries present peculiar challenges, as mentioned above.

5 Conclusion

The essence of this chapter is to analyse the international standards on independence of data protection authorities and the extent to which they have been applied in Africa. The chapter also sought to identify the possible hurdles that DPAs may face in achieving independence from a broader context. Indeed, without independence, a DPA operates like a paper tiger. Similarly, despite the initial controversies regarding the 'one-size-fits-all application of the concept', it seems to now be settled that the independence and effectiveness of a DPA are intricately linked. As rightly noted, 'there is a clear link between DPA independence and the

133 Examples of such efforts by the AU Commission include the issuance of the Personal Data Protection Guidelines for Africa that were made pursuant to the AU Convention. It is a joint initiative of the Internet Society and the Commission of the African Union, https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf (accessed 1 September 2021).

134 Network of African Data Protection Authorities 'Becoming a member or observer', https://www.rapdp.org/en/devenir-membre-observateur (accessed 1 September 2021).

135 P Schütz 'Assessing formal independence of data protection authorities in a comparative perspective' in J Camenisch and others *Privacy and identity management for life* (2011) 45.

impartiality and integrity of compliance and enforcement schemes that go beyond traditional governmental regulatory structures'.[136] While there is a difference between formal/legal independence and independence in practice, I argued that the former is crucial for a realisation of the latter. That is why the focus essentially was on an analysis of statutory provisions on independence on the continent, and future research will do well to consider the practical perspective of the topic. GDPR currently provides the most exhaustive stipulation on independence and, owing to its influence and globalising effect, it appears that those standards will be the next international metric against which independence of DPA will be assessed.

At the regional level, the ECOWAS Supplementary Act provides the most detailed provisions on independence, albeit with lapses. The AU Convention is vague in this respect and the Personal Data Protection Guidelines for Africa that were recently issued by the AU Commission add nothing significant in putting flesh to the Convention toward a better understanding. The approach to regulatory independence at the domestic level has not been good. Most African countries make very vague stipulations on independence with some not even making any provision. In practice, the DPAs of many countries have been made subject to an overwhelming supervisory role of key ministries of government, thereby significantly affecting their independence. Only the South African POPIA makes a laudable provision in this regard on the continent. Not only is the stipulation very detailed, bit it could arguably also stand the test of GDPR. It is therefore recommended that future reforms of data protection regimes in other countries could take a lesson or two from the approach of South Africa.

Another area other countries could learn from South Africa is regarding the method of establishment of certain statutory bodies called 'state institutions supporting constitutional democracy' under Chapter 9 of the South African Constitution.[137] The uniqueness of these institutions is the approach of entrenching them in the Constitution. Although the Information Regulator is not among those bodies, it is arguably designed to be like them. As mentioned in POPIA, the Information Regulators, like these institutions, are 'independent, and subject only to the Constitution and the law, and they must be impartial and must exercise their powers and

136 Cate and others (n 1) 2.

137 These are (a) the Public Protector; (b) the South African Human Rights Commission; (c) the Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities; (d) the Commission for Gender Equality; (e) the Auditor-General; and (f) the Electoral Commission.

perform their functions without fear, favour or prejudice'.[138] The uniqueness of these bodies is that the very act of constitutional entrenchment insulates them from undue politics and political interference. This has been argued to be one of the most effective means of guaranteeing the independence of certain statutory bodies.[139] African countries must, therefore, learn from this approach and probably consider constitutionally entrenching the roles and functions of DPAs in future constitutional reforms. However, given the difficulty of obtaining constitutional reforms, African countries can start by adopting the South African approach in section 39(b) of the POPIA in future reforms of their data protection legislation.

138 The Constitution of the Republic of South Africa, 1996 sec 181(2). The same provision is contained in POPIA sec 39(b).

