# The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?[*]

by

Lukman Adebisi Abdulrauf[**]

&

Charles Manga Fombad[***]

**Abstract**

It is now widely recognised that the unregulated processing of personal information has had a significant impact on key human rights like privacy, dignity, integrity, personality and autonomy. However, while other regions of the world have taken concerted action to protect the personal rights of individuals by adopting data protection instruments, Africa has generally lagged behind. This is so in spite of the steady growth in access and usage of ICT and the internet which has facilitated the exploitation of individuals' personal information with the attendant risk of infringement of their rights. An important step to change this situation was taken when African leaders in June 2014, agreed to a landmark Convention on data protection. This Convention has provoked mixed reactions from stakeholders and privacy advocates. While some are skeptical as to the effectiveness of this Convention, others have welcomed it as a cause for celebration of human rights on the continent.

This paper assesses the potential impact this Convention will have on the protection of individual's personal data. The analysis will start by providing an overview of the major data processing activities in Africa and their effects on human rights. Then, the paper will consider the previous initiatives on data protection on the continent at both regional and sub-regional levels. Furthermore, the Convention as an instrument capable of harmonising all the previous regional and local initiatives is examined. Key aspects of the Convention are analysed and compared with longstanding and influential instruments especially, the Council of Europe's Data Protection Convention and the European Union's Data Protection Directive. Based on a comparative analysis of the Convention and other regional data privacy instruments, the paper shows that the Convention is a step in the right direction to realising the right to data protection in Africa. However, it concludes that more still needs to be done by the AU for effective data protection on the continent.

**Keywords:** Data protection, Privacy, African Union, human rights in Africa, information society

## 1. Introduction

Globalisation and the increasing interdependence of states has led to the conclusion of a great number of treaties and other regional (and sub-regional) arrangements which regulate matters that had hitherto been regulated by national law.[1] This is especially so in subjects like data protection which require a great deal of harmonisation for effective implementation. Moreover, the need for free flow of information means data protection has increasingly become transnational in nature.

[*] This article was originally presented at the 7th International Conference on Information Law and Ethics (ICIL) that was held at the University of Pretoria, South Africa on 22-23 February 2016. We thank the conference organisers and participants. We also thank the reviewers for the insightful comments. All errors, however, remain ours.

[**] Centre for Human Rights, Faculty of Law, University of Pretoria, South Africa and Lecturer, Department of Public Law, Faculty of Law, University of Ilorin, Nigeria. E-mail: lukmanrauf@gmail.com

[***] Professor of Law, Institute for International and Comparative Law in Africa, Faculty of Law, University of Pretoria, South Africa.

[1] D Sloss, 'Non-self-executing treaties: Exposing a constitutional fallacy' (2002) 36(1) *UC Davis Law Review* 1, 3.

An efficient and effective data protection framework is very important because it will provide legal protection to individuals from the harm resulting from the manual or automated processing of their personal information.[2] The value of 'personal information', which is information that relates to or identifies (or is capable of identifying) a natural (or legal) person, is in its movement across borders. This raises legal issues regarding the protection of such information, which is considered 'sacred' because of its depiction of one's personality, especially when its movement across various jurisdictions cannot be easily controlled. Admittedly, such issues are essentially domestic in nature. However, problems arise when personal information is to be transported to a jurisdiction without an efficient legal regime for its protection. It is in this kind of situations that regional initiatives, such as the African Union Convention on Cyberspace Security and Protection of Personal Data ('AU Convention' or 'the Convention')[3], becomes significant.

The controversy over whether (or not) data protection is a human right now seems to be more or less settled.[4] In fact, there are strong arguments in support of the fact that the right is now a *sui generis* right independent of privacy, although such arguments are yet to find a basis in Africa. Some scholars even argue that data protection has crystallised into a norm of customary international law.[5] All these depicts the importance of data protection to any human right system. It was a recognition of the importance of data protection that led the AU to adopt the Convention. However, this Convention has provoked mixed reactions from stakeholders and privacy advocates. While some are skeptical as to its effectiveness, others have welcomed it as a cause for celebration of human rights on the continent.

In view of the above, this paper interrogates whether the Convention is likely possible to enhance the prospects for the protection of human rights in Africa. The analysis of the Convention in this paper will address two crucial issues. Firstly, whether the Convention is capable of attracting wide-scale adoption and implementation by state parties? To answer this question, the provisions of the Convention will be examined alongside long-standing data privacy instruments. In this respect, the substantive provisions of the AU Convention will be compared with the Council of Europe (CoE) Data Protection Convention[6] (and the EU Directive).[7] This is because, apart from the AU Convention, the CoE Convention is the only binding instrument on data protection as a matter of international law.[8] In fact, the CoE Convention is viewed 'as having potentially

[2] A Roos, 'Data protection' in D Van der Merwe *et al Information and communications technology law* (2008) 313. J Neethling *et al Law of personality* (LexisNexis, 2005) 267.

[3] African Union Convention on Cyber Security and Personal Data Protection EX.CL/846(XXV) available at https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf (accessed 27 January 2016).

[4] Especially in Europe. See generally GG Fuster, *The emergence of personal data as a fundamental right of the EU* (Springer, 2014). See also O Lynskey, 'Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order' (2014) 63(3) *International and Comparative Law Quarterly* 569.

[5] For example, M Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 23(2) *International Journal of Law and Information Technology* 99.

[6] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108 at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm (accessed 27 January 2016).

[7] The 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. Available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31995L0046 (accessed 27 January 2016).

[8] P De Hert & V Papakonstantinou, 'Three scenarios for international governance of data privacy: Towards an international data privacy organization, preferably a UN agency?' (2013) *I/S: A Journal of Law and Policy* 271, 278.

'universal' application, i.e. proving the basis for global data protection standards.'[9] Thus, a discussion on the AU Convention alongside the older and more mature CoE Convention may be an important determinant of the quality of the former. The second issue to be investigated is the possible obstacles the Convention may face in the realisation of effective human rights protection in Africa. Before these issues are interrogated, it is important to preface this by briefly looking at the challenges to human rights protection in the digital age in Africa.

The paper is organised in six parts. The second part examines the prospects for building the African information society and the challenges to human rights protection. Part three discusses subregional initiatives on data protection prior to the AU Convention. Part four makes an in-depth analysis of the substantive provisions of the AU Convention and compares this with the provisions of the CoE Convention (and sometimes, the EU Directive). Part five reflects on the various challenges to the AU Convention in effective human rights protection in Africa. Finally, part six concludes that paper with key recommendations on successful implementation of the Convention.

## 2. Building the information society in Africa and the challenges to human rights protection

Africa is currently making strenuous efforts at various levels 'to build the information society'[10] so as to enable it to benefit from the on-going globalisation process taking place around the world.[11] This is partly also in recognition of the fact that 'information is a crucial economic and social resource' and 'electronic networks and information technology present a new venue for social economic and cultural activity, at both local and global levels.'[12] In fact, a credible information society goes hand in hand with economic and social development which Africa desperately needs. It is therefore no surprise that, scholars and policymakers have consistently acknowledged the importance of a viable information society for economic development across the continent.[13] Two major features of the information society are the proliferation of

[9] Indeed, this is so because the CoE Convention has allowed non-member states to accede to it. See C Kuner, 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law & Security Review* 307, 313

[10] The concept of 'information society' is an elusive concept without a precise meaning or definition. According to Hamelink, the concept of information society 'refers to the growing significance of information products (such as news, advertising, entertainment and scientific data) and information services (such as provided by the World Wide Web); the increasing volumes of information generated, collected, stored and made available; the essential role of information technology as the backbone of many social services and as the engine of economic productivity; and the input of information processing into transactions in trading and finance'. CJ Hamelink, 'Human rights for the information society' in B Girard & SO Siochrú, *Communicating in the information society* (United Nations Research Institute for Social Development, 2003)122.

[11] See initiatives like the African Information Society Initiative (AISI) and the Regional Action Plan on the Knowledge Economy (ARAPKE) both specifically mentioned in the AU Convention

[12] United Nations Economic Commission for Africa (UNECA) *Africa's Information Society Initiative: An Action Framework to Build Africa's Information and communication Infrastructure* available at http://www.uneca.org/cfm1996/pages/africas-information-society-initiative-action-framework-build-africas-information-and (accessed 26 January 2016).

[13] For example, NJ Udombana, 'The information society, poverty and development: An African Perspective' (2005) 18(1) *Revue québécoise de droit international* 75, 77. Unfortunately, the digital divide, which is 'the unequally access to ICTs by various communities', is a major obstacle to a credible information society in Africa. See also UNECA (n 15).

information and communication technologies (ICTs) and the increase in demand for personal information by various entities.[14] Both features in many ways pose a challenge to human rights. For example, the demand for personal information aided by increasingly ubiquitous ICT infrastructure facilitates information collection and use in a way that often leads to loss of control by individuals' over their personal data. This may amount to a violation of individuals' rights to privacy, dignity and personality, among others. Such violations are now becoming prevalent in Africa, especially in areas such as proliferation of the internet, national identity cards schemes, SIM card registration exercise and surveillance technologies. This will be briefly explained below.

