A synopsis on data protection under the Nigerian laws : has the universality of right to privacy trickled down to Nigeria?

Elgujja, AA

10.31219/osf.io/fk5xg

A Synopsis on Data Protection under the Nigerian Laws: Has the Universality of Right to Privacy Trickled Down to Nigeria?

Abba Amsami Elgujja*

Abstract

The concept of personal data protection is no doubt, an off-shoot of the universal human right to privacy and confidentiality. Not only has it been ingrained under Article 12 of the Universal Declaration of Human Rights, it has also been incorporated in to most of the regional human rights conventions, charters and treaties, except, of course the African Charter on Human Rights (ACHR) to which Nigerian affiliates with.

Despite its conspicuous absence in the ACHR, the revolution in the internet and information management technologies have prompted the African Union (AU), and the Economic Community of West Africa States (ECOWAS) to, respectively, create Convention and Act to regulate the processing of personal data.

However, Nigeria has neither incorporated these treaties, nor enacted a comprehensive data protection law. At best, Nigeria has a Data Protection Regulations, a Data Protection Bill, and scattered pieces of legislations regulating specific aspects of the processing of personal data.

The question is, has the universal human right to privacy effectively trickled down to Nigeria? This chapter captures the issues at stake, and attempts to proffer suggestion.

*Abba Amsami Elgujja, LLB (Hons) LLM (Salford) Ph.D. (Salford) King Saud University, Riyadh, KSA. Solicitor & Advocate of the Supreme Court of Nigeria. a.a.elgujja@edu.salford.ac.uk

Key words: Data Protection, Privacy, Nigerian Constitution, Confidentiality, Data Security, UDHR

INTRODUCTION

Since its declaration the Universal Declaration on Human Rights (UDHR) in 1948, the concept and scope human rights have continued to trickle down to the national domestic laws across the world. With the fast and drastic revolutions in the area of information management technology, the right to privacy and confidentiality has, and will remain part and parcel of the UDHR and other regional, sub-regional and national domestic laws. This chapter only makes an attempt to trace and outline the genealogy of privacy rights from the universal declaration in 1948, through the African regional charter and convention along the sub-regional ECOWAS treaties/supplemental acts and down the Nigerian domestic laws.

The right to privacy and confidentiality is one of the fundamental human rights, which is protected both under international human rights instruments and domestic constitutions and legislation. This human right gives rise to a duty upon state parties and individuals to protect data that are defined or categorised as private or confidential.[1] However, although privacy right, is ingrained in the Universal Declaration on Human Rights, affirmed or ratified by several member states, and incorporated in to domestic laws, the question here is, has the spirit and substance of the Declaration trickled down to Nigeria? The chapter traces the path, if any, followed by Nigeria to protect the rights of privacy and personal data of its citizens.

Although the terms privacy and confidentiality have often been used interchangeably to mean the same thing, a deeper look would reveal that they are distinctive without much difference.[2] The terms privacy and confidentiality are sometimes used interchangeably but most often, privacy is used when relating to spatial matters, while confidentiality relates to data or informational issues.[3] While it is not in the remit of this article to delve in to the nitty-gritty of the difference between the two terms, it could be argued that, while privacy of information is based on the individual and public interest to protect personal information away from public access, confidentiality is

---

[1] For example, under Article 8 of the ECHR, the States have a duty to protect the physical and moral integrity of an individual from other persons. See: SANDRA JANKOVIĆ v. CROATIA (2009) *(Application no. 38478/05)* STRASBOURG

[2] Donna Knapp van Bogaert and GA Ogunbanjo, 'Confidentiality and Privacy: What Is the Difference?' (2009) 51 South African Family Practice 194.

[3] Keneth W Goodman and Randolph A Miller, 'Ethics and Health Informatics : Users , Standards , and Outcomes' in Edward H Shortliffe and James J Cimino (eds), *Biomedical Informatics Computer Applications in Health Care and Biomedicine* (3rd edn, Springer, New York, NY 2006). p.379-402

about protecting the personal data accessed from being unlawfully disclosed to unintended third parties.

Be that as it may, data protection forms the core element of privacy rights under the various human rights legislations. However, it is important to define the specific types of data that are the subject of such protection under the human right to privacy and confidentiality. Various statutes, covenants and regulations have defined private, personal or confidential data/information in different ways giving varying depth and scope. One of such definition of choice is:

> "*Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*[4]

Simply put, a private data is any information that could ultimately identify the data subject, even though it is remote. Following from the above, this chapter attempts to review the nature and scope of data protection rights under the various human right laws, internationally and domestically, under international law as well as under Nigerian law. In the next sections, we discuss data protection under international instruments beginning with the Universal Declaration of Human Rights as well as regional instruments down to Nigerian domestic laws.

PRIVACY AND CONFIDENTIALITY UNDER THE UNIVERSAL DECLARATION OF HUMAN RIGHTS (UDHR), 1948

The Universal Declaration of Human Rights, 1948 is generally considered as the groundwork for the international human right laws, and it has inspired a rich body of legally binding international and national human rights legislation. The UDHR has served directly and indirectly as a model for many domestic constitutions, laws, regulations, and policies that protect fundamental human rights.[5] The UDHR's appearances in domestic laws could be found in their direct constitutional reference to,

---

[4] Article 4 (1) of the GDPR, 2016; See also NITDA and ECOWAS Act

[5] UN, 'Universal Declaration of Human Rights: The Foundation of International Human Rights Law' (*United Nations Website*, 1948) <http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html> accessed 6 January 2019.

or incorporation of its provisions; replication of its substantive articles in domestic legislations; and judicial interpretation of domestic laws in the light of the UDHR.[6] Nigeria ratified the UDHR in 1993,[7] and the Nigerian court has declared that:

> "(in) as much as and for as long as the Federal Government of Nigeria remains... [committed to] the Universal Declaration of Human Rights, for so long would Nigerian courts protect and vindicate fundamental human rights entrenched in the Declaration." [8]

The UDHR presumably forms the international benchmark on privacy rights, which explicitly provide for the protection of both territorial and communications privacy.[9] Article 12 of the Universal Declaration[10] undertakes to guarantee appropriate safeguards to the right to both privacy and confidentiality as thus:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[11]

Yet, the right of privacy and confidentiality in not unqualified under the UDHR. Article 12 (2) limits the exercise and enjoyment of the right to the extent that it respects and protect the rights and freedoms of others and, in the public interest, as are determined by law, solely "for the purpose of meeting the just requirements of morality, public order and the general welfare in a democratic society. However, such restriction must have in place, a "measure of legal protection against arbitrary interferences by public authorities.[12] In other words, the restriction must meet the three basic criteria; i.e., it must be pursuant/according to, or under a law (legality test); to achieve a legitimate aim (legitimate aim test), and as proportionate to the aim pursued (proportionality test).

---

[6] Hurst Hannum, 'The Status of The Universal Declaration of Human Rights in National and International Law' (1996) 25 GA. J. INT'L & COMP. L. 287.
[7] Vanguard News Nigeria, *62nd anniversary of UDHR: Political rights as endangered species* https://www.vanguardngr.com/2010/12/62nd-anniversary-of-udhr-political-rights-as-endangered-species/ Accessed 2/1/2019
[8] ***Nolokwu v. Comm'r of Police***, [High Ct.] (Nigeria) (Agbakoba J.), reported in LAW OF HABEAS CoRPus 96 (Chief Gani Fawehinmi ed., 1986).
[9] Tasioulas ibid
[10] https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf
[11] The right is enshrined in Articles 14 and 17 of the International Covenant on Civil and Political Rights (ICCPR); Articles 16 and 40 in the Convention on the Rights of the Child (CPR); Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families; Article 22 of the Convention on the Rights of Persons with Disabilities; and Article 4 of the African Charter on Human and Peoples' Rights.
[12] Malone case para 67

The UDHR has not only form the bedrock for human right to privacy and confidentiality, but also provided for foundation for regional human rights charters and convention. Would the African charter on human and peoples' right be an exception in this regard?

AFRICAN HUMAN RIGHT LAWS RELATED TO PRIVACY AND DATA PROTECTION

The right to privacy and confidentiality is guaranteed not only under the UDHR and other related international human rights laws, but also in most of the regional human rights conventions and charters, e.g., the European Convention on Human Rights and the American Convention on Human Rights and, most of the African nations have either ratified or affirmed the UDHR and other related UN human rights covenants.[13]

Accordingly, Africa, as a continent or region, has its own regional human rights instrument: the African Charter on Human and Peoples Rights (ACHR), just like the other regional human rights charters and conventions. And though, the ACHR is claimed to be tailored specifically to the African context, this assumption is evidently contentious due to the inadequate coverage of some civil and political rights, e.g., the lack of explicit recognition of the right to privacy. Is it because privacy right is not as universally accepted as acclaimed in the UDHR, or because privacy rights has no place under the African jurisprudence?

Although human rights are widely acclaimed to be a universal concept, some critics have demanded that its application should be informed by the spirit of anthropological and cross-cultural relativity of the different continents, e.g., Africa, Asia, and the Muslim world.[14] Pollis and Schwab in 1979,[15] had reiterated this, thus:

> *"The Western political philosophy, upon which the (United Nations) Charter and (Universal) Declaration (of Human Rights) are based, provides only one*

[13] Those include, but not limited to: International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR), International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), Convention on the Rights of the Child (CRC), International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (ICRMW)

[14] Michael Goodhart, 'Origins and Universality in the Human Rights Debates: Cultural Essentialism and the Challenge of Globalization' 935 (938). <https://www.jstor.org/stable/20069700> accessed 15 August 2018.

[15] Adamantia Pollis and Peter Schwab, *Human Rights: Cultural and Ideological Perspectives* (Adamantia Pollis and Peter Schwab eds, Praeger 1979).

particular interpretation of human rights, and that this Western notion may not be successfully applicable to non-Western areas due to ideological and cultural differences." [16]

In other words, some countries have questioned the universality of human rights because, in their view, the human rights, as are written in the UDHR, are only defined according to the views of the West without taking cognisance of the peculiarities and cultures of the other nations.[17] It is not surprising, therefore that, several countries had initially abstained from assenting to the Declaration on the ground that the drafters did not take into consideration, their own uniqueness.[18] This may explain why some of the regional charters, e.g., the Arab Charter and, the African Charter in particular have not closely reflected the substance of the UDHR. As we would find in the succeeding sections, a clear example of such disparity is on the issue of the right to privacy and confidentiality. The ACHR did not adopt the spirit and substance of the UDHR as regards privacy rights.

Despite the disparity between the UDHR and the ACHR on the right to privacy, the latter had subsequently made concerted effort to protect the privacy and confidentiality of sensitive personal data, especially, in the light of the evolving and advancing information management technologies.

African Charter on Human Rights (ACHR)[19]

As earlier on stated, the right to privacy has not featured in the African Charter on Human and People's Rights.[20] The ACHR, rather, obliges the state under Article 18(2)," to assist the family which is the custodian of morals and traditional values recognised by the community."[21] This conspicuous lack of explicit reference in the Charter to a

[16] ibid. p. 1
[17] Eight countries initially abstained from affirming the UDHR: six communist nations, led by the Soviet Union, plus South Africa and Saudi Arabia.
[18] For instance, Saudi Arabia criticised the authors of the UDHR because they 'for the most part, had taken into consideration only the standards recognised by Western civilisation' and towards the Commission, when he said, 'it was not for the Commission to proclaim the superiority of one civilisation over all others.' He had expressed his advocacy for cultural relativity rather than cultural colonialism.
[19] http://www.humanrights.se/wp-content/uploads/2012/01/African-Charter-on-Human-and-Peoples-Rights.pdf
[20] Privacy International at the 62nd Session of the African Commission on Human and People's Rights (ACHPR) https://privacyinternational.org/blog/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights-achpr Accessed 30/12/2018
[21] Obinna B Okere, 'The Protection of Human Rights in Africa and the African Charter on Human and Peoples' (1984) 6 Human Rights Quarterly 141 (154) <https://heinonline-org.salford.idm.oclc.org/HOL/Page?handle=hein.journals/hurq6&div=19&g_sent=1&casa_token=&collection=journals> accessed 3 January 2019.

right to privacy is seen as one of the shortcomings of African Charter in respect to civil and political rights.[22] It is not surprising, therefore, that the AU's Convention on Cyber Security and Data Protection is seen as timely succour.