139 Fombad (n 116) 325-344.

References

Abdulrauf, LA "Giving 'teeth' to the African Union towards advancing compliance with data privacy norms' (2021) 30(2) *Information & Communications Technology Law* 87

Abdulrauf, LA & Fombad, CM 'The African Union's data protection Convention 2014: a possible cause for celebration of human rights in Africa?' (2016) 8(1) *Journal of Media Law* 67

Adams, R & Adeleke, F 'Protecting information rights in South Africa: the strategic oversight roles of the South Africa Human Rights Commission and the Information Regulator' (2020) 10(2) *International Data Privacy Law* 146

Adepetun, A 'Nigeria Data Protection Bureau awaits NASS on Startup bill' *The Guardian* 9 February 2022. Also available online at https://guardian.ng/technology/fg-creates-nigeria-data-protection-bureau-awaits-nass-on-startup-bill/ (accessed 9 April 2022)

Birnhack, MD 'The EU Data Protection Directive: An engine of a global regime' (2008) 24(6) *Computer Law & Security Review* 508

Data Protection Africa 'Mapping 55 African countries | 36 data protection laws | 3 draft laws https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf (accessed 3 March 2024)

Davis, T 'Data protection in Africa: A look at OGP member progress' https://altadvisory.africa/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf (accessed 1 September 2021)

Fombad, CM 'The role of hybrid institutions of accountability in the separation of power scheme in Africa' in CM Fombad (ed) (2016) *Separation of powers in African constitutionalism* OUP: Oxford

Flaherty, D (1987) *Protecting privacy in surveillance societies* University of North Carolina Press: North Carolina

Greenleaf, G 'Independence of data privacy authorities (Part I): International standards' (2012) 28 *Computer Law & Security Review* 1

Greenleaf, G 'Independence of data privacy authorities (Part II): Asian-pacific experience' (2012) 23 *Computer Law and Security Review* 121

Greenleaf, G & Cottier, B 'International and regional commitments in Africa data privacy laws: A comparative analysis' (2022) 44 *Computer Law and Security Review* 1

Giurgiu, A & Larsen, TA 'Roles and powers of National Data Protection Authorities' (2016) 2(3) *European Data Protection Law* Review 342

Hoofnagle, CJ ; van der Sloot, B & Borgesius, FZ 'The European Union general data protection regulation: what it is and what it means' (2019) 28(1) *Information & Communications Technology Law* 65

Ilori, T 'Data protection in Africa and the COVID-19 pandemic: Old problems, new challenges and multistakeholder solution' https://africaninternetrights.org/sites/default/files/Tomiwa%20Ilori_AfDec_Data%20protection%20in%20Africa%20and%20the%20COVID-19%20pandemic_Final%20paper.pdf (accessed 1 September 2021) 1

Jančiūtė, L 'European Data Protection Board: a nascent EU agency or an 'intergovernmental club'? (2020) 10(1) *International Data Privacy Law* 57

Kuner, C; Cate, FH; Millard, C & Svantesson, DJ 'The intricacies of independence' (2012) 2(1) *International Data Privacy Law* 1

Lynskey, O "The 'Europeanisation' of data protection law" (2017) 19 *Cambridge Yearbook of European Legal Studies* 257

Makulilo, AB 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78

Makulilo, AB 'The context of data privacy in Africa' in AB Makulilo (ed) *African Data Privacy Laws* (2016) Springer: Swizerland

Makulilo, AB 'The GDPR implications for data protection and privacy protection in Africa' (2017) 1(2) *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 12

Makulilo, AB 'The long arm of GDPR in Africa: Reflection on data privacy law reform and practice in Mauritius' (2021) 25(1) *The International Journal of Human Rights* 133-134

Merriam-Webster Dictionary online. https://www.merriam-webster.com/dictionary/independent (accessed 1 September 2021)

Network of African Data Protection Authorities 'Becoming a member or observer' https://www.rapdp.org/en/devenir-membre-observateur (accessed 1 September 2021)

Roos, A 'The European Union's General Data Protection Regulation (GDPR) and its implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles' (2020) 53(3) *Comparative and International Law Journal of Southern Africa* 1

Stein, P 'South Africa's EU-style Data Protection Law' (November 2012) *Without Prejudice* 48 available https://journals.co.za/doi/pdf/10.10520/EJC128763 (accessed 1 September 2021)

Schütz, P 'Assessing formal independence of data protection authorities in a comparative perspective' in Camenisch, J; Fischer-Hübner, S & Rannenberg, K (2011) *Privacy and Identity Management for Life* Springer: Berlin

Tarasova, E 'Data protection authorities in Central and Eastern Europe: Setting the research agenda' in P Jonason & Rosengren, A (eds)(2017) *The right of access to information and the right to privacy: A democratic balancing act* Södertörn University Publications: Stockholm

Zerdick, T 'Article 52. Independence' in Kuner, C; Bygrave, LA; Docksey, C & Drechsier, L (eds) (2020) *The EU General Data Protection Regulation (GDPR): A commentary* Oxford University Press: Oxford