### 2.1. Proliferation of the internet and online services

Building a credible information society is dependent on the availability and access to the internet. Indeed, 'internet penetration is growing exponentially in Africa.'[15] With an estimated population of above a billion (November 2015), Africa has more than three hundred (300) million internet users.[16] It thus has about thirty (30) percent internet penetration.[17] The increasing presence of the internet poses a fundamental threat to privacy. The increase in internet access also comes with proliferation of online and social networking services. Daily activities can be performed online with e-banking[18] and e-marketing services.[19] In this way, sensitive transactions are increasingly being conducted and important data stored on the internet in Africa. This situation may sometimes result in users not knowing who has access to their personal information, why their personal information is collected and what it is being used for. For example, direct marketers and online advertisers may harvest this personal information and exploit them for economic gains. Privacy and data protection has always been an issue when personal information is used without the consent and choice of the individual. A related problem with the rise in the use of the internet is identity theft. Identity theft is a category of cybercrime which involves using another person's personal information to obtain credit, loan etc. Even the AU notes that improvement in internet infrastructure is problematic as '[b]eing wired to the rest of the world means we are now within the perimeter of cybercrime, making the continent's information systems more vulnerable than ever before.'[20]

### 2.2. National Identity Cards Schemes

Many African states are in the process of developing comprehensive identity (ID) card systems to facilitate easy identification of criminals and maintenance of law and order. Using modern ICTs, extensive databases of individuals' personal data, including sensitive and biometric data, are kept by the government. According to Banisar, '[t]he most common ICT privacy issue

---

[14] N Moore 'The information society' in Y Courrier (ed) *World information* (1997) 271. (Although, she referred to three characteristic of an information society).

[15] E Tamarkin 'The AU's cybercrime response: A positive start, but substantial challenges ahead' (2015) 73 *Policy Brief* 1. Also available https://www.issafrica.org/uploads/PolBrief73_cybercrime.pdf (accessed 27 January 2016).

[16] Internet World Stats 'Internet users in the world by regions November 2015' available at http://www.internetworldstats.com/stats.htm (accessed 27 January 2016).

[17] *Ibid.*

[18] See generally A Harris *et al* 'Privacy and security concerns associated with mobile money application in Africa' (2013) 8 *Washington Journal of Law, technology & Arts* 245.

[19] Tamarkin (n 15).

[20] AU 'INFOSOC: Division of information society' available at http://pages.au.int/infosoc/cybersecurity (accessed 27 January 2016).

currently facing African nations is the development of new citizen identification systems, including identity cards and passports.'[21] This has serious implications for the right to privacy especially because there was, hitherto, no regional instrument holding states responsible for personal information in their possession. Besides, many of these ID systems are developed and operated by foreign companies.[22] For example, Nigeria is in the process of developing a comprehensive e-ID card scheme with the assistance of an American company, MasterCard which means there could be vast movement of personal information from Nigeria to the United States where the headquarters of MasterCard is situated.[23]

### 2.3. SIM card registration exercise

Another avenue for the harvesting of personal information which is increasingly becoming prevalent in Africa is the subscriber identity module (SIM) card registration schemes.[24] Many African countries have a mandatory requirement for SIM card registration without an enabling law in place.[25] This has serious data protection implications for the security of accumulated personal information. With sensitive personal information in the hands of the state, mobile surveillance is made easy with negative consequences for human rights.

### 2.4. Surveillance technologies

Surveillance technologies are now commonplace in digital age Africa. Surveillance, in this context, is a systematic means of personal information collection, especially by governments or private entities. States now have laws mandating telecommunication providers to integrate surveillance systems capable of interception of communications. For example, South Africa's Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 requires service providers to incorporate surveillance machinery before they can offer services to the public.[26] Some African countries have even created more advanced means of surveillance. In Nigeria for example, there were reports that the government was in the process of developing advanced software to monitor internet communication.[27]

The above are some of the features of the African information society which is now characterised by 'massive data collection'. It is, perhaps, in recognition of 'information power' and the potential effects of its collection and use on human rights and fundamental freedoms that the AU Convention was adopted by African leaders. By this landmark Convention, member states of the AU reaffirm their 'commitment …to fundamental freedoms and human and peoples' rights' contained in various global and regional instruments.[28] Before the Convention, however,

---

[21] D Banisar, 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16(1) *East African Journal of Peace & Human Rights* 124, 126.
[22] *Ibid.*
[23] J Oguntimehin, 'Implications of Nigeria's National ID card' http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf (accessed 27 January 2016).
[24] AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2(3) *International Data Privacy Law* 163, 173-174.
[25] *Ibid.*
[26] See Banisar (n 24) 129.
[27] Ogala Emmanuel, 'EXCLUSIVE: Jonathan Awards $40 Million Contract to Israeli Company to Monitor Computer, Internet Communication by Nigerians' *Premium Times*, April 25, 2013 available at http://bit.ly/12K1rUR (accessed 27 January 2016).
[28] See AU Convention, preamble.

a number of important initiatives had been undertaken by regional economic communities (RECs) in Africa. Some of thes initiatives will be briefly examined.

## 3. Regional and subregional initiatives on data protection prior to the AU Convention

Africa, though a relatively late entrant in the field of data protection, is making considerable efforts in the field. Developments in this area were heralded by a number of regional, sub-regional and domestic initiatives. It is also worth noting that prior to the AU Convention, a number of African countries had introduced data protection laws in their legal systems. However, national legislation does not entirely deal with the issues that may arise when personal information crosses different borders.

Due to the limitations of national legislation in dealing with the matter, subregional initiatives therefore, become imperative. RECs were the subregional groupings that championed subregional initiatives. RECs in Africa were originally not established to 'foster human rights, but to facilitate a process of economic convergence through closer economic and financial cooperation and harmonisation policies and programmes.'[29] With time however, human rights became a critical aspect of their mandates.[30] With regard to data protection prior to the AU Convention, four RECs had taken concerted actions by adopting legal instruments to address the matter.[31] The Economic Community for West African States (ECOWAS) is the first subregional body to adopt a concrete framework on data protection law.[32] In 2010, it adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS ('ECOWAS Supplementary Act').[33] According to Bygrave, the Act was the 'leading initiative' on data protection in Africa.[34] Greenleaf also contends that the Act spurred data protection laws in West Africa.[35] To make the Supplementary Act legally binding on member states, it is annexed to and forms an integral part of the ECOWAS Treaty.[36] Therefore, a violation of the Supplementary Act by member states can be enforced by the ECOWAS Court of Justice.[37] Being a supplementary Act, the ECOWAS treaty 'may be legally binding in creating substantive rights in countries where treaties have direct effect and do not require local enactment.'[38] Apart from its sectional

[29] F Viljoen, *International Human Rights Law in Africa* (Oxford University Press, 2nd edn, 2012) 482.
[30] As Viljoen argues, 'there is an obvious link between one of the main objectives of regional integration-improving the welfare of the people in the participating countries and the realization of socio-economic rights.' (n 29 ) 482.
[31] Although, the AU currently recognises only eight RECs.
[32] AB Makulilo, 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78, 82.
[33] Adopted 16 Feb 2010. ECOWAS Supplementary Act available at http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf (accessed 27 January 2016).
[34] LA Bygrave, *Data privacy law: An international perspective* (Oxford University Press, 2014) 80.
[35] G Greenleaf, 'Sheherezade and the 101 data privacy laws: origins, significance and global trajectories' (2014) 23(1) *Journal of Law, Information and Science* 8, 22.
[36] See ECOWAS Supplementary Act, art 48.
[37] Makulilo (n 33) 83.
[38] G Greenleaf & M Georges, 'African regional privacy instruments: Their effects on harmonization' (2014) 132 *Privacy Laws and Business International Report* 19.

application, the supplementary Act has been criticized for the fact that it does not provide clear sanction for a member state who fails to transpose the Act in its domestic laws.[39]

The East African Community (EAC) also developed a data protection framework - the EAC Legal Framework for Cyber Laws (Phase 1 & 2) 2008/2011.[40] Unlike the ECOWAS Supplementary Act, however, the legal framework is not binding on member states. It merely 'contains a series of recommendations made to the governments of partner states about reforming national laws to facilitate electronic commerce, to facilitate the use of data security mechanisms; to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies; to protect consumers in an online environment, and to protect individual privacy.'[41] Furthermore, the EAC legal framework was 'designed to harmonize the law reform process between the EAC Partner States, as well as reflecting international best practice.'[42] In this regard, paragraph 2.5 contains the recommendations on 'data protection and privacy'.[43] However, the frameworks 'do not provide any content principles as minimum standards for its members to adhere.'[44] This is, arguably, not a welcome development for the right to data protection which requires that certain minimum standards are specified for the processing of personal information.