Despite the evolution of the AU's cyber-security convention, there has still been persistent call for the incorporation of privacy rights in the ACHR. An example is the call by Privacy International at the 62nd session of the African Commission on Human Rights during which they emphasised that the right to privacy ought to have been taken seriously during the revision of the Declaration of the Principles of Freedom of Expression. Their call to incorporate the right to privacy and confidentiality in the mandate of the Special Rapporteur on Freedom of Expression and Access to Information is remarkable. Furthermore, there should be proper regulation of the processing of sensitive personal data such as biometrics in order to ensure adequate safeguards from abuse by both public and private organizations.[23]

With the deficiencies of the ACHR as alluded to above, is the evolution of the African Convention on Cyber-Security and Data Protection a sufficient supplement to cover the deficiency of the ACHR in respect of privacy rights?

African Union Convention on Cyber-Security & Data Protection (2014)

This convention seeks to embody the existing commitments of African Union Member States at sub-regional, regional and international levels to build the Information Society.[24] It pursues to harmonize African cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cybercrime control.

This African regional data protection legislation is heavily influenced by the Action Framework to Build Africa's Information and Communication Infrastructure as laid down by the Africa's Information Society Initiative, under the auspices of UN

---

[22] Nelson Enonchong, 'The African Charter on Human and Peoples' Rights: Effective Remedies in Domestic Law?' (2002) 46 Journal of African Law 197 <http://journals.cambridge.org/action/displayFulltext?type=1&fid=129090&jid=&volumeId=&issueId=&aid=129089>.

[23] Privacy International at the 62nd Session of the African Commission on Human and People's Rights (ACHPR); Saturday, April 28, 2018 https://privacyinternational.org/blog/2227/privacy-international-62nd-session-african-commission-human-and-peoples-rights-achpr Accessed 4/1/2019

[24] Preamble, African Union Convention on Cyber Security and Personal Data Protection 2000 (African Union Legal Instrument).

Economic Commission for Africa, [25] the Oliver Tambo Declaration,[26] Decision Assembly/AU/Decl.1(XIV),[27] the Addis Ababa Declaration[28] and the Abidjan Declaration.[29]

The Convention has made several landmark provisions related to electronic transaction,[30] personal data protection[31] and promoting cyber security and combating cybercrime.[32] The Convention finally made some supplemental provisions in Chapter IV. While the main features of the Convention include the electronic transactions and cyber security, however, this chapter would restrict itself to those related to the protection of personal data.

Personal Data Protection

In addition to the provisions on electronic transactions and cyber security, the Convention also made elaborate and extensive provisions for the protection of data, and commits member states "to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data." [33] This should be done by balancing the respect for the fundamental freedoms and rights of natural persons and the prerogatives of the State to protect public interests.

[25] UNECA, 'Africa's Information Society Initiative: An Action Framework to Build Africa's Information and Communication Infrastructure' (1995) <https://www.uneca.org/cfm1996/pages/africas-information-society-initiative-action-framework-build-africas-information-and> accessed 4 January 2019. This Framework was sequel to Resolution 795 (XXX) of 3 May 1995, entitled "Building Africa's Information Highway", of the ECA Conference of Ministers responsible for economic and social development and planning. The resolution requested the Executive Secretary to set up a high-level working group of African technical experts on information and communication technologies in Africa, to prepare a plan of action in this field for presentation to the twenty-second meeting of the Conference of Ministers.
[26] Adopted by the Conference of African Ministers in charge of Information and Communication Technologies held in Johannesburg, South Africa on 5 November 2009
[27] Of the Fourteenth Ordinary Session of the Assembly of Heads of State and Government of the African Union on Information and Communication Technologies in Africa: Challenges and Prospects for Development, held in Addis Ababa, Ethiopia from 31 January to 2 February 2010;
[28] On the Harmonization of Cyber Legislation in Africa, adopted on 22 June 2012
[29] On the Harmonization of Cyber Legislation in Africa, adopted on 22 February 2012.
[30] Chapter I, sections 2 – 7)
[31] Chapter II, sections 8 – 23)
[32] Chapter II, Section 24 – 31)
[33] Article 8

From the outset, the Convention defined a number of legal terms related to data protection, which among others, include data controller, data subject, health data, and personal data. Particularly, a personal data is defined under the 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"*[34]

Scope of application of the Convention:

The Convention applies to "any collection, processing (automated or non-automated processing of data), transmission, storage or use of personal data by a natural person, the State, local communities, and public or private corporate bodies."[35] However, data processing by a natural person that is exclusively for personal or household use or activities is not within the scope of the Convention if that data is for dissemination or systematic disclosure to third parties. So also, is a temporary copy made from an electronic system used solely for quality improvement of the services.[36] Also exempted is the processing data by a non-profit making association or body relating to its members and that is consistent with its objective.[37]

The Convention restricts processing of certain personal information unless approved by a lawful protecting authority. Such includes processing of health-related information, crime-related information, or information related to public security. Others include personal data related to or linking with national identifier; personal data involving biometric data; and personal data of public interest, particularly for historical, statistical or scientific purposes.[38] For those categories of data processing that would not potentially breach privacy, the data protection authority is empowered to establish and publish standards that simplify the process, and spells out exemptions from the obligation thereto.[39]

---

[34] Article 1, African Union Convention on Cyber Security and Data Protection (2014)
[35] Article 9(1)
[36] Article 9(2)
[37] Article 10
[38] Article 10 (4)
[39] Article 10(3)

The Convention also provides for the establishment, membership, composition and duties an independent administrative authority known as the national protection authority that is saddled with the duty of "ensuring that the processing of personal data is conducted in consistence with the provisions of this Convention." The data protection authority also ensures that information and communication technologies do not become counter-productive to the protection of fundamental freedoms and the privacy of citizens. [40]

The Convention lays down obligations relating to conditions for processing personal data. These principles include the requirement of consent, lawfulness and fairness, and those related to limitations on purpose, relevance and retention of processed personal information. Other principles covered include that of maintaining accuracy, transparency, privacy and confidentiality of processed data. Furthermore, the Convention made specific provision that prohibits any data collection and processing 'sensitive data' that reveal "racial, ethnic and regional origin, parental filiation, 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."[41]

Finally, the Convention prescribed the rights of data subjects and the obligations of state authorities. The data subjects' protected rights under the Convention are the right to information including information about purpose of processing the data, who are recipients, storage period, possible trans boarder transfer, and information about the right to request for erasure.[42] Right of access enables the data subject to ask for information as would enable him/her to evaluate and/or object to the processing, its purpose, the kind of personal data involved, and the recipients or their categories to whom the data are disclosed among others.[43] The third right of a data subject under the Convention is the right to object, on legitimate grounds, to the processing of the data relating to him/her, and to be informed before his/her personal data are disclosed for the first time to third parties or used on their behalf for the purposes of marketing.[44] The fourth and last right is that of erasure. The data subject has the right to demand the data controller to rectify, complete, update, block or erase, as the case may be, his/her

[40] Article 12
[41] Article 14
[42] Article 16
[43] Article 17
[44] Article 18

personal data where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure or storage are prohibited.[45]

Conversely, the Convention also provided for some obligations on the part of the personal data controllers. Those include maintaining confidentiality (only accessed by authorised persons), data security (to protect from unlawful access, alteration or destruction), storage (retained on for as long as is necessary for achieving the identified purpose(s)), and to ensure that processed personal information can be processed without technical hitch.[46]

However, in spite of these lofty provisions of the Convention, it is unfortunate that the Convention, as stated earlier on, is not yet domesticated in to the Nigerian law pursuant to Section 12 of the Constitution. As of the time of today, the Convention does not yet apply in Nigeria.

ECOWAS SUPPLEMENTARY DATA PROTECTION ACT (2010)

The Economic Community of West African States (ECOWAS) enacted as Supplementary Act to the ECOWAS Charter[47] but which, for all intent and purposes, is a treaty that has no effect in the member states unless enacted domestically by the national legislative bodies of the member states. This Act was triggered by the increasing use of information and communication technology (ICT) that may be prejudicial to the private and professional life of the users within the sub-region.[48]

Personal Data

One of the striking features of the Act is that it defined most of the operational terms of data protection. For instance, personal data is defined under the Act as:

> *Any information relating to an identified individual or who may be directly or indirectly identifiable by reference to an identification number or one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity*. [49]

[45] Article 19
[46] Articles 20 – 23
[47] ECOWAS Supplementary Act on Personal Data Protection No. A/SA.1/01/10 of 16th February 2010
[48] Preamble, ECOWAS Data Protection Act (2010)
[49] Article 1

Meanwhile, a health data is a form of sensitive data related to the physical and mental health, including genetic information. Other terms also defined under the Act are "data subject," "data controller," and "data processor" among many others. "Personal data processing" is defined under the Act as:

> *Any operation or set of operations carried out or not, with the assistance of processes that may or may not be automated, and applied to data, such as obtaining, using, recording, organisation, preservation, adaptation, alteration, retrieval, saving, copying, consultation, utilisation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, encryption, erasure or destruction of personal data*. [50]

The definition of some of the key terms such as 'personal data' and 'personal data processing' are apparently adapted from Articles 2 of the European Union Data Protection Directive (1995).[51]

Scope of the Act

Just like the AU's Convention, the ECOWAS' Act creates obligation on member states to establish a legal machineries for the protection of personal data during collection, processing (automated or un-automated) , transmission, storage, and use of personal data by any individual, by government, local authorities, and public or private legal entities with the exception of those processes mentioned under Article 4 of the Supplementary Act or as otherwise allowed or mandated by law.[52]It also applies to any processing of data related to public security, defence, investigation and prosecution of criminal offences or State security, subject to such exemptions as are defined by specific provisions stipulated in other legal texts in force. [53] Similar to the African Convention, this Act shall not apply to data processing carried out by an individual in the exclusive framework of his personal or domestic activities. [54]

Principle of Consent and Presumption of Legitimacy

Similar to Article 14 of the Convention, where a data subject gives a valid consent for the processing of his personal data, the Act considers the transaction as legitimate.[55]

---

[50] Article 1
[51] Uchenna Jerome Orji, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7 International Data Privacy Law 179.
[52] Article 2
[53] Article 2
[54] Article 4
[55] Article 23

However, consent may not be necessary where the processing is pursuant to a court order, or the data controller processed it is in compliance with a legal obligation or done in public interest. Additionally, consent of the data subject may be dispensed with, if the processing is necessary for complying with a binding contract, or at his request, or for safeguarding his own interest. [56]

Prohibitions and Exceptions

Within the ECOWAS space, the Act prohibits data processing intended to, or that which actually reveals the racial, ethnic or regional origin, ancestry, political inclinations, religious or philosophical beliefs, trade union membership, sexual life, genetic information or health information subject, as provided for by the AU's Convention.[57]

However, such prohibitions do not apply to the processing of public information, or where the data subject has given his written consent. Nevertheless, where the data subject is incapable of physically or legally giving a valid consent, the requirement of consent may be waived if it is necessary to protect his/her or others' vital interests. Such processing may also be permitted where necessary for establishing, exercising or defending a legal right, for or during legal proceedings or a criminal investigation, in compliance with a legal or regulatory obligation or, in public interest, for historical, statistical or scientific purposes.

