Data Protection Legal Regime and Data Governance in Africa: An Overview

Olumide Babalola

Working Paper DG-003

Bringing Rigour and Evidence to Economic Policy Making in Africa

AFRICAN ECONOMIC RESEARCH CONSORTIUM
CONSORTIUM POUR LA RECHERCHE ÉCONOMIQUE EN AFRIQUE

Data Protection Legal Regime and Data Governance in Africa: An Overview

By

Olumide Babalola[1]

AERC Working Paper DG-003
African Economic Research Consortium, Nairobi
February 2023

THIS RESEARCH STUDY was supported by a grant from the African Economic Research Consortium. The findings, opinions and recommendations are those of the author, however, and do not necessarily reflect the views of the Consortium, its individual members or the AERC Secretariat.

Published by: The African Economic Research Consortium
P.O. Box 62882 - City Square
Nairobi 00200, Kenya

Contents

Abstract

In its simplest sense, Data Governance refers to the overall management of (personal and non-personal) data to facilitate organizational goals. Data Protection, on the other hand, predominantly regulates the management of personal data for the overall protection of users' privacy and other fundamental rights and freedoms. The Fourth Industrial Revolution has greatly increased the processing of personal data for business and social purposes in Africa, hence the imminent need to regulate dealings with such personal information for undesirable purpose(s) by setting up relevant legal frameworks to address the unfavourable effects on humans, whose personal information are utilized for sundry purposes. This research paper analyses the regional legal framework around data protection in Africa in the light of their salient provisions, adequacy, efficiency, and enforceability in relation to data governance on the continent. The paper makes some juxtaposition with the European Union General Data Protection Regulation in relation to its remote or immediate impact on the African legislation on data protection. The research exposes the inadequacies of the data protection legal framework and the non-existent mechanism for cross border transfers of personal data, which ought to be regulated by the existing Data Protection Authorities (DPAs) in Africa. The paper then concludes with some incentives for data protection within the context of data governance on the continent.

Keywords: *data protection, data governance, GDPR, Malabo Convention, personal data*

1. Introduction

Overview

Data protection reportedly surfaced in Europe in 1970 when the German Federal State of Hesse (Mayer-Schonberger,1997) enacted its data protection law, which was followed by the Swedish National Data Act in 1973 (Oman, 2010). In Africa, the Republic of Cape Verde led the way in 2001 when it enacted the first data protection law in Africa. The Cape Verdean Data Protection Act was passed on 22nd January 2001 to create a legal framework for protection of personal data in the country (Makulilo, 2012).

Unlike in Europe where member States transposed the provisions of the regional international instruments into their various municipal legislation on data protection, Cape Verde heavily relied on Portuguese Data Protection Law, which itself transposed the EU Data Protection Directive 95/46/EC[2] before it was replaced by the EU General Data Protection Regulation –GDPR (Traca, and Embry, 2011). Between 2001 and 2014 when the first and only pan-African international treaty on data protection was adopted in Equatorial Guinea,[3] 14 African countries[4] had already enacted their respective data protection laws without the benefit of drawing legislative inspiration from the convention, as most of the laws were modeled after European data protection legal framework (Greenleaf and Cottier, 2018).

In a description approach, this paper examines the major international instruments regulating data protection in Africa by briefly chronicling the events that culminated in their adoption, vis a vis their aims and objectives. The paper also analyses the salient provisions of the instruments in light of their applicability and the extent to which they have sharpened data protection compliance on the continent. This paper then analyses the nexus between data protection and data governance in Africa within the context of regional instruments, and it then concludes with the necessity of legal framework for data protection in relation to data governance in Africa, with some recommendations that could be adopted to either develop new or strengthen the existing data protection frameworks, especially in relation to data governance.

Research questions

This paper, in a descriptive and normative manner, poses and analyses a number of questions, thus:

(i) What are the laws or quasi-legal guidelines (legal framework) that regulate or support data protection in Africa?

(ii) How does this legal framework measure up to international standards?

(iii) How enforced or enforceable is the framework on the continent?

(iv) In what manner does this framework influence or ought to influence data governance in Africa?

(v) What are the incentives for data protection and data governance on the continent?

2. Legal framework on data protection in Africa

Unlike what is obtainable in the European Union (EU) where the General Data Protection Regulation (GDPR) provides some sort of formidable harmonization of the erstwhile irregular data protection laws across the Union, its African counterpart does not have a Pan-African legislation that is immediately enforceable across board without domestication. This is not, however, to say that Africa does not have an existing legal framework on data protection; the elephant in the room remains the institutional capacity and political will to enforce the available instruments. This paper discusses the extant legal framework for data protection on the continent.

African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention)

Conversations around regulation of cyberspace effectively began in the late 1990s when the committee of the United Nations General Assembly contemplated an instrument on 'disarmament and international security', whose deliberations were spearheaded by a draft resolution introduced by Russia in 1998 (Kavanagh, 2017). Upon Russia's proposal, the United Nations subsequently constituted a Group of Government Experts (GGE) engaged on the developments in the field of information and telecommunications in the context of international security.

In one of its reports,[5] the GGE's notes that: "The use of ICTs in future conflicts between States is becoming more likely, the risk of harmful ICT attacks against critical infrastructure is both real and serious, and States are rightfully concerned about the danger of destabilizing misperceptions, the potential and economy deriving from the difficulty of attributing the source of an ICT incident" (Tikk and Schia, 2020). However, the UN's activities around cybersecurity did not spur many African countries into the anticipated regulation on data protection, as only 11 member States[6] had instituted frameworks on data protection as of 2011 (Ball, 2017).[7]

In 2011, the African Union (AU) took a bold step towards regulating data protection when it published a draft AU Convention on Establishment of a Credible Legal Framework for Cybersecurity in Africa,[8] which sought to, among other objectives, harmonize the laws of member States on data protection and sundry matters (Orji, 2012). In 2013, the draft was reviewed and renamed the African Union Convention on the Confidence and Security in Cyberspace,[9] but it was further reviewed and went

through another name change that culminated in the AU Convention on Cybersecurity and Personal Data Protection in 2014, which was preceded by a conference of experts from AU member States' ministries of justice where the content of the convention was thoroughly considered Abdulrauf, 2021).[10]

Ultimately, on 27th June 2014, during the 23rd Ordinary Session of the AU Summit in Malabo, Equatorial Guinea, the draft Convention on Cybersecurity and Personal Data Protection[11] was adopted by the Heads of State to establish a credible framework for cybersecurity in Africa through protection of personal data.[12]