The next significant subregional initiative prior the AU Convention is that of Southern African Development Community (SADC) with its Data Protection Model Law ('Model Law').[45] The objective of the Model Law, among others, is to 'create a uniform system in a given area in order to create a safe environment for citizens.'[46] Thus, the Model Law seeks to ensure harmonisation of data protection policies in member states. One of the factors that made this necessary was the permeability of traditional borders between countries. The model law gave prescriptive guidance to member states in enacting their data protection legislation. Like the EAC Framework, the SADC Model Law, of course, is not binding. This, therefore, limits any potential influence it may have in effective human rights protection in that region.

In 2013, the Economic Community of Central African States (ECCAS/CEMAC) made its own contribution to data protection in Africa by adopting a model law containing three texts on electronic transactions, data protection, and cybercrime. These texts were as draft directives.[47]

With these initiatives Africa has arguably become a 'home to some of the most prescriptively ambitious data privacy initiatives at regional and sub-regional levels'.[48] Greenleaf and Georges

[39] Makulilo (n 33) 87.
[40] Draft EAC Legal framework for Cyberlaws (2008) available http://www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148 (accessed 27 January 2016); Framework for Cyberlaws, Phase II (UNCTAD, 2011) http://r0.unctad.org/ecommerce/docs/EAC_Framework_PhaseII.pdf (accessed 27 January 2016).
[41] Draft EAC Legal framework for Cyberlaws (n 40) 3.
[42] *Ibid.*
[43] *Ibid*, 17.
[44] Makulilo (n 33) 84.
[45] Data Protection: Southern African Development Community (SADC) Model law https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf (accessed 27 January 2016).
[46] *Ibid*, 3.
[47] See Greenleaf and Georges (n 38).
[48] Bygrave (n 34) 80.

assert that '[n]ow it is Africa that is leading global expansion' of data protection law. Notwithstanding this, the above initiatives cannot be considered to be credible substitutes for a *unified* continent-wide data protection initiative. This is because the wider the jurisdictional scope of a data protection instrument, the better the transboundary nature of data protection. On the other hand, harmonisation at the global level is considered by some to seem like a mirage[49] because of the notoriously 'wide' and 'vague' conception of privacy in different parts of the world. Regional initiates, therefore, become the next point of call. Since the AU is making strides in human rights protection lately, it goes without saying that it was the proper institution to initiate reforms on data protection in Africa. It is on this basis that the AU's initiative – the AU Convention – deserves a detailed examination.

## 4. The AU Data Protection Convention

The AU set up, in the Constitutive Act and other instruments, Africa's regional system for promotion and protection of human rights.[50] This sets out not only to attain human rights objectives, but to use human rights-based means (or principles) to achieve those objectives.[51] As a key human right in the digital age, the role of the AU in data protection is vital – hence the Convention. This is perhaps the reason why Greenleaf and Georges describe the adoption of the Convention as 'potentially [the] most important development [on data protection] in Africa.'[52]

### 4.1. Background to the AU data protection convention

Before the adoption of the AU Convention, some efforts on data protection had been made by the AU. The first of such efforts was in 2011 with the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.[53] This draft was subsequently reviewed, albeit with a slight name change in 2013. The second draft was the African Union Convention on the Confidence and Security in Cyberspace.[54] These drafts were heavily criticised by the private sector, civil society organisations and privacy advocates because they had little involvement in the process.[55] In May 2014, there was a meeting of experts from the AU member states' ministry of justice to carry out a thorough review of the drafts.[56] On 27 June 2014, the AU Convention was adopted at the 23rd Ordinary session of the AU Summit in

[49] See generally Kuner (n 9) 307. C Kuner, 'The European Union and the search for an international data protection framework' (2014) 2(1) *Groningen Journal of International Law* 55.
[50] Viljoen (n 29)152.
[51] *Ibid*, 165.
[52] G Greenleaf & M Georges 'The African Union's data protection Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws & Business International Report* 18-21.
[53] See http://au.int/en/cyberlegislation (accessed 27 June 2016).
[54] *Ibid.*
[55] EP Kenyanito, 'Africa moves towards a common cyber security legal framework' https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework/ (accessed 27 January 2016).
[56] *Ibid.*

Malabo.[57] The reason for the slight change in name is still unclear. However, it is submitted that the present Convention is largely similar to the previous drafts.

The Convention has a broad scope to cover three important areas of cyber law viz: electronic transactions, data protection and cybersecurity and cybercrime. This paper focuses on only the data protection provisions of the Convention.

### 4.2. Object and purpose of the Convention

Like most data protection instruments, the AU Convention has two broad objectives. Firstly, it commits state parties to 'establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data and to punish any violation of privacy without prejudice to the principle of free flow of data.'[58] Secondly, the framework so established by member states shall ensure that any form of data processing respects fundamental freedoms and human rights while recognising the right of the state, local communities and the purposes for which businesses were established.[59] The objectives of the Convention shows an unequivocal human rights protection agenda. Furthermore, the Convention recognises the interests of other entities in individuals' information like states, local communities and the purpose for which businesses are established. It, therefore, enjoins member states in establishing a framework, to carefully balance these broad objectives.

The objective of the Convention contains certain obscure terms. The first is 'protection of physical data'. Obviously, the Convention seeks to protect personal data like all data protection instruments. However, questions could arise regarding whether 'personal data' has the same meaning as 'physical data'. Unfortunately, the latter term is not defined in the definition section of the Convention. It is arguable that both terms mean the same thing. Perhaps, the AU Convention adopted the term so as to distinguish personal information of natural persons from that of legal persons, since only the former falls within its scope. Furthermore, the use of the term 'local communities' as part of the institutions with rights over personal information is obscure and the term is not also defined in the Convention.

Since the AU Convention is not intended to be self-executing, certain issues, based on lessons that can be drawn from Europe, must be taken into consideration by state parties when establishing their legal regimes on data protection. Firstly, the CoE Convention, in stating its primary role as a human rights instrument, provides that it seeks to 'secure in the territory of each party for *every individual, whatever his nationality or residence*, respect for his [or her] right and fundamental freedoms, and, in particular, his [or her] right to privacy.'[60] This provision 'is in accordance with the general principles of the CoE and its member states with regard to the

[57] "Mixed feedback on the 'African Union Convention on Cyber Security and Personal Data Protection'" available at https://ccdcoe.org/mixed-feedback-african-union-convention-cyber-security-and-personal-data-protection.html (accessed 27 January 2015).
[58] AU Convention, art 8(1).
[59] AU Convention, art 8(2).
[60] CoE Convention, art 1. See also Consultative Committee (T-PD) 'Modernisation of Convention 108: Final Document T-PD (2012)' available at https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)04Rev4_E_Convention%20108%20modernised%20version.pdf (accessed 27 January 2016).

protection of individual rights.'[61] Thus, 'clauses restricting data protection to a state's own nationals or legally resident aliens would be incompatible with the convention.'[62] The AU Convention has no similar provision hence, it is arguable that the Convention only commits state parties to establish legal frameworks applicable to only citizen of state parties.[63] Secondly, based on the objectives of the AU Convention (and the CoE Convention), securing the right to privacy is explicitly mentioned as a core objective. However, from recent jurisprudence of the EU and scholars' opinion, while privacy is at the heart of data protection, the latter serves a multiplicity of interest beyond privacy concerns.[64] Thus, the trend nowadays is for data protection instruments to avoid a provision stipulating that securing privacy is a core objective.[65]

The AU Convention, like the CoE Convention, explicitly states its primary role as a human right instrument.[66] This is important because of the growing debates regarding whether or not data protection is a human right due to its substantial affiliation to trade. Besides, scholars like Makulilo, argue that African countries seem to have lost sight of the purpose for regulating data processing. [67] They mainly enact data protection legislation for trade benefits that will accrue to them from countries within the EU.

### 4.3. Scope and application

The AU Convention is applicable to any *processing* carried out in the territory of a state party of the AU.[68] State parties of the AU here refer to all the fifty-four (54) African countries with the exception of Morocco.[69] The term processing is defined in article 1 of the Convention as 'any operation or set of operations which is performed upon personal data whether or not by automatic means'. A non-exhaustive list of such activities is stipulated.[70] The Convention, further provides, again, that it applies to 'any collection, processing, transmission, storage or use

[61] Commentary on the provisions of the Convention in 'Data protection: Compilation of Council of Europe texts' available at https://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf (accessed 27 January 2016) 22

[62] *Ibid.*

[63] Indeed, the Constitution of the Federal Republic of Nigeria, for example, has been described as being discriminatory as its Bill of Rights is only applicable to Nigeria citizens. A Kusamotu, 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46' (2007) 16(2) *Information & Communications Technology Law* 149, 154.

