LéLaw
Thought Leadership *Reflections*
June 2021

X-Rays:
Deconstructing Personal Data Under the *Nigerian Data Protection Regulation 2019*

s.ngwu@lelawlegal.com

The world is always in a reformative, renewal or rediscovery process and over time, human experience has shown that the only constant is change. From the earliest days of subsistence living (nil trading), trade by barter, and cash based trading, the world has progressed to significantly transacting online in the digital economy. The technologies of Blockchain, Artificial Intelligence (AI) and Internet of Things (IoT) are the forces driving this economy and almost every country, including Nigeria is striving not to be left behind. The quest for a digital economy means more Personal Data (PD) will be processed; and this has privacy implications.

In a bid to curtail the 'negative' implications, various countries enacted regulations guiding the collection and processing of individuals' data. Following suit, Nigeria enacted the ***Nigerian Data Protection Regulation 2019* (NDPR)** to guide PD of Data Subjects (DS). The concept of PD is a bit complicated, as determining what data does or does not amount to PD, involves a holistic consideration of circumstances. Unfortunately, grasping this concept is key to complying with the principle of Data Protection (DP). Therefore, this article examines the scope of PD under the ***NDPR*** against the background of relevant ramifications.

What is Personal Data?

As a matter of law, ***NDPR*** does not apply to every kind of data; rather it applies only to *"[PD] of natural persons"*. This is provided under ***Article 1.2(a) NDPR***, viz: *"this Regulation applies to all transactions intended for the processing of [**PD**], ... intended to be conducted in respect of **natural persons** in Nigeria"*.[1] According to ***Article 1.3(xix) NDPR,*** PD is *"any information relating to an identified or identifiable natural person ('Data Subject')..."* Certain elements can be deduced from this definition: *'any information', 'relating to', 'an identified or identifiable'* and *'natural person'*; they are respectively considered *seriatim* below.

i. *Any information*

This may entail any information about an individual processed in an automatic or non-automatic medium. It does not matter if the information is true or false, about the individual.[2] Such information may be in the form of alphabetical, numerical, graphical, photographical or acoustic form, provided it represents information about an individual. Thus, a statement about a person's working condition or the person's phone or gender or blood group is information in this regard. For instance, a child who underwent a neuro-psychiatric test made a drawing representing her family, her mood and what she feels about the different members of her family. The drawing was considered information amounting to PD in a court proceeding.[3]

[1] Emphasis supplied.

[2] ***Article 29*** Data Protection Working Party, **'*Opinion 4/2007 on the Concept of Personal Data*'**, 20.06.2007:p.7.: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf (accessed 10.06.2021). According to a notation on the cover of the Opinion, *"This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC."*

[3] See ***Article 29*** Data Protection Working Party, ***(supra)***, p.8 (*Example No. 4*).

ii. 'Relating To'

This is an important element in determining whether data amounts to PD. It was not defined in the ***NDPR*** but we can assume it means information about an individual. According to Article 29 Working Party, "*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.*"[4] In certain circumstances, it may be easy to determine when information relates to an individual. For example, grade information in a student's transcript relates to the student. But in some other situations, the information may indirectly relate to an individual. Thus, information about the market value of an individual's estate can indirectly relate to him, if used to determine tax payable by him.

To determine in all cases whether or not an information relates to an individual, recourse must be made to three elements viz: the content, purpose and result of the information.[5] The classification is not provided in the ***NDPR*** and may arguably be considered academic, but in reality is helpful guidance. The *content element* occurs when information relates to an individual regardless of the purpose or impact of the information. Thus where the content of an information is about an individual irrespective of the purpose or resultant effect of the information, such information relates to an individual. For instance, the medical result of a patient contained in a medical report relates to such patient.