The Malabo Convention has a total of 38 articles, preceded by a 20-paragraphed preamble. The Convention seeks to encourage member States to create frameworks and mechanisms to protect personal data and fundamental rights, and ease the free flow of data within the continent. The first Article defines essential data protection terms such as consent, data controller, data subject, direct marketing, encryption, health data, personal data processing, recipient, sensitive data, third party, etc but surprisingly omitted the definitions of equally important concepts such as: pseudonymization, data processor, data breach, data protection authority or supervisory authority and cross-border processing. While one may argue that the omission of such terms does not superficially appear far-reaching, the Convention is meant to be a compass for data protection laws on the continent as gleaned from its Articles 8(1) and (2), which seek to establish a framework for protection of 'physical' data and a mechanism to ensure data processing guarantees the protection of fundamental rights. Yet, even this falls short of the status of a legislative model in such material respect. Therefore, it is desirable that the Convention is supplemented by relevant instruments to comprehensively define the omitted regular and fundamental data protection clauses, otherwise, its enforcement may engender unimaginable conceptual confusion.

The Convention applies to automated or non-automated processing[13] of personal data within the territory of a member State.[14] Like the GDPR, the Convention does not provide a definition or description of what constitutes 'automated' or non-automated processing but the European law defines 'profiling.'[15] Automated processing has, however, been defined as 'a processing operation that is performed without any human intervention, conversely, non-automated processing is such that it is performed partly or wholly with human intervention.[16] Profiling and automated decision-making within the African context is increasing in the banking sector, especially with the rising development of FinTechs and proliferation of automated teller machines (ATM); however, there exists no pan-African legislation on this.

The Convention requires member States to establish independent national authorities assigned with the statutory responsibility of ensuring that personal data within their respective territories are processed in accordance with the provision of the convention, while keeping faith with the universal role of Data Protection Authorities – DPAs (Giugiu and Larsen, 2016).[17] The Convention expects the respective national DPAs to educate the public on their data protection rights within their respective territories,[18] while its membership is insulated from government influence and thereby

underpinning their independence and impartiality.[19] As at June 2021, out of the 30 countries with proper data protection laws in Africa, only 20 have data protection authorities (DPAs).[20] Others are either yet to establish one or constitute its members. The Convention clearly makes provisions for the duties and powers of the DPAs to include informing the public of their rights, issuing opinions, receiving and resolving complaints, data processing audit, imposing administrative decisions, maintaining a data processing directory, regulating trans-border transfer, establishing cooperation mechanisms with other national DPAs,[21] authorizing certain processing activities,[22] data involving genetic information, information on offences, national identification number, biometric data, historical and statistical data, among others.

In what appears a renaming and re-arrangement of the universally recognized principles of data protection, the Convention groups consent together with legitimate processing,[23] separate from the principle of lawfulness and fairness. It then fuses purpose with storage limitation[24], then accuracy, and transparency stand-alone while confidentiality is grouped with security of personal data.[25] In all, the Convention recognizes six re-designated principles, none of which contemplates the principle of data minimization or accountability as recognized under European law, even though it provides for specific principles in the event of processing sensitive personal data.[26] The consequence of such regrouping and muddling of principles would not only be evident in enforcing the clustered concept, it is potentially capable of confusing data controllers on their obligations.

The Convention, like most other data protection laws, recognizes data subject's right to information, right to access, right to object, rectification or erasure, but it again omits the right to lodge complaint with the regulator, right to data portability, restriction of further processes, etc.[27] It also mandates data controllers to ensure confidentiality and security of personal data in their custody.[28]

Although the Convention was adopted in 2014, it is yet to enter into force by reason of Article 36, which makes it enforceable only 30 days after its ratification by 15 member States. As of 20th June 2021, only Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda, Senegal and Zambia have ratified the Convention.[29] In spite of its limitation, Abdulrauf (2021) however argues in favour of the Convention's perceived expansive provision and authoritative stance especially as far as they influence subsequent data protection legislation on the continent.

Supplementary Act on personal data protection within the ECOWAS (ECOWAS Act)

The Economic Community of West African States (ECOWAS) was established for the promotion of regional cooperation among member States, especially for economic growth, among other objectives (Terwase et al., 2015). Its consequent ECOWAS Treaty mandates the harmonization and coordination of national policies and promotion of integration programmes in science, technology, legal matters, etc.[30]

On 16th February 2010, 12 Heads of government within the ECOWAS gathered in Abuja, Nigeria and adopted the Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS[31] (the Act), which predominantly seeks to regulate data protection within the member States.

The Act defines data protection terms such as consent, data protection authority, personal data, sensitive data, health data, data subject, data controller, data processor, third party and recipient[32] but omits important terminologies such as processing, profiling, pseudonymization, anonymization, profiling, personal data breach, cross border, etc. The consequence of the omission may, however, come to play when the Act is invoked to settle issues relating to transborder processing of data especially before the regional courts when faced with questions of conflict of laws and decision on lead national DPAs, etc.[33] The Act applies to processing of personal data by public or private bodies by automated or non-automated means carried out within the ECOWAS, with exceptions.[34]

The Act mandates each member State to establish its own independent national DPA, with parameters guaranteeing their impartiality, professional secrecy[35] and highlights the responsibilities and powers of DPAs secrecy with powers to impose sanctions on erring parties.[36] In its own version of seven data protection principles, the Act states that processing is legitimate where it is done with data subject's consent but gives exception where the requirement of consent can be dispensed with.[37]

The second principle of legality and fairness requires processing to be done in a legal, fair and non-fraudulent manner.[38] In what appears a bifurcation of some sort, the Act separates consent, which is a ground of lawful processing from the principle of legality and fairness, which is fused under the EU principle of lawfulness, fairness and transparency (Kosta, 2013). As its third principle, the Act fuses purpose limitation, data minimization storage limitation into one principle styled 'principle of purpose, relevance and preservation,[39] which requires data to be obtained for specific purpose, kept adequate and not kept beyond the required period. The principle also imports an element of the lawfulness principle.[40] Other principles are accuracy, purpose relevance and preservation, transparency, confidentiality and security and choice of data processor.[41]

Taking a cue from the European model on transborder transfer of data to third countries, the Act restricts transfer of personal data outside ECOWAS sub-region to only countries where there is an adequate level of protection[42] for fundamental rights and freedoms. Although the Act does not provide elaborate mechanisms for regulating such transfers, it simply mandates data controllers to inform DPAs before the transfers.[43] On data subject's rights, the Act recognizes the right to be informed,[44] right to access,[45] right to object,[46] right to rectification and destruction.[47] Again, the Act omits vital data subject's rights, such as right to restriction of further processing, right to data portability, right in relation to automated decision-making, etc. The Act substantially concludes on the obligations of data controller to be confidentiality, security, preservation, and durability,[48] which obligations however appear similar to data protection principles in their objectives.