Yet, unlike under the Convention, the Act permits the processing of personal information for the purpose of carrying out legitimate activities of a foundation, an association or any other non-profit making body that exists for political, philosophical, religious, mutual benefit or trade union purposes provided that, such processing shall relate only to the concerned member of such a body but where it involves a disclosure of personal data to third parties consent is required..

Trans-Border Data Portability to a Non-member ECOWAS Country

The personal data of a subject under the ECOWAS jurisdiction shall not be transferred a non-member ECOWAS country unless such a country provides an adequate level of protection for privacy (Same as the GDPR) in the processing or possible processing of such data. The Act require the data controller to inform the Data Protection Authority

[56] Article 23
[57] Article 30 and 31

before sending such data to a non-member country.[58] Although this concept seemed to be borrowed from the European Data Protection Directive 95/46/EC of 1995, what is missing in this Act is the definition of "an adequate level of protection", and how to assess the adequacy level of the protection accorded by the third-party country. It would have made more sense to adopt the protocol provided by the EU Directive under Article 25 (2) which provides:

> *The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are compiled within that country.*

It seems that the focus of adequacy is not as much directed towards the general provisions of the law in a third country, but to the actual level of protection which will be accorded in a particular case.[59]

Application to Nigeria

The ECOWAS Supplemental Act is not yet applied in Nigeria due to some major technical impediments that have stalled the implementation of the Act within the domestic jurisdiction of member states. One of the major obstacles to the smooth application of the Act is the lack of an established mechanism and/or institution to enhance the application of regional data protection instruments.[60] Apparently, this deficiency has led to a poor harmonization and enforcement of data protection standards within the ECOWAS region. The second impediment is the lack of judicial remedies and civil liability provisions for the breach of data protection principles. [61] This leaves the aggrieved data subject with no justiciable remedies for the breach of his/her personal data under the Act.

---

[58] Article 36
[59] Alex Boniface Makulilo, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3 International Data Privacy Law 42 (43).
[60] Orji (n 55) p. 181-182.
[61] Orji (n 55) p. 181-182.

It has been argued that an ECOWAS Supplementary Act, such as this, is meant to directly apply in all Member States on basis of the principle of direct applicability.[62] Article 9(3) of the Supplementary Protocol A/SP.1/06/06 that amended the Revised ECOWAS Treaty, provides that such Supplementary Acts, as adopted by the Authority shall be binding on the "Community institutions and Member States," thereby making it directly applicable. [63] However, section 12(1) of the 1999 Constitution of Nigeria makes ineffective, any treaty entered into by Nigeria unless it has been domesticated into law by the National Assembly. It provides:

> *No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly*

Therefore, for the same reason as the AU's Convention, the ECOWAS Data Protection Act is yet to acquire the force of law, pursuant to Section 12 of the Constitution, its provisions not having been domesticated by the National Assembly, although the proposed Data Protection Bill, 2020 has made attempts to adopt the principles contained therein.

NIGERIAN STATUTORY LAWS ON DATA PROTECTION

There is, so far, no effective comprehensive data protection law in Nigeria. Neither the AU's Convention nor the ECOWAS Act on data protection have been incorporated in to the Nigerian domestic laws. Nigeria is not yet in the league of the few African nations that have so far enacted data protection legislations, so far. Ghana and South Africa have already passed their data protection laws. Ghana's Data Protection Act (DPA) was passed in to law in 2012, to establish a Data Protection Commission, and to protect the privacy of individuals and the confidentiality of personal data by regulating the processing of personal information, and for other like matters.[64] On the other hand, the South Africa's Protection of Personal Information Act (POPI) 2013 is meant to be an

---

[62] ibid p. 183.
[63] Orji (n 55) p. 182.
[64] Data Protection, 'Ghana Data Protection Act, 2012' <https://www.dataprotection.org.gh/sites/default/files/Data Protection Act %2C 2012 %28Act 843%29.pdf> accessed 5 January 2019.

exhaustive and heavily detailed policy to bring South Africa's laws in line with EU and international regulations on data protection.[65]

Nevertheless, Nigeria still relies on the loose provision of the constitution that purport to guarantee rights to privacy, and the snippets of data protection provisions scattered in various legislations. It could be argued that, these collections of data protections provisions, neither individually nor collectively, satisfy the requirement of data protection principles in the contemporary digital world. At best, the Nigerian Data Protection Regulation is struggling to keep upbeat with the fast-changing information management climate. The following sections examines these laws.

The Nigerian Constitutional Provisions on Privacy and Confidentiality[66]

The Nigerian constitution provide for all fundamental human rights as contained in the UDHR. Right to privacy and confidentiality under the constitution, 1999, which includes the right to data protection,[67] serves as a restriction on the right to free speech under section 39. Section 37 of the constitution provides:

> *"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."*

The additional protection to privacy is under section 39, part of which restricts the freedom of expression to allow for the right of privacy. It provides:

Section 39:

> "(1) *every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference… (However)*
>
> *(3) Nothing in this section shall invalidate any law that is reasonably justifiable in a democratic society:*
>
> (a) ***For the purpose of preventing the disclosure of information received in confidence****…"* (Emphasis added).

---

[65] Centre for Internet and Society, South African Protection of Personal Information Act, 2013, https://cis-india.org/internet-governance/blog

[66] Nigerian Constitution, 1999 (as amended)

[67] See ***MTN Nigeria Communication Ltd v. Barr. Godfrey Nya Eneye***, Appeal No: CA/A/689/2013 (Unreported)

However, the cumulative effect of the two sections on privacy right is subject to the restriction under Section 45 which provides as follows:

> (1) *Nothing in sections 37, ...(and) 39, … of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom or other persons*

Two points have to be made regarding these provisions on the adequacy of the protection they afford to the right of privacy. On the one hand, this is hardly a sufficient stipulation of data protection, and on the other hand, the restrictions stated under section 45 is a pretty standard restriction on human rights. Whether or not the totality of the constitutional provisions is adequate to guarantee adequate protection would depend on whether these exceptions pass certain tests, which include legality, legitimate aim and proportionality tests. In other words, for these restrictions to be justified, it must be pursuant or according to a law, that it is intended to achieve a legitimate aim, and that the restriction is proportionate to the aim pursued.[68]

Data Protection under the National Health Act (NHA) 2014

The National Health Act 2014 provides for a framework for the regulation, development and management of a healthcare delivery system and sets the required standards for delivering health services in Nigeria. As part of that regulatory framework, the Act also provides for the confidentiality of health records, and prescribes who could or should have access to it.

Disclosure of Health Information

It is imperative to note that, the National Health Act (NHA) did not clearly define the terms ‘data’, ‘personal data’ or ‘health data’, record or health information. However, the Act provides that “all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential.”[69] Although “all information concerning a data subject, including information relating to

[68] Abba Amsami Elgujja, ‘Adequacy of the Legal Safeguards for the Patients ’ Right of Confidentiality under the Saudi Arabian Legal System’ (2017).
[69] S. 26 (1) National Health Act, 2014

his or her health status, treatment or stay in a health establishment are considered confidential,"[70] the Act allows a disclosure for, and in the course of, his/her treatment or care. Under the Act, a healthcare provider that has lawful access to the health records of a data subject is permitted to disclose such personal data to, and within, the health care team or facility within the ordinary course and scope of his or her duties as is necessary for any legitimate purpose where such disclosure is in the interest of the data subject,.[71]

Apart from disclosure for the data subject's care, the Act also allows the disclosure of such information, just as under the ECOWAS Act, where the data subject has consented to such disclosure (in writing), or where the court or the law requires it or, in the case of a minor or physically/legally incapacitated, at the request of a parent or guardian. A disclosure to third party may only be allowed where a non-disclosure of the information represents a serious threat to public health. [72]

A health care provider may access the patient's health records for the purpose of treatment with the user's consent, and for study, teaching or research with the authorisation of the user, head of the health establishment concerned *and* the relevant health research ethics committee.[73] In the case of study, teaching and research, authorization is not required if no information as to the identity of the user concerned is obtained.[74]

Offenses and Penalties

The management of the health facility in possession of a user's health records is responsible to ensure that control measures are in place to prevent unauthorised access to the records, storage facility, or system by which records are kept.[75] A person (or management) who fails to protect health records, or falsifies any record, or creates, changes or destroys a record without authority to do so, commits an offence under the Act. Also, intentionally providing false information to be included in a record, or unlawfully making copies of any part of a record or without authority, connecting the

[70] S. 26 (1) National Health Act, 2014
[71] Section 27 of the National Health Act, 2014
[72] S. 26 (2) National Health Act, 2014
[73] S. 28 (1) National Health Act, 2014
[74] S. 28 (2) National Health Act, 2014
[75] S. 29 (1) National Health Act, 2014

personal identification elements of a user's record with any element of that record that concerns the user's condition, treatment or history is an offence. [76]

Additionally, gaining unauthorised access to a record or record-keeping system, unauthorised connection of any part of a computer or other electronic system on which records are kept to any other computer or other electronic system; or terminal or other installation connected to or forming part of any other computer or other electronic system is an offence under the Act. Finally, it is an offence under the Act to, without authorisation, modify or impair the operation of any part of the operating system of a computer or other electronic system on which a user's records are kept, or part of the programme used to record, store, retrieve or display information on a computer or other electronic system on which a user's records are kept. All of the listed offenses above upon conviction, attract a punishment by imprisonment for a period not exceeding two years or to a fine ofN250, 000.00 or both. [77]

Complaint Procedures

The Act empowers the data subjects or patients to make their complaint about the manner in which they were treated at a healthcare institution and, have their grievance investigated.[78] For this purpose, the appropriate health authority shall create a policy and procedure for the instituting complaints within the health system being managed by the Federal or State Ministry of Health. The concerned Ministry shall conspicuously display such complaint procedure so as to be easily visible for any person entering the establishment and to take further steps to communicate same to users on a regular basis. [79]

The procedure should allow for the acceptance and acknowledgment of every complaint directed to a health establishment, whether or not within its jurisdiction or authority, and for referral to the appropriate body or authority, if outside its authority. In the case of a private health establishment, allow for the laying of complaints with the head of

[76] S. 29 (2) National Health Act, 2014
[77] S. 29 (2) National Health Act, 2014
[78] S. 30 (1) National Health Act, 2014
[79] S. 30 (2) National Health Act, 2014

the relevant establishment.[80] And the complainant is obliged to follow the procedure so established.[81]

It seems that the NHA has been more elaborate than any other law so far in place for regulating the processing of personal data of citizens. However, it is argued that its definition is too wide, which could potentially include anonymised and other information. A standard definition which stratifies the level of confidentiality, the forms of information (soft and hard copies), period covering the data (past, present and future) would have been better as per the standard laws and regulations on data protection. For instance, the GDPR defines such information as "personal data relating to the past, current or future[82] physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[83]

Data Protection under the Child Rights Act (CRA) No. 26 of 2003

The "Child Rights Act" (CRA) regulates the protection of children (persons under the age of 18 years), and, among other provisions, limits access to their personal information except as provided by law. With regard to privacy and data protection, Section 8 of the Act provides:

> *(1) Every child is entitled to his privacy, family life, home, correspondence, telephone conversation and telegraphic communications, except as provided in subsection (3) of this section.*
>
> *(2) No child shall be subjected to any interference with his right in subsection (1) of this section, except as provided in subsection (3) of this section.*
>
> *(3) Nothing in the provision of subsections (1) and (2) of this section shall affect the rights of parents and, where applicable, legal guardians, to exercise reasonable supervision and control over the conduct of their children and wards.*

The Act also prohibits the publication of any information that could lead to the identification of a child offender, and requires that the records of child offenders be

[80] S. 30 (3) National Health Act, 2014
[81] S. 30 (4) National Health Act, 2014
[82] Recital (35) GDPR 2016
[83] Article 4 (15) of the GDPR, 2016

kept strictly confidential and protected against access by third parties except in certain limited circumstances.[84] Section 205 provides as follows:

> *(1) The right of the child to privacy specified in section 8 of this Act shall be respected at all stages of child justice administration in order to avoid harm being caused to the child by undue publicity or by the process of labelling.*
>
> *(2) Accordingly, no information that may lead to the identification of a child offender shall be published.*
>
> *(3) Records of a child offender shall-*
>
> *(a) be kept strictly confidential and closed to third parties;*
>
> *(b) made accessible only to persons directly concerned with the disposition of the case at hand or other duly authorised persons; and*
>
> *(c) not be used in adult proceedings subsequent cases involving the same child offender.*

While the Act attempts to guarantee the privacy and confidentiality of the child's personal information, it also provides the parents/guardians with the power to exercise reasonable supervision and control over the child. What is unclear is the meaning of 'reasonable control' in relation to the child's right of privacy and confidentiality. Are the parents given unfettered right of access and control over the child's confidential health information? Are there exceptional situations where the parent/guardian may be denied this right of control?

