Introduction

Generally, data protection connotes the safeguards observed in handling personal information however stored[1] and the methods adopted in securing same, from being either physically lost or seen by unauthorised persons.[2] Necessarily, data protection is the legal mechanism that ensures privacy of personal information.[3] An efficient data protection framework must be built on cardinal principles of good information handling[4] including: accuracy, adequacy, relevancy, consent, security, confidentiality, accountability, fairness, lawfulness, transparency, collection and storage for specific purposes, and non-transferability to countries without adequate protection.[5]

On 25 May, 2018, the European Union General Data Protection Regulations (GDPR) came into force to establish parameters for the collection and processing of personal information of residents within the European Union (EU). The new GDPR legislation is a significant improvement on the data protection legislation introduced in 1995. The reason for this is not far-fetched. The manner in which information is currently being used has changed exponentially in ways that could not have been envisaged in 1995.

In Nigeria, cybercrime, cyber theft and cyber fraud have increasingly posed a threat to digital security.[6] Although the Nigerian constitution provides for citizens' rights to privacy, it is not clear the extent to which data privacy is guaranteed under Nigerian

[1] Elizabeth A. Martin and Jonathan Law (eds), *Oxford Dictionary of Law* (6th edn, OUP 2006) 148.
[2] Bryan A. Garner, *Black's Law Dictionary* (9th edn, West 2009) 452.
[3] Ursula Smartt, *Media & Entertainment Law* (3rd edn Routledge, 2017) 135.
[4] Ursula Smartt, supra n. 3; World Wide Web Foundation Report, Chukwuyere Ebere Izuogu, 'Personal Data Protection in Nigeria'(March 2018) 6 <http://webfoundation.org/docs/2018/03/WF_Nigeria_Full-Report_Screen_AW.pdf/> Accessed 0n 15 April, 2018, 10; Scottish Qualifications Authority <https://www.sqa.org.uk/e-learning/ITLaw01CD/page_21.htm#OtherDPATerminology/> accessed on 15 June, 2018; IT Governance, Luke Irwin, 31 January, 2018, 'The GDPR: Understanding the 6 Data Protection Principles' <https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles/> accessed on 15 June, 2018; The University of Edinburgh, 8 September, 2015, 'The Eight Data Protection Principles' <https://www.ed.ac.uk/records-management/data-protection/what-is-it/principles/> accessed on 15 June, 2018
[5] Edmonds Marshall McMahon, Kate McMahon and Chloe Salter, 'Risky Business: Hacking, Data Theft, Rogue Employees and Corporate Protection in a Digital Age' <http://www.emmlegal.com/news/risky-business-hacking-data-theft-rogue-employees-corporate-protection-digital-age//> accessed on 15 June, 2018; World Wide Web Foundation Report, Chukwuyere Ebere Izuogu, supra n. 4, p. 9; The University of Edinburgh, March 7, 2018, 'An Introduction to GDPR' <https://www.ed.ac.uk/records-management/data-protection/what-is-it/an-introduction-to-gdpr/> accessed on 15 June, 2018.
[6] Michael Nwakalor, 'Cyber Crime is the Biggest Terror Threat to Nigeria Right Now and it is on the Rise' (27 October, 2016) < http://venturesafrica.com/why-cyber-crime-the-biggest-terror-threat-to-nigeria-is-on-the-rise/> accessed on 20 July, 2018.

law. Pursuant to section 37 of the Constitution,[7] the right to privacy is recognized as a fundamental right in the following words:

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

With the express provisions of section 37 of the Constitution, it is ostensible that the Constitution drafters clearly intended and sought expressly to prohibit any infringement of persons' rights to bodily, communications and territorial privacy. What is not as apparent or is at best arguable, from the provisions of the Constitution, is the recognition of the right of individuals to data protection. Also, section 37 of the Constitution falls short of imposing any specific or general obligation or duty on persons to protect the personal information of individuals that enters lawfully into their possession and is stored by such persons. Nonetheless, the law is trite that every enforceable right implies a corresponding legal duty.[8]

This paper therefore seeks to assess the extent of data protection in Nigeria, particularly in the wake of the GDPR and potential implications for Nigerian companies responsible for collecting and processing data of EU residents.

Overview of the GDPR Legislation

GDPR is Europe's latest framework for data protection. Overruling the Data Protection Directive 95/46/EC, the GDPR harmonizes the standard for data protection across all the 28 European Union member states. The legislation seeks to protect the personal data of all European Union residents, including their identity, address, IP address, and customer reference number, and it applies to all corporate entities involved in citizens' data processing even outside the European Union.