Southern African Development Community (SADC) Model Law on data protection

In 2009, the imperativeness of creating a harmonized and uniform set of policies for the information communication technology industry for Sub-Saharan countries in the group of African, Caribbean, and Pacific States necessitated the enactment and adoption of the Southern African Development Community (SADC) Model Law on Data Protection,[49] which was adopted in 2013. Like many data protection laws, the Model Law defines terminologies such as consent, data controller, processor, data subject, genetic data, child personal data, processing, protection authority, recipient, sensitive data third party, and transborder flow. The law, however, does not define anonymization, pseudonymization, profiling, personal data breach, data subject access request, etc.

From the wording of Article 2, it appears that the scope of the law is not limited to the SADC sub-region as it only refers to 'given country' or territory', which terms are not even defined therein. Even from the preamble, it does appear that the model law is not restricted to any region especially as contained in the concluding paragraph that:

> "It is with the above in mind that it is acknowledged that the protection of personal data involves the establishment of a specific and adapted regime to the participants of each region as set out in this Model Law."

In spite of its Pan-African scope, the Model Law is a soft law without a legally binding effect on member States, but like the OECD Guidelines in Europe, they only provide a guide to member States on the approach to law-making on data protection and an attempt at harmonizing the laws in the region (Shumba, 2015).

The law envisages the establishment of an independent regulator for member States to be constituted by judges appointed by the executive and non-governmental organizations with competent and requisite knowledge of data protection and the benefit of immunity.[50] Unlike other regional instruments in Africa, the model law provides the most comprehensive provisions on the nature, independence duties and powers of national DPAs, but it unfortunately contemplates the DPA reports to an undefined institution instead of Parliament,[51] and thereby erodes its independence (Greenleaf, 2012). The Model Law recognizes the principle of data quality, lawfulness and purpose limitation and it makes copious provisions on processing of sensitive and non-sensitive data, children's data, data relating to litigation,[52] but it however omits principles such as data minimization, storage limitation accuracy, accountability, integrity and confidentiality, etc. The Law outlines the duties of controllers in cases where personal data is collected directly from data subjects and otherwise, duty to ensure data security and accountability for third parties that access data through them, data breach or incident notification.[53]

The law also recognizes the following data subject's rights: access, objection, automated decision-making right of representation and right to judicial redress.[54] Under the Law, members of DPAs are meant to be administered to oath of secrecy[55] as they are empowered to impose fines on controllers for violation and prosecution of offenders in the law court.[56] The Law subjects cross-border transfer of data to the relevant provisions of the national law adopted for the implementation of the Model Law, and this appears as the only provision that is fixated on member States of the SADC as it requires adequate level protection before personal data can be transferred to non-member States.[57] Although the law references adequacy level, unlike the EU GDPR, it does not provide the parameters for determination of such level of protection.[58]

Despite the laudable provisions of the Model Law, it merely serves as an advisory framework for the enactment of national laws as opposed to a legally binding instrument that can be ratified.[59]

East African Community (EAC) Legal Framework for Cyberlaws 2008

In its strides to deepen East Africa's regional integration via digital interconnectivity for the seamless provision of services, the East African Community constituted a task force which recommended a legal framework for cyberlaws[60] with the main objective of developing policies facilitating cooperation between member States (Mwiburi, 2019).

The Framework defines 'data protection' as the obligations assigned to entities processing personal data. It also recognizes that a data protection regime ought to guarantee certain data subjects' rights.[61] Thereunder, data controllers are duty bound to comply with muddled principles of accountability, transparency, fairness, lawfulness, data accuracy, data security and processing limitation.[62] The Framework omits data minimization, purpose limitation and accountability but suggests a self-regulatory system to minimize costs associated with conventional compliance enforcement approach.[63]

Without prejudice to its progressive but brief provisions on data protection, it is a mere framework for member States but not legally binding on them until they transpose the provisions into their respective national laws (Greenleaf et al., 2014). It is worthy of note that the legal framework remotely or otherwise influenced the data protection legislation in Kenya, Uganda and Rwanda, which passed the legislation afterwards.

3. Interplay between data governance and data protection in Africa

Data Governance is the 'exercise of authority and control over the management of data' (Abraham, et al., 2019). It also entails the trust reposed in data and its accountability for any adverse result occasioned by its poor quality. The whole gamut of data governance as a concept speaks to the data processing principle of accountability (Weber et al., 2009). Otto et al. (2007) define the concept as a 'companywide framework for assigning decision related rights and duties to be able to adequately handle data as a company asset'. It is the 'formal orchestration of people, process and technology to enable an organization to leverage data as an enterprise asset' (Zornes, 2006).

Data Governance is concerned with the apportionment of responsibilities and liabilities among the various players in a data management system with respect to the decision-makers' rights, and accountability over an entity's data assets. While data governance principally relates to collection and management of data that ensures effective and efficient use for the overall productivity of an entity (Cheong, et al., 2007) data protection safeguards the collected personal data[64] from misuse, compromise, and/or corruption within the confines of certain principles. It is instructive that data governance is not restricted to personal data but data protection in this context only protects the personal data managed alongside the big data[65] under the data governance framework. Therefore, certain principles of data processing significantly impact data governance as far as personal data handled by the legal entity is concerned.[66] Unlike in Europe where the principles of data processing are uniformly provided by the GDPR,[67] the only readily binding and enforceable regional instrument in Africa is the ECOWAS Supplementary Act on Data Protection (Greenleaf, 2020). The AU Convention on Cybersecurity is not yet in force as its commencement provision has not been activated since less than 15 members have signed it.[68]

Notwithstanding its comatose State, the Convention provides for the principles of accuracy and storage limitation[69] but it does not expressly provide for accountability.[70] However, this principle is an offshoot of the transparency principle (Alhadeff, et al. 2021), hence since the Convention provides for the latter, accountability can be discussed thereunder in relation to data governance. Since the Malabo Convention is pan-African in its coverage, I will discuss some of its principles which interplay with data governance in Africa albeit in its current unenforceable predicament.