Data Protection under the Freedom of Information (FOI) Act No. 4 of 2011

While the protection of privacy and confidentiality is about control over who can have access to, and disclosure of confidential information, the FOI Act is about the right to access to public records and information. Therefore, the "FOI Act" have potential impacts on the protection of the personal information of certain individuals, e.g., public officials, in Nigeria.

Access to information held by public officials is consistent with the import of the right to freedom of press as provided under Section 39 of the Nigerian Constitution. The Act

[84] Section 205(2), Child Rights Act No. 26 of 2003

is intended to make public records and information more freely available, to provide for public access to public records and information, and to protect public records and information to the extent consistent with the public interest and the protection of personal privacy. Its other goals include protecting public officers from the legal liability for disclosing classified official information without approval and to establish procedures thereto. [85]

The Act empowers citizens with the right to have access to any public records held by the government or public institutions.[86] It can be argued that Section 1 of the Act is restrictive to the right of privacy and confidentiality as it allows access to public information kept by public authorities. While, it also applies to information in the custody of private institutions that is intended to be used for the public, but it does not apply to restrict the right to confidentiality of personal information. Examples of such information include bank statements of public agencies, medical research reports being held by private organisations etc.

The Act empowers illiterate or disabled applicant to request for such information through their representatives.[87] Under Section 1(3) an aggrieved applicant who has been refused access to the requested information can apply to a superior court of record for an order of *mandamus* to compel the release of the requested information.

Apparently, the right to access is in line with the provisions of several anti-corruption conventions. For example, Article 9 of the African Union Convention on Preventing and Combating Corruption[88] requires all State parties to "*adopt such legislative and other measures to give effect to the right of access to any information that is required to assist in the fight against corruption and related offences."* Similarly, Article 19 of the ICCPR provides that everyone shall have the right to freedom of expression which includes freedom to seek, receive and impart information and ideas of all kinds. Furthermore, Article 13 of the United Nations Convention against Corruption[89] demands governments to encourage citizen involvement in anti-corruption crusades by, *inter alia*, providing the public with an effective access to pertinent information.

---

[85] Freedom of Information Act 2011 Laws of the Federation of Nigeria 2011 (Laws of the Federation of Nigeria).
[86] Article 1, Freedom of Information Act 2011 Laws of the Federation of Nigeria 2011
[87] Section 3(3), Freedom of Information Act 2011 Laws of the Federation of Nigeria 2011
[88] Adopted by the 2nd Ordinary Session of the Assembly of the Union in July 2003.
[89] Adopted by Resolution 58/4 of the General Assembly of the United Nations in October 2003.

However, the Act also provides for some exceptions to the right of access to information under certain conditions.[90] For instance, the FOI Act prohibits public institution from allowing an application for access to information that contains personal data unless the individual involved consents to the disclosure, or where such information is publicly available.[91] Similarly, section 16 of the FOI Act also provides that an application for disclosure of information may be denied if that information is subject to various forms of professional privilege conferred by law (such as lawyer-client privilege and journalism confidentiality privilege).[92] Personal information denotes "any official information held about an identifiable person but which does not include information that bears on the public duties of public employees and officials." [93]

Furthermore, an application for access to information may be denied if the disclosure of the information may be injurious to the conduct of international affair, or to the defence of the Federal Republic of Nigeria, and the security of penal institutions unless it is in the public interest to disclose it.[94] Additionally, where the data was collected for the purpose of enforcing law and order, or for internal management of a public institution, an access may be denied if that disclosure would interfere with law enforcement proceedings or pending administrative enforcement proceedings, or jeopardize an ongoing investigation. The access request may, also, be denied if granting so could deny a person of a fair trial or, inevitably reveal the identity of an anonymous source or, obstruct an ongoing criminal investigation or, constitute an invasion of personal privacy under this Act.[95] However, these exceptions may not apply if it would be in the public interest to grant access to such public information. The Act further provides:[96]

---

[90] Matthias Oluwole Dawodu, 'An Overview of the Freedom of Information AcT (An Appraisal from a Lawyer's Perspective)' <http://portal.unesco.org/ci/en/files/26159/12054862803freedom_information_en.pdf/freedom_informati> accessed 9 January 2019.
[91] Section 14 of the FOI Act
[92] See Section 16, FOI Act. See also: Udo Udoma and Belo Osagie, 'Data Privacy Protection in Nigeria Data Privacy Protection in Nigeria' <http://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf> accessed 26 December 2018.
[93] Section 31, Freedom of Information Act, 2011
[94] Section 11, Freedom of Information Act, 2011
[95] See under Section 15
[96] Section 12, Freedom of Information Act.

(2) Notwithstanding anything contained in this section, an application for information shall not be denied where the public interest in disclosing the information outweighs whatever injury that disclosure would cause.

(3) A public institution may deny an application for information that could reasonably be expected to facilitate the commission of an offence.

(4) For the purposes of section (1) (a), "enforcement proceeding" means an investigation that –

(a) pertains to the administration or enforcement of any Act, law or regulation;

(b) is authorized by or pursuant to any Act, law or regulation

The FOI Act prevents the public from having access to information relating to personal information and matters touching on personal privacy unless the data subject has given consent to such disclosure, or where such information is already available in the public domain.[97] Such category of data may include files and personal data of clients, patients, residents, students, or other individuals maintained by public institutions. Others include personal data maintained with respect to public employees, or officials, any applicant, of any regulatory agency, related to taxation, or information of whistle-blowers and complainants. In all such cases, access may be granted in the public interest if doing so would clearly outweigh the private right to privacy but subject to Section 14 (2) of the Act.[98]

Whistle-blowers are protected from legal liability under the Act, if the disclosure of the information that is made in good faith, reveals a mismanagement, gross waste of funds, fraud, abuse of authority, or a substantial and specific danger to public health or safety.[99] However, whistle blowers are not protected under this Act if they reveal information obtained by virtue of professional privileges such as lawyer-client privilege, doctor-patient privilege or other privileges conferred by law.[100]

This Act clearly empowers individuals to demand access to information in the domain of public institutions. However, it also restricts access to personal information unless

[97] Section 14.
[98] Section 14 (3)
[99] Section 27. *(1)*
[100] Section 16

the disclosure is in the public interest that outweighs the right to privacy of the data subject.

Data Protection under the National Identity Management Commission Act

The National Identity Management Commission (NIMC) Act provides for the establishment of a National Identity Database[101] and the National Identity Management Commission[102] that is responsible for the maintenance of the National Database, the registration of individuals, and the issuance of national identity cards; and for related matters.[103]

Schedule 2 of the Act lists the contents of database that the Commission keeps. Those include demographic information (names, date and place of birth, gender and address),[104] identification information (photograph, signature, finger prints and other biometric information),[105] and residence status (nationality, permits, visa information).[106] The national data base also contains several personal reference numbers which includes national identity number, reference number for immigration, insurance, Nigerian passport or other related document in lieu of passport, driving licence or such other related documents).[107] Others are any record history, registration and ID card history, validation information and records of provision of information.[108]

The Act prohibits persons or corporate bodies from access to database or information therefrom, with respect to a registered data subject except with application for, or consent to its release with the approval of the NIMC[109] However, the data user's consent may be dispensed with, in the public interest,[110] where the disclosure is necessary in the interest of national security, for the purpose of preventing or detecting crime or for other such purposes regulated by the Commission.[111] An unlawful

[101] Section 14, NIMC Act, 2007
[102] Section 1, NIMC Act, 2007
[103] National Identity Management Commission Act 2007 (Laws of the Federation of Nigeria).
[104] Paragraph 1, Second Schedule of NIMC Act, 2007
[105] Paragraph 2, Second Schedule of NIMC Act, 2007
[106] Paragraph 3, Second Schedule of NIMC Act, 2007
[107] Paragraph 4, Second Schedule of NIMC Act, 2007
[108] Paragraph 5-9, Second Schedule of NIMC Act, 2007
[109] Section 26 (1), NIMC Act, 2007
[110] Section 26 (4), NIMC Act, 2007
[111] Section 26 (2) and (3), NIMC Act, 2007

authorisation of or access to database is punishable under the Act with 10 years' imprisonment without option of fine.[112]

Data Protection under the Cybercrimes Act, 2015

This Act provides for a regulatory framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. This act also provides for the protection of critical national information infrastructure, promotes cyber security and protects electronic communications, data and computer programs, intellectual property and privacy rights.[113] Under the Act, an intentional and unlawful access to a computer system or network or part thereof, for the purpose of fraudulently obtaining vital security data, is an offence which, on conviction, is punishable with an imprisonment for a term of up to five years or to a fine of up to N5, 000,000.00 or both.[114] Also, any person who, with intent and without lawful authority, directly or indirectly modifies or causes modification of any data held in any computer system or network, commits an offence and shall be liable, on conviction, to imprisonment for a term of not more than 3 years or to a fine of not more than N7,000,000.00 or to both such fine and imprisonment.[115]

Subject to the constitutional right to privacy,[116] the Act mandates service providers to maintain and retain all traffic data and subscriber information for up to two years[117] and to take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved.[118] Furthermore, the service provider shall comply to, when requested by any law enforcement agency, preserve, hold or retain any traffic data, or release any information required to be kept under the Act. [119] Unfortunately, the Cybercrime Act does not specify the categories of alleged crimes for which a request for interception of communication can be made. This could open up opportunity for

[112] Section 28 (1) (a), NIMC Act, 2007
[113] S. 1, Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Laws of Federation of Nigeria).
[114] 6. (1) ibid.
[115] 16. (1)
[116] Section 38(5), Constitution of Federal Republic of Niger (1999) as amended.
[117] Section 38 (1) Cybercrimes (Prohibition, Prevention, Etc.) Act.
[118] *See also the Electronic Transactions Bill 2017 recently passed by the Nigerian Senate on 18th May, 2017.*
[119] Section 38 (2) and (3)

abuse allowing a request involving a 'minor offence'. It is unlikely that the Constitution anticipated a law that could derogate from its effect by 'minor offences'.[120]

However, any such data retained, processed or retrieved shall only be used for legitimate purposes as may be provided by law,[121] provided that due regard is paid to the individual's constitutional right to privacy and appropriate safeguards have been applied to ensure the confidentiality of the data.[122] The questions begging for answers are, does the Act only purports to offer protection of privacy to only traffic data and subscriber information retained by these Service Providers? What constitutes, the phrase 'subscriber information'? Does it also include messages exchanged and other general data collected, collated and processed by these Service Providers? Answers to these questions could help clear concerns about non-protection on non-traffic data.