[64] Bygrave (n 34) 119. In fact, Bygrave notes that 'in some respects, data privacy canvasses more than what are typically regarded as privacy concerns.'

[65] See for example the Proposal for a Regulation of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data ('draft EU Regulation') which provides in art ((2) that 'This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.' Compare with EU Directive, art 1(1) & CoE Convention, art 1. The draft EU Regulation is available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 27 January 2016).

[66] AU Convention, art 8. See CoE Convention, art 1 and Proposals for modernization of the CoE Convention (n 60) art 1.

[67] Because of the Adequacy requirement of Article 25 of the EU Directive. AB Makulilo, '"One size fits all": Does Europe impose its data protection regime on Africa?'(2013) 7 *Datenschutz und Datensicherheit* 450.

[68] AU Convention, art 9(c).

[69] It is based on this number that some commentators observe that 'The AU Convention has more potential state parties than any other international data protection agreement currently has ratifications. See Greenleaf & Georges (n 52).

[70] Such as processing for household activates etc.

of personal data by a natural person, the state, local communities, public or private corporate bodies.'[71] Outlining specific processing activities again in section 9 appears to be superfluous. Moreover, the trend among recent data protection regulations is no longer to distinguish between these stages, but to use a generic term 'processing' which is broad enough to cover all the stages.[72]

The definition of personal information is also important to the scope of the Convention. For as Schwartz and Solove point out, the existence of personal information is a jurisdictional trigger to the application of data protection instruments.[73] The AU Convention defines personal data/information[74] as 'information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.'[75] This definition, it is submitted, is a substantial replication of the EU Directive.[76] The definition is wide enough to cover all information that identifies individuals, hence, member states can adopt the provision as it is in their legislation. It is also good for harmonisation purposes as a number of African countries have already adopted definitions, influenced by the EU Directive, in their laws.[77]

In addition, the Convention also applies to both automated and manual processing of data 'contained in or meant to be part of a file.'[78] By this provision, the AU Convention goes further than the CoE Convention as the latter only applies to automated processing of personal information.[79]

An innovation of the AU Convention with regard to scope is contained in article 9(d). This provision provides that the Convention places 'any processing of data relating to public security, defence, research, criminal prosecution or state security' within its scope. This is, however, subject to 'exceptions defined by specific provisions of other extant laws.'[80] The Convention, by this provision, as a general rule, requires that these processing activities must comply with the data processing obligations stipulated in section iii. This approach differs from the approach of the EU Directive[81] and takes care of the numerous criticisms associated with excluding these

[71] AU Convention, art 9.
[72] A Roos, 'Personal data protection in New Zealand: Lessons for South Africa (2008) 4 *Potchefstroom Electronic Law Journal* 62, 79.
[73] PM Schwartz & DJ Solove 'Reconciling personal information in the United States and European Union' (2014) 102 *California Law Review* 877, 879
[74] Both will be used interchangeably in this paper.
[75] AU Convention, art 1.
[76] See EU Directive, art 2(b) of the EU.
[77] For example, South African Protection of Personal Information Act (2013), art 1 & Ghanaian Data Protection Act (2012), sec 96.
[78] AU Convention, art 1(b).
[79] CoE Convention, art 3(1) of the Convention. The CoE explains the rational in its explanatory report that 'Compared with manual files, automated files have a vastly superior storage capacity and offer possibilities for a much wider variety of transactions, which they can perform at high speed.' see para1 of the explanatory report to the Convention (n 61) 19.
[80] AU Convention, art 9(d).
[81] The EU Directive in art 3(2) provides that it shall not apply to 'processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law…'

processing activities outright. Usually, it is argued that excluding data processing for public security, defence,[and] criminal prosecution gives public/security agencies too much leeway with regards to individuals' personal information. The approach of the CoE Convention in article 9(2) is as well noteworthy as it also prohibits derogations from the basic principles of data protection except if 'such derogations is provided for by the law of the party and constitutes a necessary measure in a democratic society' in the interest of public security and for the purpose of 'protecting the data subject or the right and freedom of others.'[82] Only the data security principle, however, admits of no derogation under the CoE Convention.

The AU Convention is not applicable to data processing undertaken for 'personal or household activities.' This exception is also not absolute as it is further stipulated that 'provided… such data are not for systematic communication to third parties or for dissemination'.[83] Another aspect of data processing excluded from the scope of the Convention is 'temporary copies produced within the context of technical activities for transmission and access to a digital network with a view to automatic, intermediate and temporary storage of data.'[84] This exception is unclear - it may be an instance of data processing which poses minimal risk based on the principle of *de minimis*. An observation with the provision on the scope of the Convention, which is indeed a welcome approach, is that it contains very few exceptions. This is an important protection against repressive African regimes who may want to rely on the Convention to provide sweeping exemptions thereby diminishing data protection in their countries.

Furthermore, it is arguable that the Convention does not apply to processing carried out for journalistic, research, literary or artistic purposes. This exception applies insofar as the processing is solely for journalistic, artistic and literary activity 'in accordance with the code of conduct of these professions.'[85] Personal information processing in this category are permitted so as to balance the potential conflict between data protection and freedom of expression.[86]

### 4.4. Fair information principles

At the heart of every data protection instrument is the fair information principles (FIPs). According to Bygrave, the principles 'denote the pith and basic thrust of a set of legal rules'.[87] In the AU Convention, the principles are contained in section III which is titled 'obligations relating to conditions governing personal data processing'. The Convention, unlike the European data protection instruments, set out the principles in a specific fashion which makes for easy reading and extraction by state parties. This is indeed a notable development in the Convention. The Convention contains six principles which could have been influenced by a combination of the Organization for Economic Cooperation and Development (OECD) Guidelines[88] and the EU Directives. The first principle is the 'principle of consent and legitimacy of personal data processing.' This principle, it is submitted, is largely taken from the OECD Guidelines as the

[82] AU Convention, art 9(2).
[83] AU Convention, art 9(2)(a).
[84] AU Convention, art 9(2)(b).
[85] AU Convention, art 14(3).
[86] See generally EU Directive, art 9.
[87] LA Bygrave, *Data protection law: Approaching its rationale, logic and limits* (MIT Press, 2002)57.
[88] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 10 January 2016).

neither the CoE Convention nor the EU Directive makes consent a specific principle.[89] The AU Convention requires states to provide, in their domestic frameworks, that processing of personal data shall be legitimate if the data subject consents. Instances where the requirement of consent may be waived are also stipulated. These include cases of compliance with a legal obligation by the controller, performance of a public related task, performance of a contract which the data subject is a party and for the protection of the vital interest or fundamental right of the data subject.[90] Consent of the data subject is defined as 'any manifestation of express, unequivocal, free, specific and informed will by which a data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subject to manual or electronic processing.' From this provision, the Convention requires member states to provide for an opt-in regime for consent rather that an opt-out consent. This is in line with current best practice in data protection regulations.[91]

Opt-in regime for consent appears to be in conflict with the legitimate interest of entities, like businesses, and may thus be problematic. This is more so that the Convention, unlike the EU Directive, does not provide for 'legitimate interest' ground to validate processing of other entities.[92] Thus, it is arguable that the AU Convention's provision for consent as the main legitimising factor for data processing by other entities may conflict with the rights of others. This may therefore question the human rights agenda of the Convention. The problem with the 'legitimate interest' ground for data processing is its extremely vague nature which makes it prone to abuse by businesses. It is, perhaps, in recognition of this fact that the AU Convention avoided 'legitimate interest' as an alternative to consent. Nevertheless, it is arguable that since the Convention states *ab initio* that the legal regime of member states should ensure that data processing 'respects the fundamental freedoms and rights of natural persons while recognising *…the purposes for which businesses were established*',[93] it is submitted that the interest of business must also be taken into consideration. Striking a balance between privacy rights of individuals' and interest of other entities is therefore required of the implementing authority.