Accuracy principle

Accuracy is one of the components of data quality (Cong et al., 2017). The principle of accuracy entails the accuracy, completeness, and consistency of data and it goes without saying that organizations require the highest quality of data for them to function optimally (Joshi, 2021). In an entity's use of (personal) data, privacy issues such as transparency, security, compromise of (personal data) are always thrown up and sometimes the relevant questions are left unanswered. Bair (2004) notes that, data quality is defined by 'data type and domain, completeness, uniqueness, and referential integrity, consistency across all data bases, freshness and timeliness and business rules conformance'.

On the relationship between the principle of accuracy and data governance, Cohn (2015) argues that 'data governance is a catalyst for quality and value is derived from well governed quality data. Relevant, timely, consistent, reliable and accurate data is an expectation and it is not achieved serendipitously. In data protection parlance, the principle of data quality[71] requires personal data to be effective, fit, relevant and all-embracing for its intended purpose of processing.[72] The principle stipulates that, when organizations use client data for decision-making, they must ensure that such personal information are not only utilized in a manner that is relevant to the purpose of collection but they must also be accurate, wholesome and regularly updated. This will ensure that personal information used for critical organizational decisions are accurate to prevent undue violation of fundamental rights and freedoms of data subjects (Lee, 2002).

Under this principle, organizations (private and public) are duty bound to ensure the accuracy of information they keep and opinions that they express regarding data subjects especially when decisions affecting the latter are made (Hallinan and Borbesius, 2020). It mandates data controllers to take reasonable steps to ascertain the aptitude of personal information processed within the context of their organizational activities. As a representation of this principle, Article 13, principle 3 of the Malabo Convention mandates data collection to be adequate relevant and not excessive in relation to the proposes for which they there collected.[73] Ultimately, legal entities must set up mechanisms to ensure the validity and quality of personal data in their custody by imbibing a business culture of periodic updates and timely deletion of the outdated or irrelevant ones.

Storage limitation

Storage of data is one of the main components of data governance. Sometimes, they are stored indefinitely in unregulated and unguarded databases for the controllers' whimsical analyses and/or utility, often time without the consent of data subjects (Pike, 2020). The passage of data protection legislation in Europe, for example, threw many organizations into panic mode especially when auditing the legal bases for collecting

and/or storing online visitors' data through their digital platforms without necessarily fixing the mechanisms for obtaining informed consent (Francesco et al., 2021). While businesses are not precluded from storing customers' personal data, such storage must be within the confines of the applicable data protection laws and its exceptions (Duceto, 2020). For example, data processing for research purposes constitutes one of the exceptions to the principle of storage limitation, since data can be kept for longer than necessary especially for verification of research results (Pormeister, 2017).

The indiscriminate and indefinite storage of customers and other data subjects' personal data by organizations pose unimaginable privacy risks attributable to unregulated and most times, insufficient and inadequate technical and organization security measures (if any) by data controllers (Biega and Finick, 2021). Essentially, personal data must not be kept in a form that identifies data subjects for longer than is justifiable by law. Where personal data is no longer needed or it has become irrelevant or out of date, data controllers can either outrightly delete, anonymize or pseudonymize them in certain cases (Mourby et al., 2018).

Under the AU Malabo Convention, storage limitation is, however, not a principle but an obligation on the data controllers. Article 22 emphatically prohibits personal data from being kept for longer than necessary for its purpose of collection, but the provision is bereft of exceptions or parameters for the applicable retention period. The principle interplays with data subject's right to be forgotten or deletion or erasure of personal data, which is no longer relevant or up to date. Without prejudice to the circumstances surrounding an organization's collection of personal data, this principle still operates to provide them from keeping and/or storing the data for longer period than reasonably necessary. Therefore, once data has been used for the purpose of collection, it behoves the organization to immediately delete or anonymize such personal data to reduce the risk of violating the principles of data minimization and accuracy when they become irrelevant, surplus to requirement, inaccurate or outdated. There are no specific retention periods in the regional instruments; however, the relevant national laws should be consulted on data retention limits but ultimately a formidable data governance policy ought to be devised to plug the legislative gaps in this regard.

Legislative and stakeholder's engagement for data governance, however, becomes very important when it is considered that out of 55 African countries, at least 49 have (or about to) enacted laws or regulations requiring prospective subscribers to provide personal data as conditions to own telephone lines (Donovan and Martyin. 2013), but sadly only about 19 of those countries have established Data Protection Authorities[74] to enforce compliance with relevant data protection laws.

Accountability

This principle originated from the OECD Guidelines[75] of 1980 and is repeated in its revised version of 2013. The principle principally requires legal entities to acknowledge and assume liability for their operations on personal data in the course of the organizational activities. Data controllers have the bounden duty of demonstrating

adequate technical and organizational measures to secure data in compliance with the relevant data protection legislation for the ultimate protection of data subjects' rights (De Hert et al., 2012). In compliance with this principle, legal entities are obliged to document the observance of their obligations under the relevant data protection legislation (Becker, 2019).

Accountability is not expressly provided under the Malabo Convention, but the principle is closely linked to the principle of transparency, and it has been regarded as a privacy and data protection–enhancing principle.[76] In demonstrating their accountability, organizations must take hands-on approach to data protection and privacy issues by adopting effective and contemporary measures that are not only discernable at a glance but transparently demonstrable upon regulatory request or audit (Falk, 2016).

Data controllers must take full responsibility for how they directly or indirectly deal with data and implement appropriate measures and documentation in proof of their compliance with applicable laws (Bennet, 2021). They are responsible and must demonstrate data quality.

Confidentiality and integrity

This is recognized under principle 6 of the Malabo Convention. This principle simply mandates organizations processing personal data to employ appropriate organizational and technical measures to protect such personal information from misappropriation, corruption, theft and/or destruction. Confidentiality in this sense speaks to the duty of the organization handling data to ensure that such information are not shared or exposed to unintended persons while keeping them as safe and secret as technically possible.

4. Incentives of legal framework for data protection/data governance in Africa

The benefits of data protection to data governance are numerous. However, for the purpose of this paper, I shall briefly discuss the incentives from the rights-protection and economic gains for organizations and governments.