In addition to some of the pitfalls already mentioned above, it is noteworthy that the Act does not define personal data, nor does it stipulate the rights of data subjects, or prescribe legal remedy for data breach. Furthermore, the mandatory sign-in register by cybercafés could create a potential security risk for the users without providing for appropriate safeguards against abuse. Mandating cybercafé users to sign-in before accessing the service may provide opportunity for unscrupulous cybercafé proprietors to pool the users' personal information that could be sold to commercial entities for profit, or potentially for more nefarious activities.[123]

Data Protection under the Credit Information Reporting Act (2017)[124]

This Act provides for the framework for credit reporting, licensing and regulation of credit bureaux. Among its primary objectives are, promoting access to accurate, fair and reliable credit information and to protect the privacy of such information.[125] For these purposes, the Act provides for the licensing and regulation of Credit Bureaux on one hand, and provide an appropriate framework for facilitating sharing of reliable

---

[120] 5 Controversial Aspects of the Nigerian Cybercrime Act 2015, https://lawpadi.com/5-controversial-aspects-of-the-nigerian-cybercrime-act-2015/ Accessed January 5th, 2019
[121] Section 38 (4) Cybercrimes (Prohibition, Prevention, Etc.) Act.
[122] Section 38 (5) ibid.
[123] 5 Controversial Aspects of the Nigerian Cybercrime Act 2015, https://lawpadi.com/5-controversial-aspects-of-the-nigerian-cybercrime-act-2015/ Accessed January 5th, 2019
[124] National Assembly, 'Credit Reporting Act, 2017'.
[125] Section 1, Credit Information Reporting Act, 2017

credit information amongst key stakeholders.[126] Under the Act, all credit bureaus must be licensed by the CBN to lawfully operate in Nigeria[127] and they have the obligation to create and maintain a database of credit, receive, collate and compile credit related information, and issue credit reports to Credit Users**.** [128]

In order to prevent the indiscriminate use of individual's personal information, the credit bureau is obliged to take reasonable steps to verify the accuracy of such credit information, and clear any doubt abouts its accuracy, completeness, or if it appears to be misleading, or contains any obvious error.[129] The credit bureau shall also not include information relating to race, ethnicity, colour, religion or political affiliation of the data subjects.[130] The credit bureaux shall retain data collected for 6 years from the date it was submitted to it, or provided to the credit user, and then further archive for 10 years before it may be destroyed eventually.[131]

The bureau shall, in addition to its other obligations under the Act, utilise the credit information collected solely for the purposes allowed under the Act, adopt measures and procedures to detect the misuse of data and ensure the confidentiality and security of such data, and adopt procedures to allow Credit Information Providers 'to correct data found to be inaccurate, invalid, incomplete or out of date.' [132]

Permissible use of Credit Information

Credit information may only be used for purposes allowed under the Act. Such purposes include for considering an application for credit or a qualification as a guarantor or, for managing existing credit facilities, employment checks on prospective employees, and for assessing the credit worthiness of a prospective tenant. Others includes for matters related to insurance policies and claims, for credit contracts or other post-paid services, or for debt collection or enforcement of a monetary judgment or debt.[133]

---

[126] Oladele Oladunjoye and Bisola Oguejiofor, 'A Critical Evaluation Of The Credit Reporting Act 2017 – Practical Issues Arising' (*Mondaq*, 2018) <http://www.mondaq.com/Nigeria/x/757320/Consumer+Credit/A+Critical+Evaluation+Of+The+Credit+Reporting+Act+2017+Practical+Issues+Arising> accessed 14 January 2019.
[127] Section 2, Credit Information Reporting Act, 2017
[128] Section 3, Credit Information Reporting Act, 2017
[129] Section 3 (3) (c)
[130] Section 3 (3) (d)
[131] Section 5
[132] Section 6 (1)
[133] Section 7 (2) (a) to (g)

The credit information may also be used to validate the correctness or otherwise of the credit information itself, for providing credit scoring services or, for complying with any court order, a law or, a regulatory authority or a public body to provide credit information. Finally, the credit information is considered permissible under the Act if it is used to carry out know-your-customer checks on any person for any permissible purpose or as may be required by law, or for such other purposes as the Central Bank may specify or direct.[134]

The Act also requires that a data exchange agreement must be executed between the credit bureau and the party requesting the information except where the data subject provides a written consent that such information be released. To keep the processes confidential, the Act specifically prohibits the use of credit information for purposes other than those prescribed in the Act.[135]

Rights of data subjects

In addition to prescribing the obligations of the Credit bureaus, the Act also provides protection to the interest of potential borrowers. To ensure confidentiality and to protect subject's information, credit bureaus are compelled to keep their data safe, secure and confidential.

The Act also allows the data subjects to challenge the accuracy of the credit information, and to request for the correction of credit reports which may be found to be false or inaccurate by providing additional information to rebut disputed information or to support additional claims. Also, Section 13 of the Act gives an aggrieved individual, who challenges the accuracy or validity of his/her credit information, the right to make a formal complaint to a credit bureau concerning a credit report and where such issue remains unresolved, he/she has the right to escalate such complaint to the CBN before finally filing a claim before a court of competent jurisdiction.[136]

[134] Section 7 (2) (h) to (m)
[135] See sections 7 and 12 (b), Credit Information Reporting Act 2017
[136] Assembly (n 125).

Data Protection under the Regulation of Telephone Subscribers (RTS) Regulation, 2011

The NCC issued regulations[137] to regulate the use of (personal) data by telecommunications operators and/or Internet Service Providers (ISP),[138] and to protect the security and confidentiality of the data held and managed by telecommunication companies and independent agents. Under the Regulations, all custodians of telecommunications data are required to retain data of subscribers and to take reasonable steps to ensure its security, and to protect it against unlawful disclosure. It also provides that customer information must "not be transferred to any party except as otherwise permitted or required by other applicable laws or regulations". However, the Regulations apply only to the operators in the communication industry in Nigeria.

Section 9 provides that subscribers information contained in the Central Database shall be held in strict confidentiality basis and no person or entity shall be allowed access to any subscriber's information that is on the Central Database that contains the biometric and other registration information of all Subscribers except as prescribed by the Regulation.

The Regulation does not specify such exceptions, and the conditions under which access to the central database is allowed. Section 21 of the Regulation provides penal sanctions for violators.

Data Protection under the CBN's Biometric Verification Number (BVN) Regulatory Framework

The Central Bank of Nigeria Act 2007 establishes the Central Bank of Nigeria (CBN) with the objectives of, among others, promoting a sound financial system in Nigeria.[139] The Act also empowers the CBN to make and modify regulations for the good order and management of the Bank,[140] for the efficient operation of all clearing and settlement

[137] Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission (NCC Regulation), and RTS Regulation (2011) to protect the security and confidentiality of the data held and managed by telecommunication companies and independent agents.
[138] Section 35 of the NCC Regulation captures the standard data protections of fairness, lawfulness, with restrictions on purposes, data retention, improper or accidental disclosure; as permitted by any permission or approval of the Commission etc.
[139] Section 2 (d),Central Bank of Nigeria Act 2007 (Federal Republic of Nigeria Official Gazette).
[140] Section 51, ibid.

systems,[141] and to ensure high standards of conduct and management throughout the banking system.[142]

Therefore, pursuant to Sections 2 and 42 of the Act, the CBN issued the Regulatory Framework for BVN Operations and Watch-List for the Nigerian Banking Industry.[143] This, the CBN says in the release, is to put in place an efficient and effective payments system for the settlement of transactions, including those involving electronic payment systems.

The Regulatory Framework requires the creation of a unique ID for each bank customer, and to link the unique ID to all related bank accounts, irrespective of which bank the account is domiciled[144] This ensures that the customer would not be able to enrol twice and that the customer's activities in other banks (especially suspicious ones) can be easily made available to all banks where the customer has account(s).

Consequently, certain entities may have lawful access to the BVN information, after providing a valid court order, subject to the approval of the CBN.[145] Those include deposit money banks, other financial institutions, mobile money operators, payment service providers, law enforcement agencies, credit bureaus and other entities as applicable.[146] However, to ensure the security and protection of the customers' personal information, the operators of BVN shall protect the security of the technologies used within the BVN network. Furthermore, the database shall be domiciled in Nigeria and can only be routed across borders with the consent of the CBN.[147] Furthermore, users of the BVN information shall establish adequate security procedures to ensure the safety and security of all related information, and also ensure that all information that its employees have obtained in the course of discharging their responsibilities are classified as confidential. [148] Participants are also obliged to establish a reliable system

---

[141] ibid. Section 47 (3)
[142] ibid. Section 42 (1)(b)
[143] Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017 as ammended by Circular No. BPS/DIR/GEN/CIR/05/007 of July 4, 2018
[144] Section 1.2 of the BVN Regulatory Framework.
[145] Section 1.6 Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry' as ammended.
[146] Section 1.6, CBN Regulatory Framework
[147] Section 1.8 (i) & (ii), Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.
[148] Section 1.8 (iii) & (iv), Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.

is to minimize risks and. to avoid susceptibility to sustained operational failures, as a result of system outages.[149]

Any bank or other stake holder that fails to abide by the requirement of this Regulation by not enlisting fraudulent customers would incur penalty from the CBN.[150] Furthermore, the bank shall not establish relationship with any customers on watchlist.[151] However, the Regulation does not stipulate penalties for wrongful disclosure of BVN data. The Framework only stipulated that, in the event of complaints by a bank customer, disputes shall be resolved by banks or escalated to the CBN, when unable to resolve.[152] The Framework also does not state the various data protection principles, nor the standard rights of data subjects.

Nigerian Case Laws on Privacy and Data Protection

It appears that there is a paucity case laws or judicial precedents specifically with respect to privacy and data protection laid down by the Nigerian court. The case of **Habib Nigeria Bank Limited v. Fathudeen Syed M. Koya[153]** involved an alleged disclosure by a bank of a customer's transactional information. The Court of Appeal held that, it is elementary knowledge that the bank owed its customer a duty of care and secrecy. In other words, other than the statutory protection afforded to information provided to lawyers, doctors and journalists, banks too owe a duty to maintain confidentiality to their clients even though such duty is not expressly prescribed by law.[154]

Similarly, in **CPC v. INEC and 41 others**[155] the appellant contested the INEC's refusal to release the registered voter's biometric database to the Appellant to enable it make

---

[149] Section 1.9, Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.
[150] Section 2.3, Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.
[151] Section 2.3.2., Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.
[152] Section 1.10, Central Bank of Nigeria Regulatory Framework For Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry, Reference No. BPS/DIR/GEN/CIR/04/010 of October 18, 2017.
[153] [1990 – 1993] 5 NBLR p. 368 at 387
[154] Udo Udoma & Belo-Osagie *Data Privacy Protection in Nigeria* http://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf
[155] [2011] LPELR -3999(CA)

copies for use as evidence to prove voting irregularities in the petition filed to contest the validity of the Presidential Election conducted by INEC. It was held that such access to the database would be inimical to the voters' right to privacy, and jeopardize national security. The Court based its decision on the potential national implication in taking copies of the database.