It ensures that customers have control over the way their data is obtained and used by including safeguards to protect the rights of the consumers whose data companies have access to. The regulation achieves this by primarily expanding the scope of what companies must consider as personal data. By the provisions of the regulation, personal data expressly includes genetic data, biometric information and, in certain circumstances, location data, IP addresses and mobile device IDs. Further, the concept of 'pseudonymous data' – personal data that has been subjected to technological measures such as encryption, is officially introduced in the Regulation.[9]

[7]The Constitution of the Federal Republic of Nigeria, 1999 (as amended) (Constitution).
[8] Wiktor Osiatynski, *Human Rights and Their Limits* (1st edn, Cambridge University Press 2009) 37-38.
[9] Opinion 4/2007 of the EU Article 29 Working Party <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en/> accessed 19 June, 2018. See also: The University of Edinburgh, 7 March, 2018, 'An Introduction to GDPR' supra n. 5.

The GDPR also requires companies to be accountable for the data they have stored on EU residents,[10] and it empowers EU residents to request for their personal data to be deleted from or edited on a company's database. Provision is made for compulsory data protection audits, which are designed to ensure compliance with the provisions of the law.[11] Companies that hold, use and share personal data are the subject of these audits. The Regulation goes further to ensure that EU residents can object to companies' use of their data in specific ways as well as stipulate the manner in which such data may be used. In the event of a breach of the Regulation, companies are also under the additional burden to notify the subjects of the data within 72 hours of a breach.[12]

The introduction of tough sanctions for non-compliance is a distinct feature of the Regulation.[13]As with global anti-bribery and anti-trust laws, GDPR is recorded as having one of the highest sanctions for non-compliance, including revenue-based fines of up to 4% of annual worldwide turnover.[14] Notably, the Regulation now compels organizations to self-report to the regulators and to those individuals whose personal data has been compromised under their watch.

The Extent of the Applicability of the GDPR in Nigeria

As highlighted earlier, the GDPR provides international best practice standards on data protection. It is applicable to all 28 (twenty-eight) European Union (EU) member states, including the UK. The Regulation seeks to protect the personal information of all EU residents[15] and applies to all corporate entities involved in their data processing, including entities operating outside the EU. It also seeks to impose cringe-worthy/prohibitive penalties for non-compliance to be administered by the supervisory authorities of individual member states.

It must be mentioned that the GDPR has extraterritorial applicability and as such embraces both multinational and national companies collecting and processing the

[10] Michael Nadeau, 'GDPR: What You Need to Know to Stay Compliant' <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html> (23 April, 2018) accessed 24 July, 2018.
[11] Simply Docs, 'GDPR Data Protection Audit Template' < https://simply-docs.co.uk/IT--Data-Protection-Policies/GDPR-Data-Protection-Audit> accessed 24 July, 2018.
[12] Information Commissioner's Office, 'Report a Breach' < https://ico.org.uk/for-organisations/report-a-breach/> accessed 24 July, 2018.
[13] GDPR Report, 'Guidelines and Consequences for Non-Compliance' (16 June, 2017) <https://gdpr.report/news/2017/06/16/gdpr-guidelines-consequences-non-compliance/> accessed 24 July, 2018.
[14] GDPR, 'Fines and Penalties' <https://www.gdpreu.org/compliance/fines-and-penalties/> accessed 24 July, 2018.
[15] This is quite instructive as it does not apply to citizens of EU member states strictly speaking but rather to residents of EU member states. Naturally, the term 'resident' would contemplate a wider range of individuals irrespective of their nationality. Accordingly, the GDPR inures for the benefit of Nigerians resident in the EU.

personal data of EU residents in Nigeria.[16] In view of the indispensable, transnational and ubiquitous nature of their services, financial institutions, quasi-financial institutions, and Fintech companies in Nigeria appear to be the most vulnerable institutions in light of the extensive application of GDPR, as they collect, process and store vast amounts of personal data of individuals across the world. This means that these institutions will, in the event that they have not already done so, have to create effective internal control measures to ensure prompt compliance with the GDPR's standards, at the risk of being penalised for non-compliance under the GDPR.

An Assessment of Nigeria's Data Protection Framework

In Nigeria, there is currently no singular, all-encompassing legislation on data protection. While this may be so, there are a few legislations and subsidiary legislations which represent industry-specific, yet disjointed efforts to protect personal data in different areas of the society. Some of such legislations include:

- The Credit Reporting Act 2017 (CRA)

The CRA provides for the licensing and regulation of Credit Bureaus, which primarily collect information and prepare credit reports on legal persons. These reports may be utilised by potential lenders to determine the creditworthiness of loan applicants. The CRA makes robust provisions for data protection[17] and imposes a duty on Credit Bureaus to ensure the accuracy, security and confidentiality of personal data collected and stored by them[18]. In specific instances, the CRA also recognises the rights of aggrieved individuals to seek redress in Court for the breach of their rights in relation to their personal data.[19]