Privacy right guarantees

Even though the African Charter does not expressly recognize privacy as a fundamental right, it does not rule out African's entitlement to enjoy private family life.[77] This idea of a privacy entitlement for individuals is what also underpins the notion of data protection. In fact, data protection originated from the right to privacy, hence a proper and formidable legal framework for data protection would not only guarantee certain data subjects' rights, but it would also ensure considerable control over their personal information and ultimately repose consumers' trust in the processing activities.

Healthy democracy

A healthy democratic State is one in which its citizens can make informed and autonomous choices (Forde, 2016). Yet, processing data without consideration for the impact it may have on individuals may have the effect of limiting the ability of individuals to make choices or limit the choices available to such individuals in a way that limits their autonomy (Feldman, 1994). This is even more crucial in today's world of technological reliance where automated processing and digital identities are gradually becoming more significant determinants of an individual's real-life choices. Data protection laws militate against this. The idea that when consent is relied upon as the legal basis for processing, it must be informed and must not be obtained using coercive tactics echoes these concerns for democratic autonomy. Furthermore, even in instances where data is processed without consent, the notion of data subjects' rights and the transparency, fairness and accountability obligations, grant the much-needed controls individuals need to maintain their ability to make truly free choices. Thus, it is safe to conclude that a world where data protection is respected is one in which the seeds of corporate or governmental totalitarianism cannot flourish.

Economic gains from free flow of data

The concept of free flow is not merely one where there are no legal barriers to cross-jurisdictional data transfers. Instead, it entails that where these legal barriers exist, they do not impose data localization requirements. Data localization requirements have the direct effect of raising the costs for doing business across jurisdictions. Particularly, for data-driven businesses such as cloud service providers, these costs have the added effects of posing significant barriers for entry into new markets within the continent. This disincentivizes the creation of such businesses and creates an environment that limits the growth of African start-ups and small and medium enterprises (SMEs). Furthermore, the free flow of personal data would ease information dissemination and beneficial collaboration of businesses and corporate entities within the region. However, these benefits extend to collaboration opportunities outside the region. The European Data Protection framework is setting the global trend for technological collaborations across the world. Implementing and initiating an African data protection framework may create an opportunity for the recognition of African countries as having an adequate level of data protection. This has the potential to facilitate more cross-border collaboration, even for non-data driven businesses looking to partner with African businesses.

5. Conclusion

Data governance predominantly speaks to the management of data for organizational growth. Experience has shown that the management of big data would always involve the handling of personal data, hence the activation of data protection principles.

Africa currently has only one binding regional instrument - ECOWAs Supplementary Act on Data Protection - among other international instruments with provisions on various principles that persuasively impart data governance on the continent. Out of 55 African countries, only 30 have fully dedicated data protection laws, and 19 of them have established DPAs to enforce compliance with the laws, hence it is crystal clear that data governance on the continent remains largely unsupported by legislative and enforcement framework.

With the magnitude of personal data exchanged, stored or transmitted within the data governance system in Africa, an appropriate and formidable data protection legal framework becomes very essential to guarantee users of control over their personal information, and to regulate the data controllers' processing/management of such information against misuse, compromise, theft or other untoward dealings with personal data.

For a properly regulated data governance, it is hoped that African countries would evenly ratify the Malabo Convention and strengthen their respective municipal data protection legal frameworks to compliment public and private organizational management of personal data not only within their respective territories but also across the continent.

The transborder cooperation of national DPAs envisaged by the regional treaties ought to be encouraged and strengthened to boost enforcement of regional and municipal data protection laws with the aim of enhancing trans-border flow of data and international data governance within the confines of uniform cross border data protection rules.

Notes

1. LLM (Reading); Barrister and Solicitor of the Supreme Court of Nigeria; Managing Partner, Olumide Babalola LP; Member, International Association of Privacy Professionals (IAPP); Member, International Network of Privacy Law Professionals (INPLP); Author, Privacy and data protection law in Nigeria.

2. The Directive was enacted by the European Union in 1995, to harmonize all the data protection laws within the union and to regulate the processing of personal date stored in digital databases. See Rebecca Wong, 'The Data Protection Directive 95/46/EC: Idealisms and Realisms' (2012) International Review of Law Computers & Technology, 1.

3. The AU Convention on Cybersecurity and Personal Data Protection was adopted in Malabo on the 27th day of June 2014.

4. Cape Verde (2001), Mauritius (2004), Seychelles (2004), Tunisia (2004), Burkina Faso (2004), Senegal (2008), Morocco (2009), Benin (2009) Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Mali (2013) and Cote d'voire (2013).

5. The Reports that date back to 2014 was recently updated in March 2021 when participating States generally resolved to beef up their capacity building towards critical information infrastructure especially on "Information sharing and coordination at the national, regional and international levels." See UN General Assembly, 'Final Substantive Report' < https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> accessed 26 October 2021.

6. Cape Verde (2001), Mauritius (2004), Seychelles (2004), Tunisia (2004), Burkina Faso (2004), Senegal (2008), Morocco (2009), Benin (2009) Angola (2011), Gabon (2011) and Lesotho (2011).

7. Bautlin M. Ball, 'Introductory Note to African Union Convention on Cyber Security and Personal Data Protection' (2017) The American Society of International Law, 165.

8. Found at https://au.int/en/cyberlegislation.

9. Found at https://ccdcoe.org/uploads/2018/11/AU-130101-DraftCSConvention.pdf.

10. Lukman Adebisi Abdulrauf and Charles Manga Fombad, 'The African Union' Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa' (2016) 8(1) Journal of Media Law, 1, 8.

11. Found at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

12. The 23rd ordinary session of African Union ends in Malabo. See https://au.int/fr/newsevents/29258/23rd-ordinary-session-african-union-ends-malabo#:~:text=Malabo%2C%20Equatorial%20Guinea%2030%20June,from%2026%2D27%20June%202014.> accessed 26 May 2021.