The second principle is the 'principle of lawfulness and fairness of personal data processing.' In terms of the Convention, states parties are required to provide that processing of personal information 'shall be undertaken lawfully, fairly and non-fraudulently.' This principle is also contained in the CoE Convention.[94] The third principle is the 'principle of purpose, relevance and storage of processed personal data'.[95] This principle applies mainly at the data collection stage of the processing cycle and it requires that 'data collection shall be undertaken for specific, explicit and legitimate purposes.' It is further provided that personal information must not be

[89] It is however noteworthy that the proposal for modernisation of the CoE Convention takes note of the important place of consent and a specific section is dedicated to it. See Proposals for Modernisation (n 61), art 5(2) which provides that '[e]ach Party shall provide that data processing can be carried out on the basis of the free, specific, informed and [explicit, unambiguous] consent of the data subject or of some legitimate basis laid down by law….'
[90] AU Convention, art 13. Principle 1.
[91] See the draft EU Regulation, art 4 on the definition of 'the data subject's consent.' See also Proposals for modernizing the CoE Convention, art 5.
[92] EU Directive, art 7(f); Draft EU Regulation, art 6(1)(f). See also Proposals for modernizing the CoE Convention, art 5(2).
[93] [emphasis added]. AU Convention, art 8(2).
[94] CoE Convention, art 5(2).
[95] AU Convention, art 13 principle 3.

further processed in a way incompatible with the original purpose.[96] This principle is also contained in the CoE Convention.[97] The principle also contains the requirement that data collection shall be 'adequate, relevant and not excessive in relation to the purposes for which they were collected and further processed.'[98]

The fourth principle is the 'principle of accuracy of personal data.'[99] This principle requires that data collected shall be accurate and kept up to date where necessary. The Convention requires reasonable steps to be taken to 'erase or rectify' inadequate, incomplete processed personal information. This principle is also contained in the CoE Convention.[100] The fifth principle, the principle of transparency of personal data processing, is rather strange and vague. It requires data controllers to mandatorily disclose information on personal data. The Convention does not say who the data controller should disclose the information to. Is it the data subject or the National Protection Authority (NPA)? The principle is not contained in either the CoE Convention or the EU Directive. The recent reform process in European data protection regimes, however, shows the (possible) introduction of the principle. For example, the proposal for modernisation of the CoE Convention provides for the principle of 'transparency of processing' where state parties are required to see to it that the data controller ensures the *transparency of data processing* by informing the data subjects of 'the identity and habitual residence or establishment of the controller, the purposes of the processing carried out, the data processed, the recipients or categories of recipients of the personal data, and the means of exercising the rights set out in article 8, as well as any other information necessary to ensure fair and lawful data processing.'[101] Similarly, in the draft EU Regulation, the requirement of transparency is merged with the principle of fair and lawful processing where it is provided that personal information must be 'processed lawfully, fairly and in a *transparent manner* in relation to the data subject.'[102] The transparency principle in the AU Convention is most likely influenced by these developments and it is arguable that the principle was intended to operate in a like manner. This could, therefore, mean a possible introduction of a new norm in data protection law and its provision in the AU Convention is, indeed, a welcomed idea. However, it needs to be further explained in an explanatory memorandum.

The last principle is the principle of confidentiality and security of personal data processing where provision is made for processing of personal information to be carried out confidentially and in a protected manner, especially where the processing involves the transmission of the data over a network.[103] It is further provided that where the processing is carried out by a third party on behalf of a controller, the latter must choose a processor who provides sufficient guarantee and it is incumbent on the controller to ensure compliance with the security measures in the Convention. This principle is also contained in the CoE Convention.[104] There, it is an obligation on state parties to require that data controllers put in place appropriate security measures for the protection of personal information 'against accidental or unauthorized destruction or accidental

[96] *Ibid.*
[97] CoE Convention, art 5(b).
[98] This requirement is also a duplicate of the CoE Convention. See art 5(c).
[99] AU Convention, art 13 principle 4.
[100] CoE Convention, art 5(d).
[101] Proposals for modernisation of the CoE Convention, art 7bis on 'transparency of processing'.
[102] (Emphasis added). See draft EU Regulation, art 5(a). See also art 11.
[103] AU Convention, art 13. Principle 6.
[104] CoE Convention, art 8.

loss… [and] unauthorized access'. It is submitted that the provision of the CoE Convention is more explicit than the AU Convention with regard to this principle. The proposals for modernisation of the CoE Convention makes an important addition to the security safeguard principle which is surprisingly missing in the AU Convention. This is a requirement of data breach notification where the controller must notify (at least) the supervisory authority of serious breaches.[105]

An important principle which is omitted in the AU Convention is the accountability principle. Accountability is an 'umbrella concept which covers a myriad of obligations'[106] and it commits a data controller to put in place the necessary mechanisms to ensure that all other principles are complied with. This principle is derived from the OECD Guidelines.[107] Van der Sloot argues also that it is implicitly contained in the draft EU Regulation.[108] The principle is neither contained in the EU Directive nor the CoE Convention. It is can be argued that the absence of the principle in these key instruments is because it is embedded in other principles and obligations of the data controller and may therefore appear redundant to provide specifically for it.[109]

#### 4.4.1. Sensitivity

Although some scholars choose to treat sensitivity as part of the principles,[110] we will discuss it separately here because of its significance in data protection law. The AU Convention, in article 14, provides that parties should prohibit any processing of sensitive data. Sensitive data is data 'revealing racial, ethnic, and regional origin, parental affiliations, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject'.[111] Sensitive data is further defined in article 1. A long list of exceptions is contained in the provision.[112] The categories of sensitive data provided under article 14 of the AU Convention, like its counterpart, the CoE Convention, appears to be closed. Both Conventions make it appear as if all the information listed in the respective provisions are the only category of information that may be considered sensitive.[113] The CoE Convention, in its explanatory report, however, maintains that the list is not meant to be exhaustive and a state party may add to it in its domestic legislation.[114] In any case, there is now a growing debate regarding the relevance of extra protection for a special category of personal information. De Hert and Papakonstantinou, for example, contend that processing intensive

[105] See Proposals for modernization of CoE Convention, art 7(b). This requirement is also contained in the draft EU Regulation but not among the FIPs. See draft EU Regulation, art 31.
[106] B Van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4(4) *International Data Privacy Law* 307, 314.
[107] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data para 14. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 27 January 2016). See also Asia Pacific Economic Cooperation (APEC) Privacy Framework, principle IX. Para 26.
[108] According to Van der Sloot, it is linked to the obligation of transparency in art 22 of the draft EU Regulation. (n 106) 311.
[109] For example, see AU Convention, art 13, principle 6 para (b).
[110] See for example Bygrave (n 34) 165 & Bygrave (n 87) 68.
[111] AU Convention, art 14.
[112] AU Convention, art 14(2).
[113] Ignoring obviously modern-day sensitive information like information genetic data and biometric data.
[114] Explanatory Report to the CoE Convention, para 48.

methods have blurred the distinction between sensitive and non-sensitive information.[115] Therefore, processing of an otherwise non-sensitive information (like meal preference) may lead to information that is considered sensitive (like religious belief). According to the CoE, 'the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which there are used.'[116] The CoE, however, went further to justify its continued inclusion in data protection instruments that 'there are [however] exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests.'[117]

### 4.5. Specific rights of data subjects and duties of data controllers

The AU Convention contains certain key rights of the data subject. These are the rights to information, access, object and rectification or erasure.[118] It has now become a tradition for data protection instruments to set out specific rights of data subjects, although the effects of these rights can still be gotten from the FIPs (which establishes obligations or duties of data controllers). For example, the right to information under the AU Convention in article 16 has the same effect as the principle of transparency of personal data processing (principle 5). The right to information requires data controllers to provide data subjects with some information like his or her (the data controller's) identity, the purpose of processing, the categories of data involved etc.[119] The approach may appear to be unnecessary since every duty bestows a corresponding right and *vice versa*. From this perspective, a 'right and duty are correlative and inseparable.'[120] There are no specific provisions on the rights of data subjects in the CoE Convention.[121] However, it was later inserted in the proposals for modernisation of the CoE Convention.[122] Certain rights are also separately provided for in the EU Directive and draft Regulation.[123] Since these influential data protection instruments have adopted this approach, it can be safely argued that the AU Convention, in this regard, is in harmony with international prescripts.