- The Freedom of Information Act 2011 (FOIA)

The FOIA provides for public access to public records and information.[20]Nevertheless, the Act obliges a public institution to deny a Freedom of Information Request (FOIR) seeking to access information that contains personal information,[21] unless the individual involved consents to its disclosure, where such information is otherwise publicly available,[22] or where the public interest clearly outweighs the individual's right to privacy.[23]A public institution is also authorised to deny a FOIR that seeks

[16] See Article 3(1) of the GDPR.
[17] Section 6 of the CRA.
[18] Sections 6 & 9 of the CRA.
[19]See section 13(4) of the CRA.
[20] See the Preamble to the FOIA.
[21] See section 14(1) of the FOIA.
[22] See section 14(2) of the FOIA.
[23] See section 14(3) of the FOIA.

access to information which is subject to various forms of professional privileges conferred by law e.g. legal practitioner-client privilege, health worker-client privilege, journalism confidentiality etc.[24]

- The Cybercrimes (Prohibition, Prevention etc.) Act 2015 (Cybercrimes Act)

  The Cybercrimes Act appears to give an expansive interpretation to the constitutional right to privacy under section 37 of the Constitution.[25]According to the provisions of the Cybercrimes Act, law enforcement agencies have a duty to safeguard the confidentiality of information collected, retained and/or processed for the purpose of law enforcement under the Act.[26]

- The National Health Act 2014 (NHA)

  The NHA provides a framework for the regulation, development and management of a National Health System and sets standards for rendering health services in the Federation.[27] Pursuant to the NHA, health service providers are mandated to maintain a database of health service users' information, including information about a health user's health status or treatment,[28] which information is considered confidential[29] and must not be disclosed to third parties without the consent of the health user.[30] The NHA imposes a duty on health service providers to set up internal control measures to ensure the security and integrity of health user information and to prevent unauthorised access to such information.[31] Failure to comply with the provisions of the NHA on data protection is criminalised and is punishable by imprisonment and/or fine.[32]

- The Child Rights Act, 2003 (CRA 2003)

  The CRA 2003 codifies the rights of a child to privacy.[33] The CRA equally prohibits the dissemination of a fostered[34] and adopted[35] child's information to any member of the public except by an order of court. However, the court,[36] government,[37] and Minister[38] charged with responsibility for matters relating to children may be allowed

[24] See section 16 of the FOIA.
[25] See section 38(5) of the Cybercrimes Act.
[26] Section 38(5) of the Cybercrimes Act.
[27] Preamble to the NHA.
[28] Section 25 of the NHA.
[29] Section 26 of the NHA.
[30] Or by order of court. See section 26(2) of the NHA.
[31] Section 29 of the NHA.
[32] Section 29(2) of the NHA.
[33] Section 8 of the CRA 2003.
[34] Section 112 (9) of the CRA 2003.
[35] Section 142 (9) of the CRA 2003.
[36] Section 46 (1) (b) of the CRA 2003.
[37] Section 45 (4) of the CRA 2003.
[38] Section 198 (4) of the CRA 2003.

to access and inspect the records of a child. In respect of a child offender, the CRA prohibits the publication of personal information of a child offender.[39]

- The Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations 2011 (NCC Registration Regulations)

  In line with the Nigerian Communications Commission (NCC)'s objectives and powers to make regulations enshrined under the Nigerian Communications Act (NCA),[40] the NCC published the NCC Registration Regulations in 2011, to provide a regulatory framework for the registration of subscribers to mobile telephone services in Nigeria and the establishment, control, administration, and management of the database of said subscribers' information.[41] The NCC Registration Regulations seek to ensure that key principles of data protection are observed and upheld by network service providers.[42]

- The Nigerian Communications Commission (Consumer Code of Practice) Regulations 2007 (NCC Consumer Code of Practice Regulations)

  Also, the NCC, by its Consumer Code of Practice Regulations, provides for the privacy and protection of consumer information.[43] It is pertinent to note that the provisions of the NCC Registration Regulations and the NCC Consumer Code of Practice Regulations on data protection inure to the benefit of all customers of the relevant network service provider, regardless of their nationality.