13. Article 9(1), Malabo Convention.

14. The 55 Members of the AU include: Burundi, Cameroon, Central African Republic, Chad, Congo, DR Congo, Equatorial Guinea, Gabon, Sao Tome, and Principe, Comoros, Djibouti, Eritrea Ethiopia, Kenya, Madagascar, Mauritius, Rwanda, Seychelles, Somalia, South Sudan, Republic of Sudan, Tanzania, Uganda, Algeria, Egypt, Libya, Mauritania, Morocco, Sahrawi Arab Democratic, Tunisia, Angola, Botswana, Kingdom of Eswatini, Lesotho, Malawi, Mozambique, Namibia, South Africa, Zambia, Zimbabwe, Benin, Burkina Faso, Cape Verde, Cote d'voire, Gambia, Ghana, Guinea, Guinea- Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

15. See article 4(4); Klaus Wiedemann, K. 2018.

16. IAPP https://iapp.org/resources/article/automated-processing/ accessed 29 May 2021.

17. Andra Giugiu and Tine A. Larsen, 'Role and Power of National Data Protection Authorities' (2016) 3 EDPL, 342.

18. Art. 11(1)(a).

19. Art. 11(1)(b); Graham Greenleaf. 2012.

20. Angola, Benin, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Egypt, Gabon, Ghana, Kenya, Lesotho, Mali, Mauritius, Morocco, Niger, Nigeria, Sao Tome and Principe, Senegal, South Africa and Tunisia. See Paradigm Initiative and Olumide Babalola, 'Data Protection Authorities in Africa: A Report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

21. Article 12(2) (a)-(o).

22. Art. 10 (4).

23. Article 13 (1).

24. Article 22.

25. Article 13 (3) – (6).

26. Article 14.

27. Article 16 and 17.

28. Article 20 and 21.

29. Status List found at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 20 June 2021.

30. Art. 32(a) ECOWAS Reviewed Treaty 1993 found at < https://www.ecowas.int/wp-content/uploads/2015/01/Revised-treaty.pdf>; see also Abiodun Ashiru, 'A Comparative Analysis of the Legal Framework for the Criminalization of Cyberterrorism in Nigeria, England and the United States' (2021) 12(1) NAUJILJ, 99, 107.

31. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf> accessed 22 June 2021.

32. Art. 1.

33. In Europe, the national DPAs sometimes attempt to usurp the jurisdiction of courts to settle such transborder disputes by resorting to other dispute resolution mechanisms. See Olga Estadella-Yuste, 'Transborder Data Flows and the Sources of Public International Law' (1991) 16(2) North Carolina Journal of International Law and Commercial Regulation, 380, 412.

34. Art. 3 and 4.

35. Art.14 and 19.

36. Art. 20.

37. Art. 23 (1) and (2).

38. Art. 24.

39. Art. 24.

40. Art. 25.

41. Articles 25, 26, 27, 28 and 29.

42. This is a European concept which was recognised by the OECD Guidelines but became prominent under the repealed Data Protection Directive 95/46EC by regulating international transfer of personal data. See Julian Wagner, 'The Transfer of Personal Data to Third Countries under the GDPR: When Does a Recipient Country Provide an Adequate Level of Protection? (2018) 8(4) International Data Privacy Law, 319.

43. Art. 36.

44. Art. 38.

45. Art. 39.

46. Art. 40.

47. Art. 41.

48. Art. 42 – 45.

49. Found at < https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/SA4docs/data%20protection.pdf> accessed 19 June 2021.

50. Art. 3(2).

51. Art. 3(10).

52. Art. 11-17.

53. Art. 21-27.

54. Art. 31-38.

55. Art. 41(1)

56. Art. 42.

57. Art.44 (1)(a).

58. Art. 44 (1) (b). See also Wagner. 2018.

59. Parliament of the Republic of South Africa. < https://pmg.org.za/files/RNW2764-150825.docx> accessed 9 June 2021.

60. Found at http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq> accessed 11 June 2021.

61. Clause 2.5.

62. Ibid.

63. Ibid.

64. This is defined under the Malabo Convention as: "any 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."

65. Defined as "Big data refers to datasets that are not only big, but also high in variety and velocity, which makes them difficult to handle using traditional tools and techniques" See Elgendy and Elraga. 2014.

66. The principles of accuracy, storage limitation and accountability will be discussed in detail later in this paper.

67. Principles of lawfulness, fairness and transparency; data minimization; storage limitation; purpose limitation; accuracy; integrity and confidentiality and accountability. See art. 5(1) and (2). These principles are similar to the ones provided under the repealed EU Data Protection Directive 15/46 EC. See Bygrave. 2014.

68. List of Countries Which Have Signed, Ratified/Acceded To The African Union Convention On Cyber Security And Personal Data Protection <
< https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> accessed 22 June 2021.

69. Article 13 (3).

70. The principle has been part of the European data protection law since 1980 when it was introduced into the Organization for Economic Cooperation and Development's 'The Recommendations of the Council Concerning Guidelines Governing Protection of Privacy and Transborder flow of Personal Data' on 23 September 1980 <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 21 June 2021.

71. Some scholars however argued that, although this principle was provided under article …. Of the repealed UE Data Protection Directive 95/46EC, such inclusion was ill-conceived since data quality does not necessarily play a stand-alone role in data protection law as opposed to the data economy i.e – the data processing industry itself. See Thomas Hoeren, 'Big Data and Data Quality' in Big Data in Context Legal, Social and Technological Insights Thomas Hoeren and Barbara Kolany-Raiser (eds) (Springer, 2018,) 2.

72. 'Processing' is a technical word for alteration, use, transmission, collection, storage, destruction, transfer and any operation or sets of operation on personal data as defined by article 1 of the Malabo Convention.

73. Art. 13 (4) provides that data collected shall be accurate and where necessary, kept to date.

74. Angola (Agência de Protecção de Dados); Benin (Autorité de Protection des Données à caractère Personnel); Burkina Faso (Commission de l'Informatique et des Libertés); Cape Verde (Agência de Protecção de Dados); Chad (Agence Nationale de Sécurité Informatique et de Certification Électronique); Côte d'Ivoire (Autorité de Régulation des Télécommunications de Côte d'Ivoire); Egypt
(Personal Data Protection Centre); Gabon (Commission nationale pour la protection des données à caractère personnel); Ghana (Data Protection Commission); Kenya (Office of Data Protection Commissioner); Madagascar (Commission Malagasy de l'Informatique et des libertés); Mali
(Autorité de Protection des Données à Caractère Personnelles); Mauritius (Data Protection Office);
Morocco (Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel);
Niger (Haute Autorité de Protection des Données à caractère Personnel); Nigeria (National Information Technology Development Agency); Sao Tome and Principe (Agência Nacional de Protecção de Dados Pessoais); Senegal; (Commission des Données Personnelles); South Africa (Information Regulator); and Tunisia (Instance nationale de protection des données personnelles).