In the case of **Godfrey Nya Eneye v MTN Nigeria Communication Ltd,**[156] the plaintiff, a lawyer, alleged that without his consent, MTN disclosed his mobile phone number to unknown third parties who sent unsolicited text messages to him. This action, he alleged, violated his fundamental right to privacy guaranteed under section 37 of the Nigerian Constitution.

The court held that MTN's conduct amounts to a violation of the Applicant's fundamental human right to privacy of his person and correspondence under Section 37 and 39(3)(a) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended) and, section 1 and Article 14 of the African Charter on Human and People's Right (Ratification and Enforcement) Act, CAP A9, LFN 2004.

In a similar case of **Ezugwu Emmanuel Anene v. Airtel Nigeria Ltd,**[157] which was decided under the undefended claims procedure, in which the plaintiff who is a legl practitioner sued Airtel, a telecommunications service provider, at the FCT High Court in 2015, alleging that countless unsolicited calls and text messages by Airtel and third parties it granted access to his number breached his constitutional right to privacy, among other claims. As Airtel did not defend the suit, the trial court relied on the evidence produced by Mr Anene and delivered judgement in his favour, awarding Five Million Naira (5,000,000.00) damages to him for violation of his privacy right.

Although data protection right is not explicitly stated under section 37 of the constitution, the decisions of the few cases tried above have clearly incorporated data protection as part and parcel of the right to privacy and confidentiality as protected under the Constitution, 1999 (as amended).

[156] Appeal No: CA/A/689/2013 (Unreported)
[157] Suit No: FCT/HC/CV/545/2015 (Unreported).

Data Protection under the National Information Technology Development Agency (NITDA) Guidelines 2013

The NITDA Act establishes the Agency (NITDA) and authorises the "NITDA" to develop guidelines for electronic governance and to monitor the use of electronic data interchange.[158] Pursuant to this statutory mandate,[159] NITDA developed the 2013 Guidelines for Data Protection also popularly known as the "NITDA Guidelines"[160] which set standards for the processing of information relating to identifiable individual's personal data, including the obtaining, holding, use or disclosure of such information from inappropriate access, use, and disclosure.[161] The Guidelines is, so far, the only set of rules that prescribes the minimum data protection standards for handling of personal information.[162,163]

The NITDA Guidelines defines *"Personal data"* as:

> *"Any information relating to an identified or identifiable natural person (data subject); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, and posts on social networking websites, medical information, or a computer's IP address".*[164]

Those with responsibility for managing the data under the Guidelines include, but not limited to, the data controller, processor and custodian. *Data controllers*, determine why and how personal data should be processed, and are obliged to control any cross-border transfer of data to any country where there is not adequate level of data protection. The *data custodian* is responsible for ensuring the infrastructural security, while the *data processor*, being natural person, corporate body, public authority, undertakes in the processing of the personal data. On the other hand, a *third party* is a

---

[158] Section 6, NITDA Act 2007
[159] Pursuant to Sections 6, 17 and 18 of the NITDA Act, 2007. See Section 1.2 of the NITDA Guidelines, 2013.
[160] Version 3.1 of 2013 is the prevailing Guideline in force presently, but it is already reportedly under review by NITDA.
[161] Section 1.6, NITDA Guidelines, 2013
[162] Section 1.5, NITDA Guidelines, 2013
[163] Ngozi Aderibigbe, 'Data Protection 2018 / Nigeria' (*International Comparative Legal Guides*, 2018) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria#> accessed 7 January 2019.
[164] Section 1.6, NITDA Guidelines, 2013

person, natural or corporate, other than the data subject, controller, processor or persons authorised by the data controller or processor to process the personal data.[165]

The guideline applies to any form of handling of personal data, whether or not by wholly or partly automatic means.[166] It regulates the handlers of personal data within or outside Nigeria if they handle personal information of Nigerian citizens and residents.[167] However, the Guidelines does not cover the processing personal data related to public security, defence, national security and activities in the areas of criminal law.[168]

In May, 2020, the NDTA, pursuant to Section 6 of the NITDA Act 2007 and the NDPR 2019, issued a guideline for the implementation of NDPR within public institutions in Nigeria.[169] The Guideline is a version of the NDPR itself fashioned for use in public institutions. It also sets out the required standards for maintaining information securities,[170] for the appointment of data protection officers,[171] and for the establishment of an administrative mechanism for seeking redress following a determination of breach by NITDA.[172]

Scope of Application:

Although there are arguments suggesting that the NITDA Guideline's permissive language makes it sound advisory and therefore lack the force of the law. However, the Guideline, being a subsidiary legislation, draws its legal force from its principal legislation (the NITDA Act) thereby giving it the weight of law.[173] Thus, compliance with the NITDA Guidelines on Data Protection is a requirement of law, not a matter of choice.[174] It is not surprising, therefore, that Guidelines itself affirms that "a breach of

---

[165] Section 1.6, NITDA Guidelines, 2013
[166] Section 1.3 (1), NITDA Guidelines
[167] Section 1.3 (3), NITDA Guidelines
[168] Section 1.3 (2), NITDA Guidelines
[169] NITDA, Guidelines for the Management of Personal Data by Public Institutions in Nigeria, 2020. Available at https://nitda.gov.ng/wp-content/uploads/2020/08/GuidelinesForImplementationOfNDPRInPublicInstitutionsFinal1.pdf Accessed September 28th, 2020
[170] Paragraph 2.4 of the Guideline
[171] Paragraph 2.7 of the Guideline
[172] Paragraph 8.0 of the Guideline
[173] Aderibigbe (n 163).
[174] Ngozi Aderibigbe, 'Nigeria Has A Data Protection Regime - Data Protection - Nigeria' (*Mondaq*, 2018) <http://www.mondaq.com/Nigeria/x/721166/data+protection/Nigeria+Has+A+Data+Protection+Regime> accessed 26 December 2018.

the Guidelines shall be deemed to be a breach of the Act."[175] This is further strengthened by the NITDA Act:

> *Where a person or body corporate fails to comply with the guidelines and standards prescribed by the Agency in the discharge of its duties under this Act, such person or body corporate commits and offence.* [176]

And if such offense under this Act is committed by a body corporate, unless otherwise specified by the Act, that body is liable on conviction to a fine of N 200,000.00 or imprisonment for a term of 1 year or to both such fine and imprisonment, on first instance, to a fine of N 500,000.00 or to imprisonment for a term of 3 years or to both such fine and imprisonment, for any subsequent offense.[177]

Lawful Processing of Personal Data under the Guideline

The Guideline provided for circumstances under which personal data may be lawfully processed.[178] Those conditions include where the data subject has clearly, freely, and unambiguously given a valid consent, or if the processing of the data is pursuant to a contract to which the data subject is bound, or is in furtherance of compliance with a legal obligation to which the controller is subjected. Others are where the processing is necessary to protect the vital interest of the data subject or other stakeholder, or was done in the exercise of the controller's official authority. So also is the processing by a HCW for delivering healthcare but subject to the duty of professional confidentiality, or it involves the commission of crimes, or in connection with administrative sanctions or judgments in civil cases.

Data Protection Principles

The NITDA Guidelines laid down eight data protection principles to guide the data controllers and processors in complying with the Guidelines and, possibly, other related laws and regulations. These data protection principles are the same as those found under the European GDPR, 2016.[179]

---

[175] Section 1.2 of the NITDA Guidelines
[176] Section S. 17 (4), National Information Technology Development Agency Act 2007 (Laws of the Federation of Nigeria).
[177] Section 18, NITDA Act, 2007
[178] Section 2.2 2., and 3.1.1 (Principle 1), NITDA Guidelines, 2007
[179] See discussion on the impact of GDPR on data protection in Nigeria (infra).

Rights of Data Subjects

The Guidelines also provided for a number of rights for the data subject, just like those obtainable under the European GDPR, 2016. Those rights include:

1. *Right to Data Portability/Access to Data or Copies:* The data subject is entitled to obtain copy of own personal data, and be sent electronically, to another processing system. Entitled to receive within 7 days.[180]
2. *Right to Rectification of errors***,** if not in compliance with the Guidelines.[181] See Principle 4 on accuracy.[182]
3. *Right to Deletion or to be forgotten***:** Rectify, erase or block data *if it is not in compliance* with the Guidelines**.**[183] None under other legislations**.**
4. *Right to object to, or restrict processing, or withdraw consent***:** Option to object to processing, or to opt out, if data is used for marketing purpose.[184]
5. *Right to Compensation for Damages:* Any aggrieved data subject who has suffered damage as a result of unlawful operation or of any incompatible with the Guidelines, is entitled to receive compensation from the controller for the damage suffered.[185]

Pitfalls of the NITDA Guidelines:

1. The NITDA Guidelines makes no legal requirement to report data breaches to the relevant data protection authority.
2. There is no specific penalty provision in the NITDA Guidelines for breach of data security.
3. The NITDA Guidelines have no specific applicable administrative or civil sanctions.

---

[180] Section 2.3. NITDA Guidelines, 2007. So also, under the Credit Reporting Act S. 9(6) (a) – can request credit info that is personal data. Under Also under Registration of Telephone Subscribers Regulation, subscriber can view own data. And is entitled to request updates and amendments.
[181] Section 2.3.3 (c) (iii) NITDA Guidelines, 2007
[182] So also, under the Credit Reporting Act S. 9(6) (b) - contest within 15 days of receiving the credit report. Also, under Registration of Telephone Subscribers Regulation- entitled to request updates and amendments.
[183] Section 2.2.3 (d), NITDA Guidelines, 2013
[184] Section 2.2.7, NITDA Guidelines, 2013.The CBN Consumer Protection Framework require a consent given in writing before shared with 3rd party, or before being used for future promotional offers via emails, SMS etc
[185] Section 2.3.6, NITDA Guidelines, 2013

4. The NITDA Guidelines are silent on the individual's right to complain. The Guidelines does not stipulate procedure for, and authority responsible for securing any entitled compensation from the controller, nor the quantum of compensation, fine other penalties for violations. It appears an action for violation of the guideline will be brought pursuant to the NITDA Act.[186] However, under Section 13 of the Credit Reporting Act, the aggrieved data subject can submit complaint in writing to the credit information provider. There is no penal or administrative fine regime for violation.
5. The Guidelines does oblige Companies to register or notify NITDA regarding its data processing activities. Therefore, no specifications on what need to be notified to NITDA.[187]
6. The NITDA Guidelines have no express provision as to extent of the Data Security Officer's mandate. However, it does state that organisations shall designate an employee of that organisation as the organisation's Data Security Officer.
7. There is no provision for the immunity of the officer from disciplinary measures in the NITDA Guidelines.
8. There is no requirement for the registration of Data Security Officers in the applicable legislations.
9. The NITDA Guidelines do not impose an obligation on a business to register or notify NITDA regarding its data processing activities.
10. There no clear timeframe for notification of the supervisory authorities and, no requirement of, and provision for notification to the data subject or the public, in the event of breach, as can be seen under the GDPR. The Cybercrime's Act clear provide for a compulsory report of breach.[188]
11. It is not clear which court has the requisite jurisdiction to try such matters on breach of personal data by data controllers/processors.
12. The NITDA Guidelines do not provide for notification or prior approval for transfer of data outside Nigeria.
13. Anonymous reporting is not applicable under the Guidelines
14. No provision on which limits the purposes for which CCTV data may be used.