The Convention, furthermore, specifically outlines some obligations of a data controller. These obligations include confidentiality, security, storage and sustainability obligations.[124] In our view, highlighting these obligations again is unnecessary. This is because section III is a section which basically contains obligations of data controllers. The obligations contained in the AU Convention are largely influenced by the EU Directive.[125] The Directive, on the other hand, does

[115] P De Hert & V Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28 *Computer Law & Security Review* 130, 133.
[116] Explanatory Report to the CoE Convention, para 43.
[117] Explanatory Report to the CoE Convention, para 43.
[118] AU Convention, art 16-19 respectively.
[119] AU Convention, art 10. These rights seems to have been inspired by the EU Directive
[120] SJ Charles Coppens, *A brief text-book of moral philosophy* (Literary Licensing, 1985).
[121] However, the convention provides for some of these rights in art 8 under 'Additional safeguards for the data subject.'
[122] See art 8 titled 'rights of a data subject'.
[123] See EU Directive, arts 12 & 14. See draft EU Regulation, chap iii.
[124] AU Convention, section V 'Obligations of the Personal data controller'.
[125] AU Convention, section VIII.

not provide for some of these obligations in the section on principles/conditions of data processing.[126]

The obligation in article 23 of the AU Convention - sustainability obligations - is rather odd. It requires the data controller to take all appropriate measures to ensure that processed personal data can be utilised.[127] It further mandates the processing official to ensure that 'technological changes' are not an obstacle to utilisation of personal data. There is no similar provision in other international data protection instruments which makes it the more confusing. The obligation is probably included in the AU Convention so as to re-emphasize the commitment of the AU member states to building a credible information society.[128] Thus, any obstacle to the free flow (and utilisation) of personal information, be it technical devices of the data controller, must be prevented. This obligation appears to be consistent with the objective of the AU Convention of protecting privacy 'without prejudice to the principle of free flow of data.'[129]

### 4.6. Data export regime

A fundamental objective of data protection law in general, and the AU Convention, in particular, is to ensure the free flow of information across borders.[130] This objective must, however, be reconciled with human rights and fundamental freedom of individuals. Personal information is exposed to the greatest risk in the process of exchange between countries. This is why it is now customary for data protection instruments to establish a special regime for data export. Article 14(6) of the AU Convention provides for rules on transborder data flows (TBDF). By the provision, a data controller is prohibited from transferring personal data to a non-member state of the AU except such a state guarantees 'adequate level of protection of privacy, freedoms and fundamental rights' of persons whose data are to be processed (transferred). This rule is, however, not applicable where the data controller requests authorisation from the NPA before the intended transfer.[131]

Certain issues arise with regard to the AU Convention's provision on this very vital rule. Firstly, regulation on data export is contained under the provision on sensitive data processing. This gives the impression that only sensitive data, as narrowly defined, is to benefit from this regime. The CoE Convention, for example, dedicates a whole provision for transborder data flow[132] and

[126] For example, the 'confidentiality and security of processing' in section VIII of the EU Directive, are not contained in neither articles 6 nor 7 which contains the FIPs. In the AU Convention however, they are provided in principle 6 of art 13 and repeated again in arts 20 and 21.
[127] AU Convention, art 23.
[128] See AU Convention, preamble.
[129] In support of this view, Bygrave's comment on 'sustainability' in data protection laws seems relevant where he points out that '[d]ata privacy law has much the same aim and function as that policies of 'sustainable development' have in the field of environmental protection. Just as the latter policies seek to preserve the natural environment at the same time allow economic growth, data privacy law seeks to safeguard the privacy related interests of data subjects at the same time as it secures the legitimate interest of controllers in processing personal data.' See Bygrave (n 34) 122.
[130] For more on the importance of TBDF and the need for data protection, see LA Abdulrauf, 'Regulation transborder data flows for development in the G-77+ China: The role of data protection law' 31(1) *UNISA Latin American Report* (2015).
[131] AU Convention, art 14(6)(2).
[132] CoE Convention, art 12.

a protocol to supplement the provision.[133] Similarly, the EU Directive provides for TBDF in a whole chapter.[134] Another issue with the AU Convention's treatment of data export (or TBDF) is that the section is scanty. For example, the Convention says transfer can only be effected to non-member state with an adequate level of protection. What is considered adequate is not stated. Some commentators contend that it 'has a meaning informed by the usage of the same term by Article 25 of the European Union's data protection Directive.'[135] This view, however, amounts to too much speculation since the AU Convention operates in a totally different region. The CoE Convention also uses the term 'adequacy' without stating clearly what it means.[136] Greenleaf therefore argues that 'this is very similar to 'adequacy' in the context of the EU data protection Directive.'[137] This argument is plausible with regard to the CoE Convention rather than the AU Convention since the former largely operates in largely the same locality as the EU Directive. An obvious omission from the Convention is that it does not provide for an exception where information can be transferred to a non-member state without 'adequate' data protection regime. The CoE Convention[138] and the EU Directive[139] make exceptions where transfer can be effected in such a situation, especially where the data subject consents, for the legitimate interest of the data subject or if the data controller uses 'adequate' contractual clauses to safeguard such an information.[140] Such an omission has the effect of compromising the 'free flow of information' objective of the AU.

Admittedly, conventions usually do not make elaborate provisions so as to enable member states to make provisions for details in their legislation. However, leaving out important details will only jeopardise effective protection and complicate harmonisation efforts.

### 4.7. Oversight and enforcement in member states

According to Hustinx, data protection 'is special in the sense that it is considered to be in need of 'structural support' through the establishment of an independent authority with adequate powers and resources.'[141] The supervisory authorities are an element of effective protection of individuals with regard to the processing of their personal information.[142] Oversight and enforcement institutions will be particularly useful for African countries because data protection is a relatively new subject on the continent. There is therefore the need for dedicated institutions

[133] See Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows'
[134] EU Directive, chapter V
[135] Greenleaf & Georges (n 52).
[136] Addition Protocol to the CoE Convention, art 2. But it is more logical to argue that the CoE will adopt the approach of the EU since they are both European institutions. 'Adequacy' as the criteria for transfer to non-state parties was replaced with 'appropriate' in the modernised convention. Greenleaf seriously criticised this replacement. According to him, there is a danger in replacing adequate with appropriate without an explanation as 'appropriate' has little or no meaning in the history of data protection law.' G Greenleaf, ''Modernising data protection convention 108: A safe basis for a global privacy treaty' (2013) 29(4) *Computer Law & Security Review* 8.
[137] Greenleaf (n 136) 7.
[138] CoE Convention, art 2(2)(b).
[139] EU Directive, art 26.
[140] Makulilo (n 32) 88.
[141] P Hustinx, 'The role of data protection authorities' in S Gutwirth *et al* (eds) *Reinventing data protection?* (Springer, 2009)133.
[142] CoE Additional Protocol, preamble.

to interpret and administer the legislation. The AU Convention requires member states to establish institutional frameworks, NPA, to protect personal data.[143] The NPAs must be independent and ensure data processing is carried out in accordance with the Convention.[144] Very robust provision is made for the duties and powers of NPAs which include enforcement, education, auditing, issuance of codes and guidelines and participating in international negotiations.[145]

The AU Convention further requires that NPAs must establish mechanisms for cooperation with data protection authorities of third countries.[146] There is, however, no specific provision for NPAs of state parties to cooperate among themselves. The essence of a treaty of this nature is to promote harmonisation of laws and policies so as to enhance the free movement of personal information and advance the goal of building an information society in Africa. There is no better means of achieving greater harmonisation than by making provision for NPAs to cooperate among themselves. The CoE Convention specifically provides that 'supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties.'[147] This provision, without a doubt, fosters teamwork among member countries.

## 5. Some reflection on possible challenges of the AU Convention for effective human rights protection in Africa

The AU Convention contains far-reaching provisions on the protection of individuals with regard to the processing of their personal information. It shows that Africa, through the AU, is now coming to terms with the realities of the digital age by confronting head-on emerging human rights challenges. Notwithstanding this, there are a number of issues on effective realisation of the objectives of the Convention. These problems may be categorised into two – problems with the convention itself and other problems which are of a general nature.

### 5.1. Problems with regard to the Convention itself

With regard the Convention itself, there a number of issues. Firstly, it is extremely broad in scope. The Convention may be described as a 'package' which seeks to regulate Africa's most pressing problems in relation to ICTs. Thus, it is divided into three chapters – electronic transactions, data protection and cybersecurity. In essence, the Convention is a commercial at the same time, human rights and criminal law instrument. The regulation of these diverse subject matters in one legal document has implication for a proper organisation of the document. For example, the provision on direct marketing which is a crucial aspect of data protection law is placed in the chapter on electronic transactions.[148] Though, it is arguable that direct marketing is a subject matter for both electronic transactions and data protection.

Another issue with this approach (of combining data protection with other instruments) adopted by the AU is the confusion that may arise when a state party is only interested in one of the

[143] AU Convention, art 11(1).
[144] AU Convention, art 11(1)(b).
[145] AU Convention, art 12(2).
[146] AU Convention, art 12 (2)m.
[147] Addition Protocol to the CoE Convention, art 1(5). See also EU Directive, art 28(6).
[148] AU Convention, art 4, Chapter 1.

subject matters regulated by the Convention. For example, can a state party ratify only the data protection aspect and leave out the rest? Or can a state party, after ratifying the Convention as a whole, decide to withdraw[149] from its obligations under a particular segment? Obviously, if a state does not want to be bound by certain provisions, the right way to go about it is by way of reservation. Unlike the CoE Convention, the AU Convention does not limit the right to making reservations.[150] Nevertheless, from the human rights perspective, combining the data protection with other subject matters, like e-commerce and cybercrime, is not a commendable approach. Besides, there is the possibility that so much attention will be placed on certain aspects at the expense of others. Since cybercrime is such a notorious phenomenon currently in Africa, it is likely that it gets most of the attention. For example, there are calls from some quarters that 'African states should focus on the convention's cybersecurity and cybercrime provisions first, as it is unrealistic to expect states to implement the entire convention in a timely manner.'[151] This is problematic for effective data protection in Africa.