75. Article 14 provided that: "A data controller should be accountable for complying with measures which give effect to the principles stated above.'

76. Guagnin and Leon (2012), and also Zimnerman and Cabinakova (2015).

77. Article 18, African Charter of Human and Peoples Rights enjoins member states to protect the family - 'natural unit and basis of society'.

References

Abdulrauf, Lukman Adebisi and Fombad, Charles Manga. 2016. "The African Union Data Protection Convention 2014: A possible cause for celebration of human rights in Africa". *Journal of Media Law*, 1,8. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Abdulrauf, Lukman Adebisi. 2021. "Giving 'teeth' to the African Union towards advancing compliance with data privacy norm". *Information and Communication Technology Law*, 1, 30(2).

Abraham, Rene, Jan vom Brocke and Schneider, Johannes. 2019. "Data governance: A conceptual framework, structured review and research agenda". *International Journal of Information Management,* 1, 49.

Alhadeff, J., van Alsenoy, B. and Dumorhier, J. 2021. "The accountability principle in data protection regulation: Origin, development and future directions". In Daniel Guagnin, Carla Liten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). *Managing privacy through accountability*. Palgrave Macmillan.

Ashiru, Abiodun. 2021. "A comparative analysis of the legal framework for the criminalization of cyberterrorism in Nigeria, England and the United States". Nnamdi Azikiwe University Journal of International Law and Jurisprudence 12(1) 99, 107. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf. Accessed 22 June 2021.

Bair, J. 2004. Practical data quality: Sophistication levels? http://www.knightsbridge.com/pdfs/in_the_news/. Accessed 21 June 2021.

Ball, Bautlin M. 2017. "Introductory note to African Union Convention on Cyber Security and Personal Data Protection". *The American Society of International Law,* 165. https://au.int/en/cyberlegislation.

Becker, Regina. 2019. "A data information system for accountability under the General Data Protection Regulation". *Giga Science*, 8(12): 122.

Bennet, C.J. 2021. "The accountability approach to privacy and data Protection: Assumptions and caveats". In Daniel Guagnin, Carla Iiten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). *Managing privacy through accountability.* Palgrave Macmillan.

Biega, A. and Finick, M. 2021. "Reviving purpose limitation and data minimization in personalization, profiling and decision-making system". Max Planck Institute for Innovation and Competition Research Paper No. 21.04, 1, 5.

Brendan, Joseph A., van Alsenoy and Dumorhier, J. 2021. "The accountability principle in data protection regulation: Origin, development and future directions in managing privacy through accountability. In Daniel Guagnin, Carla Iiten, Daniel Neyland, Leon Hempel, Inga Kroener and Hector Postigo (eds). Palgrave Macmillan.

Bygrave, Lee A. 2002. *Data protection law: Approaching its rationale, logic and limits*. Kluwer International.

Bygrave, Lee A. 2014. *Data privacy law: An international perspective.* Oxford: Oxford University Press.

Cheong, Lai Kuan and Chang, Vanessa. 2007. The need for data governance: A case study. 18th Australasian Conference on Information system.

Cohn, Barbara L. 2015. "Data governance: A quality imperative in the era of big data, open data and beyond. *Journal of Law and Policy for the Information Society*, 10 (3): 812.

Cong, G., Fan, W., Geerts, F. and Ma, Shuai. 2017. "Improving data quality: Consistency and accuracy. Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23-27, 1.

De Hert, P., Papa, V.K., Wright, D. and Gutwirth, S. 2012. "The proposed regulation and the construction of a principles-driven system for individual data protection". *The European Journal of Social Science Research*, 26(1).

Donovan, Kevin P. and Martyin, Aaron K. 2013. "The rise of African SIM registration: The emerging dynamics of regulatory change". https://firstmonday.org/ojs/index.php/fm/article/view/4351/3820. Accessed 15 June 2021.

Duceto, R. 2020. "Data protection, scientific research and the role of information". *Computer and Security Review,* 37: 1, 5.

Elgendy, Nada and Elraga, Ahmed. 2014. "Big data analytics: A literature review paper. *Lecture Notes in Computer Science*, 8557, 214-227.

Estadella-Yuste, Olga. 1991. "Transborder data flows and the sources of public international law". *North Carolina Journal of International Law and Commercial Regulation*, 16(2): 380-412.

Falk, T.T. 2016. The concept of accountability as a privacy and data protection principle. https://www.cpomagazine.com/data-privacy/concept-accountability-privacy-data-protection-principle/. Aaccessed 17 June 2021.

Feldman, David. 1994. "Secrecy; dignity or autonomy? Views of privacy as a civil liberty". *Current Legal Problems*, 47(2): 42-54.

Forde, Aidan. 2016. "The conceptual relationship between privacy and data protection". *Cambridge Law Review*, 1: 135-137.

Francesco, G., Palazzani, L., Dimitiou, D., Domingo, J.D. Jiame Fons-Martinez, J., Jackson, S., Tozzi, P.V. and Caterina Rizzo, C. 2021. Digital tools in the informal consent process: A systematic view. https://www.researchsquare.com/article/rs-1273/v2. Accessed 13 June 2021.

Gao Cong, Gao, Wenfei Fan, Wenfei, Floris Geerts Floris and Ma S. 2017. "Improving data quality: Consistency and accuracy". Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23-27.

Giugiu, Andra and Tine A. Larsen. 2016. "Role and power of national data protection authorities". Eueopean Data Protection Law, 3: 342.

Greenleaf, Graham and Coltier, Bertil. 2020. "Comparing African data privacy laws: International, African and regional commitments". *University of New South Wales Law Research Series*, 1: 21.

Greenleaf, Graham and Cottier, Bertil. 2018. "Data privacy laws and bills: Growth in Africa, GDPR influence". *Privacy Laws and Business International Report*, 152: 11.

Greenleaf, Graham and Georges, Marie. 2014. "African regional privacy instruments: Their effect on harmonization". *Privacy Law and Business International Report,* 132: 19-21.

Greenleaf, Graham. 2012. "Independence of data privacy authorities international standards and Asia-Pacific experience". *Computer Law and Security Review*, 1, 28(1).

Guagnin, D. and Leon, H. 2012. *Managing privacy through accountability*. Palgrave Macmillan UK.