---

[186] Section 18, NITDA Act, 2007
[187] Motunrayo Akinyemi, 'A Comparative Analysis of the NITDA Draft Data Protection Guidelines 2017 With the GDPR By Motunrayo Akinyemi — Lawyard' (2018)
[188] Under section 21 of the Cyber-crimes Act.

15. Has no provision on whistle-blowing: It would appear that the provisions of Section 16 of the Freedom of Information Act apply to whistle blowers, their protection and other incidental matters thereto.

Data Protection Bill, 2010

Nigeria's Data Protection Bill 2019 is still yet to be passed in to law.[189] The purpose of this Bill is to establish rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organisations to manage personal information only for intended reasonably appropriate purposes.

Scope of Application of the Bill

It applies to every organisation, whether in the private and public sectors, that is involved in the collection, processing or disclosure of personal information, whether by automated or unautomated means, related to citizens, residents, or persons who are not established in Nigeria but who use equipment or processors in Nigeria to process personal data of data subjects who are located in Nigeria.[190]

The scope of Bill seems to be wider than what is obtainable under the NDITA Regulations.[191] The NITDA Regulation does not apply to non-Nigerians residing outside of Nigeria even if they process data of persons domiciled in Nigeria.[192] Furthermore the Regulation does not require the registration, with the Commission, of companies that are not incorporated in Nigeria as it is under the Bill.

The Bill requires data controllers, not being an incorporated company in Nigeria, to register with the Commission if they process data covered by the Bill. It has been argued that the registration requirement may 'prove onerous for foreign companies particularly as it pertains to making Nigeria an attractive destination for foreign investment. [193]

---

[189] http://placbillstrack.org/view.php?getid=6958 First Reading: 10/12/2019 and http://placbillstrack.org/view.php?getid=7011 First Reading: 26/11/2019. The Integrated Data Management Commission (Est. etc.) Bill, 2019. http://placbillstrack.org/view.php?getid=6708 First Reading: 14/11/2019 The NITDA recently published an update Data Protection Bill, 2020 for public comments. Available here: https://nitda.gov.ng/wp-content/uploads/2020/08/Draft-Data-Protection-Bill-2020.pdf

[190] Generally, see Section 2 of the Bill

[191] Emmanuel Salami, 'Nigerian Data Protection Law' (2019) 9 Datenschutz und Datensicherheit 576 <https://nitda.gov.ng/>.

[192] See Part two, para 1.2. of the NITDA Regulation, 2019

[193] Salami (n 200).

Rather, the Bill should have adopted a more favourable approach of the GDPR that requires such companies to have representatives in Nigeria.[194]

Trans-Border Data Transfers

The Bill allows for transborder transfer of personal data if the recipient country secures an adequate level of protection acceptable under the provisions of the bill.[195] The determination of adequacy of the level of protection is based on adequacy, accountability, authorization and reciprocity in the recipient country or organization, or the existence of data protections laws, or the implementation of a legally binding and enforceable instruments that provide a standardized safeguards.[196] These criteria for determining adequate level of protection are almost the same with the relevant provisions under the GDPR.[197]

However, these requirements may be dispensed with if, the data subject gives an explicit, informed free consent, or it is in his best interest, or in the public interest allowed by law.[198]

Exceptions to Disclosures of Personal Information to Third Parties

The Act allows for collection of personal information even if without knowledge or consent, if it is in the best interests of the data subject where obtaining a valid consent is impossible or if delay could compromise availability or accuracy. Also, collection of personal information is not unlawful if is already a public info, or is required by or mandated by law., or for journalist, artistic or literary use.[199]

A personal information may be disclosed if the information could be useful in the investigation of a crime, or in an emergency that threatens the life, health or security of an individual, or used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality.[200]

---

[194] See Article 27 of the GDPR, 2016
[195] Section 43 (1) of the Bill & Reg. 2.11 NDPR.
[196] See Section 43 (2) of the Bill.
[197] Articles 44-50, Recitals 101, 112 of the GDPR, 2016
[198] See Section 43 (3) of the Bill.
[199] Section 5 (1)
[200] Section 5 (2)

Other exceptions are; disclosure to a legal practitioner, or for the purpose of debt collection or in compliance with a court order, or such disclosures to public authorities in the interest of national security, the defence of Nigeria or the conduct of international affairs, or for the purpose of administering any law of Nigeria. Finally, the Act allows for disclosures made for statistical, or scholarly study or research, or purposes that cannot be achieved without disclosing the information, or the conservation of records of historic or archival importance.

The Bill also replicated the definition[201] of sensitive data as defined under the African Convention on Cybersecurity and Data Protection (2014)[202], and under the West African Supplementary Data Protection Act (2010).[203] However, it exempts restrictions on the disclosure of sensitive data where such information is processed by religious organization in respect of its members that is consistent with, and is necessary to achieve its aims and objectives.[204] This exemption would seem to be a departure from the six legal exemptions laid down under the GDPR.[205] The counter argument is that, the member of a religious organisation is considered to have impliedly consented to the processing, having voluntarily chosen to belong to the religious organisation.[206]

Data Protection Principles:

All of the data protection principles alluded to above under the NDITA regulations have been reflected in the proposed Bill. We will discuss them in more details while considering the European Data Protection Regulations, 2016, below.

Data Breaches

Although the Bill does not define the phrase 'data breach', it still requires all data breaches to be reported to the Commission.[207] The Bill requires that data subjects are to be informed of data breaches which pose a high risk to their rights and freedoms.

---

[201] See Article 70 (Interpretations) of the Bill, for the definition of sensitive data.
[202] See Article 14 of the Convention (2014)
[203] See Article 30 of the Act (2010)
[204] Section 24 of the Bill.
[205] See Article 6 of the GDPR, 2016
[206] Salami (n 200). p. 578
[207] Section 32 of the Bill

THE IMPACT OF EUROPEAN UNION (EU) DATA PROTECTION LAWS ON NIGERIA

European Convention on Human Rights (ECHR)

The European Convention on Human Rights does not, directly or indirectly, apply to Africa or Nigeria. However, given that the EU has just recently updated their data protection laws which has implications for extra-territorial jurisdictions, including Nigerians, it would not be out of place to review it. Consequent to the effectuation of the General Data Protection Regulations, many countries have felt the need to update their own data protection laws as well. This can serve as a guide for other regions and countries including Nigeria. [208]

As stated above, the EU has developed a holistic data protection regime. The European regional institutions, ECHR and the European Court of Human Rights (ECtHR), constitute the global most extensive and effective system of international institutions designed for protecting human rights.[209] It is widely considered as "an unprecedentedly effective system for the collective enforcement of human rights in Europe, and indeed a model for the world."[210] It has the only compulsory international human rights judicial mechanism where individuals may file applications directly to the Court since the entry into force of Protocol 11 (1998).[211]

Article 8 of the ECHR provides for a qualified right to respect for private and family life in essentially the same way as the UDHR. And, the justification for the restriction to this right under article 8 (2) of the ECHR are, for all intent and purposes, essentially the same as those listed under Article 12(2) of the UDHR:

> *1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

---

[208] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[209] ANDREW MORAVCSIK, 'Explaining International Human Rights Regimes: Liberal Theory and Western Europe' (1995) 1 European Journal of International Relations 157 <https://www.princeton.edu/~amoravcs/library/explain.pdf> accessed 16 July 2018.
[210] F.G. Jacobs, the Sovereignty of Law: The European Way (2007), at 34.
[211] Veronika BÍLKOVÁ, Anne PETERS and Pieter van DIJK, 'On The Implementation of International Human Rights Treaties in Domestic Law and The Role of Courts Adopted by The Venice Commission at Its 100th Plenary Session (CDL-AD(2014)036)' (2014) <www.venice.coe.int> accessed 23 September 2018.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

There is no doubt that the ECHR has reinforced the privacy rights as encapsulated under the UDHR, and it is a force to reckon with when issues on right to privacy is being considered.

General Data Protection Regulations (GDPR), 2016

The GDPR,[212] became effectively applicable to the European Union on May 26th, 2018, whereas the NDPR became effective on 25 January 2019. It would seem that the GDPR has strongly influenced the NDPR as both regulations provide for a more comprehensive data protection within their respective jurisdictions. Their similarities extend to the fact that, both the GDPR and the NDPR provide for data controllers and data processors ('data administrators' under the NDPR), for definitions of data breaches, for accountability requirements, and for the right to erasure. They are also consistent with each other as both provide similar definitions for 'processing,' 'personal data' and 'sensitive personal data.'

While the scope of both regulations are materially similar,[213] the critical application of the GDPR to Nigeria is that it applies whether the data controller or, the processor is based within or outside any EU member state, if they collect or process personal data of EU citizens and residents,[214] or offers goods or services to people in the EU, or monitor their online behaviour (e.g., tracking web visits through cookies)[215] whereas the NDPR applies to Nigerian citizens (based in Nigeria or outside) and residents only. Another distinction between the two regulations is that the NDPR does not explicitly

[212] General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), went into effect on 25 May 2018

[213] The material scope of the two laws is also very consistent and both provide similar definitions for 'processing,' 'personal data' and 'sensitive personal data'. However, the GDPR applies to the processing activities of data controllers and data processors that do not have any presence in the EU, but where their processing activities are related to the offering of goods or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU.

[214] See Article 3.1, GDPR 2016

[215] See Article 3.2, GDPR 2016

require any of the record-keeping obligations required by the GDPR, and does not outline how NITDA will calculate fines.

The National Information Technology Development Agency (NITDA) has recently raised concern of the implication of the GDPR to Nigerian businesses. This regulation might, according to NITDA, have a huge impact on Nigerian businesses and/or individuals that use information technologies to collect, store, process and transact on EU citizens personal data in EU territory or elsewhere. [216] Some corresponding effort has become imperative to protect Nigerian businesses from unnecessary exposure to the risks of this regulation and/or any regulations that might have negative impact on their businesses as well as the rights of Nigerians that have dual citizenship of any EU member state.

The GDPR requires that data controllers and processors must seek consent from data subjects in an intelligible and easily accessible form, clearly specifying the purpose for the collection. It also stipulates that consent must be clear and distinguishable from other matters and presented in a clear and plain language. The GDPR, which replaces the Data Protection Directive, lays down a number of data protection principles that are intended to enhance the protection of personal data in the contemporary digital society. Fortunately, these data protection principles have already been incorporated in the proposed Nigerian Data Protection Bill (2010) which is still yet to be enacted into law. These data protection principles are largely culled from the previous Data Protection Directives: [217]

1. Personal data must be processed fairly and lawfully. Inform data subject of the purpose of processing.[218] (See also Article 6(1a) Data Protection Directive 95/46/EC). [219,]

[216] Zakariyya Adaramola, 'EU's Data Regulation: What Nigerians Should Know' *Daily Trust* (25 February 2016) <https://www.dailytrust.com.ng/eus-data-regulation-what-nigerians-should-know.html>.
[217] Abubakar Sanni Aliyu, 'The Nigeria Data Protection Bill: Appraisal, Issues, And Challenges' (2016) 9 Innovative Issues and Approaches in Social Sciences 48.
[218] Section 2.2. 1., NITDA Guidelines, 2007
[219] See Draft Data Protection Bill (2010) Schedule 1 Section 4(4)

2. Personal data shall be obtained only for one or more **specified and lawful purposes**, and shall not be further processed in any manner incompatible with that purpose or those purposes (See Article 6(1b)). [220, 221]
3. Personal data shall be **adequate, relevant and not excessive** in relation to the purpose or purposes for which they are processed (See Article 6(1c)).[222, 223]
4. Personal data shall be **accurate** and, where necessary, kept **up to date** (See Article 6(1d)).[224, 225]
5. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes (See Article 6(1e)).[226] But no time limit, the Guideline only requires controllers to develop data retention policy.[227, 228]
6. Personal data shall be processed in accordance with the **rights of data subjects** under this Act (See Article 12).[229] Entitled to request to view their data as held by the controller who is obliged to respond to such requests without delay.[230]
7. **Appropriate technical and organisational measures** shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (See Article 17). [231]
8. While the principle that data should not to be transferred out of Nigeria unless adequate protections are in place to protect the data in the receiving country is replicated in the GDPR,[232] the principle of proportionality as provided under the GDPR, 2016 is not captured in the Guidelines.