A second problem with the Convention is that it contains a number ambiguous and archaic provisions. For example, it consistently uses the term 'local communities' without defining it. Similarly, article 10 on 'preliminary personal data processing formalities', requires that certain 'actions' are exempted from the 'preliminary formalities'. The question then is, what is preliminary formalities? Does it refer to steps that must be taken by a data controller before the commencement of processing? This seems to be the most logical interpretation of that provision taking into account the subsections in article 10 which make provision, *inter alia*, for declaration, notification and authorisation before processing. Article 10 (2) provides that a certain category of processing must be declared before the protection authority. Similarly, article 10(4) requires that certain processing must only be carried out after authorisation by the NPA. The question that arises in this regard is how can a NPA enforce these provisions in a world of increasingly complex and ubiquitous data processing activities characterised by Web 2.0 and cloud computing applications? Here also is an example of an archaic provision, as requiring declaration and notification for certain categories of processing may be practically impossible. Every processing activity could be easily monitored when data controllers are known and carry out processing in a definite environment which is far from the case today. It is perhaps in recognition of this fact that the reforms initiated by the EU is proposed replacing the notification requirement.[152] No such provision for notification is contained in the CoE treaty.

Furthermore, the Convention contains some inconsistencies. For example, the term personal data has been defined in article 1. However, in some cases, the Convention makes reference to 'electronic data'[153] or 'physical data'[154] or even 'computerized data'.[155] Unfortunately, the Convention, like many other African international instruments, does not contain an explanatory

[149] Although, the Vienna Convention on the Law of Treaties (VCLT), in art 56(1) provides that a treaty without provision on withdrawal is not subject to withdrawal. Nevertheless, the right to withdrawal may be may be implied from the provisions of the AU Convention, art 38(4). Thus, this satisfies the provisions of article 56(2) of the VCLT.
[150] See CoE Convention, art 25. However, international law scholars, like Viljoen argue that 'a boundless discretion [to enter reservation] could result in the absurd situation where a state ratifies a treaty, but then enters reservations to just every important aspect thereof.' (n 32) 26.
[151] Tamarkin (n 19).
[152] De Hert & Papakonstantinou (n 115) 139.
[153] AU Convention, the preamble.
[154] AU Convention, art 8
[155] AU Convention, art 1

memorandum which may aid in the understanding of its provisions. On another level, there are a number of patent omissions from the Convention. For example, it does not contain a provision for data breach notification or privacy impact assessment. These are important features of modern-day data protection instruments. This is a reason why they are provided for in the reform process of the CoE Convention[156] and the EU Directive.[157]

Perhaps, the most serious problem of the Convention is the absence of a provision establishing a supervisory authority at the regional level. While the Convention requires member states to establish NPAs, there is no body linking their activities so as to ensure harmonisation (and increased cooperation) at the continental level. Article 32 of the Convention merely provides that the AU Commission Chairperson is responsible for implementing the Convention, but this cannot be a viable proposition for a regional data protection body because of the expertise needed. Both the CoE and EU have such a body. In the CoE Convention, a 'Consultative Committee' is established comprising of representatives of each state party.[158] The functions of the Committee include making proposals for facilitating and improving the Convention and expressing opinions on any questions regarding the application of the Convention.[159] Article 29 Working party plays a similar role under the EU Directive.[160] The AU may consider establishing a specific body for this purpose.

Some of the Convention's provisions are couched in a 'broad fashion' allowing member states to 'domesticate' or 'incorporate' in a manner that suits their local circumstances. This gives states some latitude to provide for specific details in their laws. It also 'helps battle obsolescence in the face of technological developments.'[161] However, there is a problem with this method especially in the African context. Firstly, it may undermine efforts at harmonisation and secondly, there is no strong obligation on states to ensure that the standard established by the Convention is the minimum standard. The Convention merely requires NPAs to ensure data processing is consistent with the provisions of the Convention.[162] The implication is that state parties can enact data protection legislation with a far lower standard. The CoE Convention provides useful lessons in this regard. Article 11 encourages member states to provide 'a wider measure of protection' than that stipulated in the Convention. Thus, the principles in the CoE Convention 'constitutes only a basis on which states may build a more advanced system of protection.'[163] This is a useful lesson for the AU.

### 5.2. Other problems

Some other problems of a general nature may impede the smooth and expeditious realisation of the objectives of the Convention.

---

[156] See proposals for modernization of the CoE Convention, art 7(2).
[157] See draft EU Regulation, arts 31 & 32.
[158] CoE Convention, art 18(2).
[159] CoE Convention, art 18(3), in fact, the committee has been renamed as 'convention committee' and further strengthened in the proposals for modernization of the CoE Convention. See art 19. See also Greenleaf (n 136) 6.
[160] See EU Directive, art 29. It has also been replaced with a permanent European Data Protection Board and its powers has also been expanded in the draft EU Regulation. See arts 64-72. See also De Hert & Papakonstantinou (n 115) 141.
[161] Comment made by Bygrave with regard to the modernization efforts of the CoE Convention. (n 34) 40.
[162] AU Convention, art 12(1).
[163] Explanatory report to the CoE Convention, para 61.

The first issue is the general 'African problem' towards international (human rights) treaties. Ratification is the first problem in this respect. For example, the AU Convention has been adopted since June 2014. So far, no African state has ratified the Convention.[164] The Convention further complicates this 'African problem' by requiring at least fifteen (15) African countries to ratify it before it can come into force.[165] Attaining this number will not be easy which means it may take a very long time (possibly, years) before the Convention takes effect.[166] Even if the number of ratifications is attained, there are other hurdles. One such hurdle is that African states often ratify treaties without taking the necessary steps to implement them. Indeed, '[w]hen states ratify international human rights treaties, they undertake to domesticate and comply with their provisions.'[167] But such is rarely the case. The dualist nature of the relationship between international and domestic law which prevails in many African states further complicates this problem. For an international treaty to have legal effect, such a treaty must not only be ratified but must also be domesticated.[168] Without domestication, the AU Convention (unlike the ECOWAS Supplementary Act) is just like any other instrument since it is a non-self-executing treaty.[169] Thus, individual rights cannot be derived from it.

Besides the challenges of ratification and domestication (incorporation), another serious 'African problem' is compliance. Viljoen notes that 'the greatest challenge [in Africa] is to bring about compliance with the treaty provisions by government officials and nationals alike.'[170] Unfortunately, the Convention does not contain a provision providing sanctions for state parties who do not comply. Indeed, even the AU Constitutive Act 'is vague on enforcement and the imposition of sanctions in cases where states do not conform to AU norms.'[171] According to Makulilo, the lack of clear sanctions on member states who do not establish a framework will definitely undermine compliance level.[172] But then, Viljoen points out, quite rightly, that 'international legal norms only become truly effective if compliance is not motivated by coercion or self-interest, but flows from personal motivation brought about by an internal process of norm acceptance ('internalization').'[173]

A third problem which may be an obstacle to the AU Convention is the general African attitude towards privacy. The prevailing perception is that the concept of privacy is alien to Africa

[164] In fact, even the details of the Convention and its status list are yet to be uploaded on the AU website of treaties, conventions, and protocol. See http://www.au.int/en/treaties (accessed 27 January 2016).
[165] Article 36 provides that 'This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification.' This is Unlike the CoE which merely requires ratification by 5 countries to take effect. See CoE Convention, art 22(2).
[166] Indeed, history has shown attaining 15 ratifying state will be a huge challenge. see Vijoen (n 29) 156.
[167] Viljoen (n 29) 9.
[168] Especially, common law countries for example Nigeria, based on sec 12 of the Constitution of the Federal Republic of Nigeria.
[169] The treaty provides as an objective that 'Each state party shall commit itself to establishing a legal framework aimed…' AU Convention, art 8. Note that a non-self- executing treaty according to Vázquez, is "a treaty that may not be enforced in the courts without prior legislative 'implementation'." See CM Vázquez, 'The Four Doctrines of Self-Executing Treaties' (1995) 89 *The American Journal of International Law* 695. He relied on a host of US cases like *Frolova v. Union of Soviet Socialist Republics*, 761 F.2d 370, 373 (7th Cir. 1985); *Tel-Oren v. Libyan Arab Republic*, 726 F.2d 774, 808 (D.C. Cir. 1984).
[170] (n 29) 25.
[171] *Ibid*, 165.
[172] Makulilo (n 32) 87.
[173] Viljoen (n 29) 25.

because of its communal orientation as against individualism which is perceived to be a Western idea.[174] Individualism goes with privacy and communalism is the antithesis. Even the African Charter on Human and Peoples' Rights (ACHPR) does not contain a right to privacy. In trying to rationalise the omission of privacy from the catalogue of rights in the ACHPR, Olinger *et al* contend that 'privacy was simply not seen as a necessary right for Africans to live freely and peaceably.'[175] Another commentator contends that Africans generally suffer from 'privacy myopia' which means they underestimate the value of their personal data and the need for its protection.[176] Although scholars like Makulilo strongly reject the 'so-called' African conception of privacy, it must be admitted that privacy is still a largely underdeveloped concept in Africa. This will definitely have an effect on the implementation and compliance with the AU Convention. Many African leaders will not attach so much importance to the Convention and will prefer to rather focus on more contentious human rights issues. This may be a reason why there is as yet no ratification. Implementation of the Convention will definitely suffer because of the lack of political will.