Hallinan, D. and Borbesius, F.Z. 2020. "Opinions can be incorrect (in our opinion) on data protection law's accuracy principle". *International Data Privacy Law*, 1, 10(1)

Hoeren, Thomas. 2018. "Big data and data quality". in Thomas Hoeren and Barbara Kolany-Raiser (eds), *Big data in context legal, social and technological insights*, Springer.

Joshi, Aurko. 2021. "Data quality and data governance: Where to begin". https://www.collibra.com/blog/data-quality-vs-data-governance. Accessed 11 June 2021.

Kavanagh, Camino. 2017. The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century. https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf. Accessed 25 May 2021.

Klaus Wiedemann, Klaus. 2018. "Automated processing of personal data for the evaluation of personally traits: Legal and ethical issues". Max Plank Institute for Innovation and Competition Research Paper No. 18-04, 3. IAPP https://iapp.org/resources/article/automated-processing/. Accessed 29 May 2021.

Kosta, Eleni. 2013. *Consent in European data protection law.* Nijhoff Publishers.

Lee A. 2002. *Bygrave, data protection law: Approaching its rationale, logic and limits*. Kluwer International.

Makulilo, Alex B. and Mophethe, Kuenu. 2016. "Privacy and data protection in Lesotho". *African Data Privacy Laws*, 337-347.

Makulilo, Alex Boniface. 2012. "Privacy and data protection in Africa: A state of the art". *International Data Privacy Law*, 2(3), 163.

Mayer-Schonberger, Victor. 1997. "Generational development of data protection in Europe". In Phillip Agre and Marc Rotenberg (eds), *Technology and privacy: The new landscape.* Cambridge: MIT Press.

Mercer, Shannon Togawa. 2020. "The limitations of European data protection as a model for global privacy regulation". American Journal of International Law Unbound, 114: 20-25.

Mourby, M., Mackey, E., Elliot, M., Gowans, H., Susan E. Wallace, Bell, J. Smith, H., Aidinlis, S. and Kaye, J. 2018. "Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK". *Computer Law and Security Review*, 34: 222-233.

Mwiburi, Abel Juma. 2019. *Preventing and combating cybercrime in East Africa. Lessons from Europe's cybercrime frameworks.* Berlin: Duncker and Humblot.

OECD. 2021. Guidelines on the protection of privacy and transborder flows of personal data. https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 9 June 2021.

Oman, Soren. 2010. "Implementing data protection in law". *Stockholm Institute for Scandinavian Law,* 1.

Orji, Uchenna Jerome. 2012. "The defects of the draft African Union convention on the establishment of a credible legal framework for cybersecurity". Institute of Electrical and Electronics Engineers, 1. https://ccdcoe.org/uploads/2018/11/AU-130101-DraftCSConvention.pdf.

Otto, B., Wende, K.; Schmidt, A. and Osl, P. 2007. "Towards a framework for corporate data quality management". 16th Australasia Conference on Information Systems University of Southern Queensland, Toowoomba Australia, 916-926.

Parliament of the Republic of South Africa. 2021. https://pmg.org.za/files/RNW2764-150825.docx> accessed 9 June 2021.

Pike, E.R. 2020. "Defending data: Towards ethical protections and comprehensive data governance". *Emory Law Journal*, 69: 687.

Pormeister, Kart. 2017. "Genetic data and the research exemption: Is the GDPR going too far?". *International Data Privacy Law*, 7(2): 137-140.

Schwartz, Paul M. 2019. "Global data privacy: The EU Way". 94 New York University Law Review, 94: 771.

Scott, Mark and Cerulus, Lauren. 2018. "Europe's new data protection rules export privacy standards worldwide". *Politico*, January 31.

Shumba, Tapiwe. 2015. "Revisiting legal harmonization under the Southern African Development Community treaty: The need to amend the treaty". *Law Democracy Development,* 19:1.

Terwase, I.T., Abdul-Talib, Asmat-Nizam and Zengeni, K.T. 2015. "The role of ECOWAS on economic governance, peace and security perspectives in West Africa". *Mediterranean Journal of Social Sciences,* 6(3): 257.

Tikk, Eneken and Schia, Niels Nagelhus. 2020. "The role of the UN Security Council in cybersecurity". In Eneken Tikk and Mika Kerttunen (eds), *Handbook of International Cybersecurity.* Routledge.

Traca, Joao Luis and Embry, Bernado. 2011. "An overview of the legal regime for data protection in Cape Verde". *International Data Privacy Law,* 1, 3.

United Nations. 2021. Recent developments in the field of information telecommunications in the context of international security. https://ccdcoe.org/incyder-articles/united-nations-recent-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security/. Accessed 25 May 2021.

UN General Assembly. 2021. Final substantive report. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. Accessed 26 October 2021.

Wagner, Julian. 2018. "The transfer of personal data to third countries under the GDPR: When does a recipient country provide an adequate level of protection? *International Data Privacy Law,* 8(4): 319.

Wiedemann, Klaus. 2018. “Automated processing of personal data for the evaluation of personally traits: Legal and ethical issues”. Max Plank Institute for Innovation and Competition Research Paper No. 18-04, 3.

Weber, K., Otto, B. and Osterle, H. 2009. “One size fits all - A contingency approach to data governance”. *Journal of Data and Information Quality*, 1(1): 1-27.

Wong, Rebecca. 2012. “The data protection directive 95/46/EC: Idealisms and realisms”. *International Review of Law Computers and Technology*, 1.

Zimnerman, C. and Cabinakova, J. 2015. “A conceptualizing of accountability as a privacy principle”. In BIS, W. Abramowicz (ed). Springer International publishing.

Zornes, Aaron. 2006. Corporate data governance best practice. The CDI Institute Market Plus TM Depth Report.

Mission

To strengthen local capacity for conducting independent, rigorous inquiry into the problems facing the management of economies in sub-Saharan Africa.

The mission rests on two basic premises: that development is more likely to occur where there is sustained sound management of the economy, and that such management is more likely to happen where there is an active, well-informed group of locally based professional economists to conduct policy-relevant research.

www.aercafrica.org

Learn More

www.facebook.com/aercafrica

www.instagram.com/aercafrica_official/

twitter.com/aercafrica

www.linkedin.com/school/aercafrica/

Contact Us
African Economic Research Consortium
Consortium pour la Recherche Economique en Afrique
Middle East Bank Towers,
3rd Floor, Jakaya Kikwete Road
Nairobi 00200, Kenya
Tel: +254 (0) 20 273 4150
communications@aercafrica.org