- The Central Bank of Nigeria (CBN)'s Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Financial System, 2017 (BVN Framework)

  In February 2014, the CBN, in collaboration with the Bankers Committee, launched the BVN as part of its overall strategy to promote a safe, reliable, and efficient payment system in Nigeria. The BVN gives a unique identity to each customer of Nigerian banks.[44] Subsequently, the CBN released the BVN Framework which, among other things, provides guidelines and institutional safeguards for the protection of personal information of bank customers identified by the BVN.[45]

---

[39] See section 205 (2) of the CRA 2003.
[40] See section 70 of the Nigerian Communications Act, Cap N97, Laws of the Federation of Nigeria, 2010.
[41] Section 2 of the NCC Registration Regulations.
[42] Section 9(4) of the NCC Registration Regulations.
[43] See the schedule to the NCC Consumer Code of Practice Regulations. Particularly, Part VI of the Model Consumer Code of Practice.
[44] The BVN number can be classified as pseudonymous personal data.
[45] Paragraph (1.8) of the BVN Framework.
***** This table is not intended to be exhaustive. The penalties highlighted therein are without prejudice to other remedies which may be awarded by a competent court of law for breach of any of the duties imposed by the relevant legislation on an obligor in relation to data protection.

S/N	Applicable Law	Regulator	Obligor	Consequence(s) of Non-Compliance*
	The Credit Reporting Act	CBN	Credit Bureaus	Revocation or Suspension of Licence and/or Fine
	The National Health Act 2014	N/A	Health Service Providers	Imprisonment and/or Fine
	The Nigerian Communications Commission Regulations	NCC	Mobile Telecommunications Providers	Fine
	CBN Regulatory Framework for BVN Operations 2017	CBN	Banks and other Financial Institutions	N/A

- Professional Codes of Ethics

  By law, certain professional relationships require that information obtained, stored and/or processed within the confines of such relationships are kept confidential and accordingly imposes duties on these professionals to ensure the integrity, security and confidentiality of information obtained in confidence. By law, information disclosed in confidence in any of these relationships enjoys the legal privilege of confidentiality:

  - Legal practitioners;[46]
  - Medical Practitioners;[47] and
  - Journalists.[48]

- Received English Law

  It is pertinent to note that Nigeria's legal system is predicated on received English law, including Common Law and the doctrines of Equity.[49] Accordingly, antiquated rules on

[46]Rule 19 (3) of the Rules of Professional Conduct for Legal Practitioners, 2007 made pursuant to the Legal Practitioners' Act, Cap L11, Laws of the Federation of Nigeria, 2010. See also: section 195 of the Evidence Act, 2011.

[47]See the Code of Medical Ethics made pursuant to the Medical and Dental Practitioners Act, Cap M8, Laws of the Federation of Nigeria, 2010. Also available at <http://www.mdcnigeria.org/Downloads/CODE%20OF%20CONDUCTS.pdf/> accessed on 25 July, 2018.

[48]For the journalist-informant/source relationship, see Rule 4 of the Code of Ethics for Nigerian Journalists made pursuant to section 9 of the Nigerian Press Council Act, Cap N128, Laws of the Federation of Nigeria, 2010.Also available at <http://www.presscouncil.gov.ng/?page_id=281/> accessed on 25 July, 2018.

[49] See generally F. Ajogwu, SAN, *Law & Society* (Centre for Commercial Law Development, 2013) 14-58.

data protection or the privacy of information aptly provided for under Common Law and Equity, form part of Nigeria's legal framework on data protection.[50]

Conclusion

The reality of our time is that personal data is becoming increasingly valuable and is constantly sought for by unscrupulous persons who intend to misuse same to the detriment of the data subjects. The current state of our laws show that that there is a need to establish a holistic regulatory framework for data protection in Nigeria. Noteworthy in this regard are the efforts of the National Information Technology Development Agency (NITDA) to issue the Data Protection Guidelines, a proposed framework to provide guidelines and prescribe minimum data protection requirements for organisations within and outside Nigeria that collect, store, and process the personal data of Nigerian citizens and residents.[51]

Conclusively, however, an amendment of section 37 of the Constitution could provide greater clarity of the scope of the right to data protection of citizens and/or residents of Nigeria and impose a duty on all data controllers collecting, storing, and/or processing personal data of Nigerian citizens and residents to ensure the security and confidentiality of such data.

Furthermore, the introduction of a general data protection law by the National Assembly to apply generally to all data controllers in both the private and public sector would further enhance the legal framework for data protection in Nigeria. Such legislation would impose express duties on all data controllers to protect the personal data of Nigerian residents and citizens in their possession, vest in data subjects a reciprocally enforceable right to data protection, and provide for prohibitive penalties/fines in the event of non-compliance by data controllers.

[50] E.g. Confidentiality resulting from a banker-customer relationship.

[51] See NITDA, 22 February, 2018 <http://nitda.gov.ng/2018/02/22/nitda-alerts-nigerians-on-european-unions-general-data-protection-regulation-implementation-and-enforcement/> accessed on 24 July, 2018. Draft Guidelines available at <http://nitda.gov.ng/wp-content/uploads/2018/02/DATA-PROTECTION-GUIDELINES-Reviewed..pdf/> accessed on 25 July, 2018.