The AU Convention will also have to compete with other data protection regimes. On the one hand, the EU Directive has been a major force in the adoption of data protection law in Africa.[177] Thus, African states prefer to adopt the EU-style data protection law so as to serve as a first step in satisfying the EU's adequacy requirement as contained in article 25 of the EU Directive. The EU's regime may, however, not be a problem *per se* since the AU Convention has basically similar provisions with the EU Directive. On the other hand, the AU Convention has to contend with regional data privacy instruments. African states tend to pay more allegiance to their sub-regional bodies than the AU. Rationalising the basis for this, Viljoen states:

> The scale of the subregional is smaller than that of the continental level: it has greater geographic proximity, allowing for strategic closeness. It also has greater potential for trade links, increasing the immediacy of mutual incentives, presenting closer linguistic and cultural ties, and holding the promise of greater effectiveness in implementation and enforcement…[178]

If subregional instruments provide for similar principles as the AU Convention, then, this will not be so much of a problem. The difficulty arises if a subregional instrument makes provision that conflict with those of the AU Convention. It is then that allegiance becomes an issue. While the AU Convention acknowledges existing instruments of RECs, its ability to bring their provisions in harmony with the Convention remains to be seen. Besides, some RECs, arguably, have relatively long-standing and more advanced data protection regimes than that of the AU Convention.[179]

The success of the Convention will very much depend on how well it is able to integrate and coordinate prior subregional and domestic initiatives on data protection. However, it would seem that 'integration on an Africa-wide scale is extremely ambitious' especially because of the

---

[174] See LA Bygrave, 'Privacy and data protection in an international perspective' (2010) 56 *Scandinavian Studies in Law* 165-200. S Gutwirth *Privacy and the information age* (Rowman & Littlefield Publishers, 2002).
[175] HN Olinger *et al*, 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *The International Information & Library Review* 31, 37.
[176] EM Bakibinga, 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan Perspective' (2004) http://www.thepublicvoice.org/events/capetown04/bakibinga.doc (accessed 27 January 2016).
[177] Makulilo (n 67 ). See also MD Birnhack, 'The EU Data Protection Directive: An engine of a global regime' (2008) 24 *Computer Law & Security Report* 508-520.
[178] Viljoen (n 29) 470.
[179] For example, ECOWAS.

population and size of the continent.[180] This will be the more difficult since there is an absence of a continent-wide normative standard for privacy in Africa's principal human right instrument, the ACHPR.

Finally, the tension between data protection and other human rights may also be a challenge to the effective implementation of the Convention. In this regard, the right to freedom of information (FOI)/access to information comes to light. Unlike the right to privacy, freedom of information is guaranteed and protected under the ACHPR.[181] In Africa today, there an intensive campaign by CSOs and others drive for states to adopt and implement freedom of information legislation because of the strong desire for accountability of public office holders. Data protection is usually seen as antithetical to freedom of information since the former, in a way, restricts access to information while the latter promotes its free access. Thus, unlike data protection, freedom of information has attracted more attention from several actors which has led to its relative success on the continent. It is important to state that while both human rights seem conflicting, there are, in fact, meant to serve different objectives which should not create any tension.[182] Besides, both rights 'complement each other in holding governments accountable to individuals.'[183]

## 6. Conclusion: A reason to celebrate human rights in Africa?

2016 is a very significant year for human rights in Africa. According to the Vice-President of the African Court of Human and People's right in an address, '…2016 is a veritable watershed in the continental human rights trajectory: 2016 marks the 35th anniversary of the adoption of the African Charter in 1981; the 30th Anniversary of the entry into force of the African Charter in 1986; the 29th Anniversary of the operationalization of the commission in 1987… The year also marks the 10th Anniversary of the operationalization of the African Court.'[184] Because of the significance of 2016 to Africa, the international community will certainly pose some critical questions regarding the state of human rights. One such question is how human rights have fared in the face of relative advances in technology on the continent. Privacy and data protection will definitely attract more attention because of challenges advances in technology pose to their effective protection. The international community and relevant stakeholders will be interested in knowing what measures have been taken in advancing the right to privacy and data protection. Similarly, the international business community in particular, will want to know whether Africa is a safe destination for the transfer of personal data for business purposes. The state of privacy and data protection is therefore critical in establishing whether or not human rights can indeed be celebrated on the continent especially in this digital age and information society.

---

[180] Viljoen (n 29) 471.
[181] ACHPR. Art 9.
[182] For more on the conflict between both human rights, see D Banisar, 'The right to information and privacy: Balancing conflicting rights and managing conflicts' working paper, World Bank available at https://www.ip-rs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf (accessed 7 April 2016)
[183] *Ibid*, 1.
[184] Address by Hon. Justice Bernard M. Ngoepe, Vice President of the African Court on Human and Peoples' Rights, on the occasion of the Opening of the 55th Ordinary Session of the African available at http://www.achpr.org/sessions/55th/speeches/opening-statement-court/ (assessed 27 January 2016).

The initiative of African leaders through the AU in agreeing to this landmark Convention on data protection is definitely laudable. It shows that Africa is now ready to move a step further in human rights protection as part of its strong desire to build a credible information society. A number of important questions must, however, be answered to determine whether the Convention is a possible reason to celebrate human rights in Africa. Firstly, is the Convention in harmony with best practices on data protection? This question is significant because of the transboundary nature of information processing. It is therefore very important that the AU Convention is consistent with other influential data protection instruments. In this respect, the AU Convention can be celebrated as its provisions are, *prima facie*, a combination of the CoE Convention and EU Directive. Besides, it is provided in the Convention that its provisions 'shall not be interpreted in a manner that is inconsistent with the relevant principles of international law.'[185] Although it contains a number of ambiguous provisions, member states can extract its contents and incorporate it into their domestic legislation. Nevertheless, it is submitted that the provisions of the Convention must be used as a minimum standard in enacting data protection legislation by state parties.

Secondly, and most importantly, is the question of implementation and compliance. As earlier noted, ratification is not a problem *per* se in Africa, rather, implementation of (human rights) treaties is the big problem. This raises a lot of concern. The AU may face a particularly difficult challenge with regard to the implementation of the Convention because of the general attitude of Africans towards privacy related issues. The Convention further complicates the situation by giving states too much leeway towards compliance with its provisions. Perhaps, this was done because of the weak conception of privacy on the continent. Thus, it was thought that there should be some latitude given to state parties to decide on implementation based on their local circumstances. If this state of affairs remain, the Convention will just be another human rights treaty which African countries merely ratify on paper without implementing.

African leaders need to understand that data protection is an imperative, therefore necessary mechanisms must be put in place to ensure that the Convention is not only domesticated but enforced. Governments have to appreciate the fact that they have the responsibility to 'respect', 'protect', 'fulfil' and 'promote' human rights. These obligations apply equally to all human rights.[186] The AU must also, at the regional level, put in place appropriate mechanisms to ensure that parties not only ratify but strictly comply with their treaty obligations. Effective monitoring mechanism/agency must be established. This agency should adopt innovative mechanisms, such as state reporting and fact-finding missions, to ensure compliance. Furthermore, individual countries and RECs must ensure that their regimes are in harmony with the AU Convention. Since the AU is presumably the proper institution to set human rights standard on the continent, RECs' initiatives must be consistent with the AU Convention. This will go a long way in facilitating the easy flow of personal information within and across Africa. Similarly, a clear relationship must be established between the AU Convention and the RECs' initiatives. In this regard, the AU must ensure that the Convention plays a leading role in steering data protection on the continent. As such, regional (and domestic) initiatives must be consistent with the AU Convention. On the whole, the AU must appreciate the fact that while building a credible information society is crucial for economic development on the continent, human rights protection is equally important and should take precedence.

[185] AU Convention, art 33.
[186] Vijoen (n 29) 6.

On the whole, it is submitted that the fact that the AU adopted this Convention shows that data protection is, at least, recognised as crucial. On this basis, human right may be celebrated in Africa. However, much more needs to be done by the AU for the international community to take Africa serious on this subject matter.