---

[220] See Draft Data Protection Bill (2010) Schedule 1 Section 4(4)
[221] Section 4.1.2., and 3.1.2 (Principle 2) NITDA Guidelines, 2007. Also, the NCC Consumer Code of Practice Regulations provided similarly. Subscribers' data should not be used in any manner other than the company's operations.
[222] See Draft Data Protection Bill (2010) Schedule 1 Section 4(5)
[223] Section 4.1.2., and 3.1.2 (Principle 2) NITDA Guidelines, 2007. Also, the NCC Consumer Code of Practice Regulations provided similarly. Subscribers' data should not be used in any manner other than the company's operations.
[224] See Draft Data Protection Bill (2010) Schedule 1 Section 4(6)
[225] Section 3.1.4 (Principle 4) NITDA Guidelines, 2007
[226] See Draft Data Protection Bill (2010) Schedule 1 Section 4(5)
[227] Section 3.1.5 (Principle 5) NITDA Guidelines, 2007
[228] Under the Credit Reporting Act: Maintain credit info for 6 years, then archive for 10 years. Then, may be destroyed; S. 38 of Cybercrimes Act: Keep traffic data and subscriber info for 2 years
[229] See Draft Data Protection Bill (2010) Schedule 1 Section 4(8) & 4 (10)
[230] Section 3.1.6 (Principle 6) NITDA Guidelines, 2007
[231] Section 2.2.4., and 3.1.7 (Principle 7) NITDA Guidelines, 2007
[232] Section 2.3.4., and 3.1.8 (Principle 8) NITDA Guidelines, 2007

It could be argued that the GDPR is the foundation for the standards of protection of modern personal data the world over. Not only does it have jurisdiction over data processing within the European Union, but also on such data processing done outside that involve European citizens irrespective of the geographic location. It would seem to serve as an international benchmark on data protection for other national laws for the next few foreseeable future. The proactive steps of the drafters of the Nigerian Data Protection Bill by including these data protection principles in the Bill, is remarkable.

CONCLUSION

This chapter has been able to trace the historical and jurisdictional source of the right to privacy right from the universal declaration through the regional and sub-regional human right instruments to the Nigerian domestic laws. We realised that, although all fundamental human rights under the UDHR are considered as universally applicable, and affirmed to all regional human rights laws, the African Charter on Human Rights did not feature the privacy rights for application in Africa.

Although it is still unclear why the privacy right did not feature under the ACHR, the establishment of the African Convention of Cyber-securities and Data Protection (2014) may have been a subtle attempt to right the wrong. The further follow up by the ECOWAS sub-regional Supplemental Data Protection Act (2010) may have strengthened the lose link to the UDHR.

Nigeria have acceded to, and domesticated the privacy rights under UDHR as enshrined in the constitution (1999 as amended), but the elaborate provisions relating to data protection as laid down African and ECOWAS conventions and supplemental acts have not yet been enacted in to the Nigerian laws. Several attempts have been made by way of Data Protection Bills, but until now, it has not yet gone past the first reading at the National Assembly. This lacuna in our law creates a huge opportunity for criminal gangs and even legitimate organizations/companies to target data of Nigerians with the sole purpose of fishing out data that could be used in a criminal or discriminatory manner.

It is remarkable the NITDA, pursuant to the NITDA Act, has issued Data Protection Regulations that can be likened to the European GDPR in its scope and applications. While the debate on its legal weight rages on, it is our considered view that the National Assembly should do the needful to pass the proposed Data Protection Bill (2020) to significantly address some of the common data protection violations including unlawful and unjustifiable personal data processing, the failure to provide the necessary information to data subjects, unregulated data transfers etc. [233]

The call by the National Assembly for public comment is an opportunity to have a wholistic look at the Bill with a view to harmonising and streamlining it with the contemporary challenges to international data protection laws. [234] This is because, there is an urgent need for legislative and judicial intervention in respect of data protection law in Nigeria, if the country is to truly develop economically and otherwise.[235]

5. Bibliography

Adaramola Z, 'EU's Data Regulation: What Nigerians Should Know' *Daily Trust* (25 February 2016) <https://www.dailytrust.com.ng/eus-data-regulation-what-nigerians-should-know.html>

Aderibigbe N, 'Data Protection 2018 / Nigeria' (*International Comparative Legal Guides*, 2018) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria#> accessed 7 January 2019

——, 'Nigeria Has A Data Protection Regime - Data Protection - Nigeria' (*Mondaq*, 2018) <http://www.mondaq.com/Nigeria/x/721166/data+protection/Nigeria+Has+A+Data+Protection+Regime> accessed 26 December 2018

Akinyemi M, 'A Comparative Analysis of the NITDA Draft Data Protection Guidelines 2017 With the GDPR' (*Lawyard*, 2018) <https://www.lawyard.ng/a-comparative-analysis-of-the-nitda-draft-data-protection-guidelines-2017-with-the-gdpr-by-

[233] Salami (n 200). p. 282
[234] Aliyu (n 228). p. 581
[235] Salami (n 200).

motunrayo-akinyemi/> accessed 5 January 2019

Aliyu AS, 'The Nigeria Data Protection Bill: Appraisal, Issues, And Challenges' (2016) 9 Innovative Issues and Approaches in Social Sciences 48

Assembly N, 'CREDlf REPORTING ACT, 2017' (2017) <https://nass.gov.ng/document/download/9420> accessed 5 January 2019

BÍLKOVÁ V, PETERS A and van DIJK P, 'On The Implementation of International Human Rights Treaties in Domestic Law and The Role of Courts Adopted by The Venice Commission at Its 100th Plenary Session (CDL-AD(2014)036)' (2014) <www.venice.coe.int> accessed 23 September 2018

Dawodu MO, 'AN OVERVIEW OF THE FREEDOM OF INFORMATION ACT (An Appraisal from a Lawyer's Perspective)' <http://portal.unesco.org/ci/en/files/26159/12054862803freedom_information_en.pdf/freedom_informati> accessed 9 January 2019

Elgujja AA, 'Adequacy of the Legal Safeguards for the Patients ' Right of Confidentiality under the Saudi Arabian Legal System' (2017)

Enonchong N, 'The African Charter on Human and Peoples' Rights: Effective Remedies in Domestic Law?' (2002) 46 Journal of African Law 197 <http://journals.cambridge.org/action/displayFulltext?type=1&fid=129090&jid=&volumeId=&issueId=&aid=129089>

Goodhart M, 'Origins and Universality in the Human Rights Debates: Cultural Essentialism and the Challenge of Globalization' (2003) 25 Human Rights Quarterly 935 <https://www.jstor.org/stable/20069700> accessed 15 August 2018

Goodman KW and Miller RA, 'Ethics and Health Informatics : Users , Standards , and Outcomes' in Edward H Shortliffe and James J Cimino (eds), *Biomedical Informatics Computer Applications in Health Care and Biomedicine* (3rd edn, Springer, New York, NY 2006)

Hannum H, 'THE STATUS OF THE UNIVERSAL DECLARATION OF HUMAN RIGHTS IN NATIONAL AND INTERNATIONAL LAW' (1996) 25 GA. J. INT'L & COMP. L. 287 <https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=https://www.google

.com/&httpsredir=1&article=1396&context=gjicl> accessed 2 January 2019

Makulilo AB, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3 International Data Privacy Law 42 <http://idpl.oxfordjournals.org/content/3/1/42%5Cnhttp://idpl.oxfordjournals.org/content/3/1/42.abstract%5Cnhttp://idpl.oxfordjournals.org/content/3/1/42.full.pdf>

MORAVCSIK A, 'Explaining International Human Rights Regimes: Liberal Theory and Western Europe' (1995) 1 European Journal of International Relations 157 <https://www.princeton.edu/~amoravcs/library/explain.pdf> accessed 16 July 2018

Nigeria CB of, 'CENTRAL BANK OF NIGERIA REGULATORY FRAMEWORK FOR BANK VERIFICATION NUMBER (BVN) OPERATIONS AND WATCH-LIST FOR THE NIGERIAN BANKING INDUSTRY' <https://www.cbn.gov.ng/Out/2017/BPSD/Circular on the Regulatory Framework for BVN Watchlist for Nigerian Financial System.pdf> accessed 4 January 2019

Okere OB, 'The Protection of Human Rights in Africa and the African Charter on Human and Peoples' (1984) 6 Human Rights Quarterly 141 (154) <https://heinonline-org.salford.idm.oclc.org/HOL/Page?handle=hein.journals/hurq6&div=19&g_sent=1&casa_token=&collection=journals> accessed 3 January 2019

Oladunjoye O and Oguejiofor B, 'A Critical Evaluation Of The Credit Reporting Act 2017 – Practical Issues Arising' (*Mondaq*, 2018) <http://www.mondaq.com/Nigeria/x/757320/Consumer+Credit/A+Critical+Evaluation+Of+The+Credit+Reporting+Act+2017+Practical+Issues+Arising> accessed 14 January 2019

Orji UJ, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7 International Data Privacy Law 179 <https://search-proquest-com.salford.idm.oclc.org/docview/2056427233?rfr_id=info%3Axri%2Fsid%3Aprimo>

Pollis A and Schwab P, *Human Rights: Cultural and Ideological Perspectives* (Adamantia Pollis and Peter Schwab eds, Praeger 1979)

Protection D, 'Ghana Data Protection Act, 2012'

<https://www.dataprotection.org.gh/sites/default/files/Data Protection Act %2C 2012 %28Act 843%29.pdf> accessed 5 January 2019

Salami E, 'Nigerian Data Protection Law' (2019) 9 Datenschutz und Datensicherheit 576 <https://nitda.gov.ng/>

Udoma U and Osagie B, 'Data Privacy Protection in Nigeria Data Privacy Protection in Nigeria' <http://www.uubo.org/media/1337/data-privacy-protection-in-nigeria.pdf> accessed 26 December 2018

UN, 'Universal Declaration of Human Rights: The Foundation of International Human Rights Law' (*United Nations Website*, 1948) <http://www.un.org/en/sections/universal-declaration/foundation-international-human-rights-law/index.html> accessed 6 January 2019

UNECA, 'Africa's Information Society Initiative: An Action Framework to Build Africa's Information and Communication Infrastructure' (1995) <https://www.uneca.org/cfm1996/pages/africas-information-society-initiative-action-framework-build-africas-information-and> accessed 4 January 2019

van Bogaert DK and Ogunbanjo GA, 'Confidentiality and Privacy: What Is the Difference?' (2009) 51 South African Family Practice 194

African Union Convention on Cyber Security and Personal Data Protection 2000 (African Union Legal Instrument)

Central Bank of Nigeria Act 2007 (Federal Republic of Nigeria Official Gazette)

Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 (Laws of Federation of Nigeria)

Freedom of Information Act 2011 Laws of the Federation of Nigeria 2011 (Laws of the Federation of Nigeria)

National Identity Management Commission Act 2007 (Laws of the Federation of Nigeria)

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY ACT 2007 2007 (Laws of the Federation of Nigeria)