The *purpose element*, relates to when the information is used to evaluate, learn or influence the status or behaviour of an individual. For instance, collecting information about the market value of Mr. A's house at Lekki Lagos to determine tax payable by him. The information about the market value of the house itself is not a PD; but because the purpose relates to Mr. A, may make it a PD. A data can become a PD due to the *result element* when the use of the data is likely to have an impact on the individual. For instance, collecting information about the odometer of car to determine whether a driver drove carelessly either to promote or demote him. It does not matter if the potential result is a major or minor effect. It is sufficient if an individual is treated differently based on the information processed.[6]

It is pertinent to note that the three elements need not occur concurrently, it suffices if one of them is present.[7] If after considering all the circumstances, a PD or an information does not relate to an individual, such will not be protected under the ***NDPR.*** For instance, emails written by a lawyer to their client about the client's matter all contain references to the lawyer's name and place of work, which will be the lawyer's PD. However, the contents of the emails relates to the client's instructions, rather than the lawyers in the engagement team. The contents of the emails are not, therefore, the lawyers' PD where same represents legal advice to the client. However, if a complaint was subsequently made about the lawyer's performance or advice, and the emails were then used to investigate this, the legal advice given in them would become PD.[8]

[4] Working Party Document No WP 105: ***'Working Document on Data Protection Issues Related to RFID Technology'***, *(adopted on 19.01.2005), p.8.* Cited in Article 29 Data Protection Working Party *(**supra**), at p.10.*
[5] Information Commission Office, ***'What is the Meaning of "Relates To"?'***, *Guide to General Data Protection Regulation, 01.01.2021:*https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-the-meaning-of-relates-to/ (last accessed 21.05.2021).
[6] ***Article 29*** Data Protection Working Party ***(supra)****, p.10.*
[7] ***Ibid.***
[8] See *footnote 5.*

iii. 'Identified or identifiable Person'
According to ***Article 1.3(xix) NDPR***, an identified or identifiable person is a "*natural person 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, the mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII)*".

Where a person can be distinguished directly, such person is identified. But where a person can only be distinguished from other persons with the help of one or more identifiers, such person is identifiable. The identification may be directly or indirectly. A common example of direct identification is name. Nevertheless, whether a piece of information is capable of directly identifying an individual is dependent on circumstances. For instance, a name may be too common to be capable of identifying an individual and there may be need to add more identifiers to be able to identify such person. '*Jumoke Forsyth*' may not identify if a person if there two or more persons with the name, but '*Jumoke Forsyth working at PN Ltd as data analyst*' should be able to identify the person. Indirect identifiers alone cannot identify an individual and there maybe need to combine two or more identifiers to be able to identify such a person. For instance, phone numbers or car registration numbers are all indirect identifiers and require further information before it can identify an individual. The element "*identified or identifiable person*" is very important, because where information cannot distinguish an individual, such information will not amount to PD.[9] In determining whether a person is identifiable or not account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.[10]

iv. 'Natural person'
This element entails that the information or data must relate only to living human beings. This means that information relating to legal personality or none living things are not deemed PD under the *NDPR*. For any information to constitute PD under the ***NDPR*** such information must contain all of the four elements listed above.

Categories of Personal Data

PD are categorised into ordinary PD and special or sensitive PD. " *'Sensitive Personal Data' means data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information*".[11] It also includes Bank Verification Number (BVN), and biometrics.[12] These set of PD require high level of consent (explicit consent) and care by data controllers. Ordinary PD are every other data apart from sensitive PD.

Determination: What is and What Is Not Considered Personal Data?

I. *Personal Data identified by* ***NDPR***
NDPR expressly identified the following as PD: *name, an identification number, location data, an online identifier, physiological data, genetic data, mental data, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII)*. Notwithstanding the above listed data, there is an inexhaustive list of what may constitute personal data.

[9] ***Ibid.***
[10] ***Ibid.***
[11] ***Article 1.3(xxv).***
[12] NDPRAdmin, ***'Processing Sensitive Personal Data'***, *NDPR Academy*, 16.04.2021: https://blog.ndpracademy.ng/processing-sensitive-personal-data/ (last accessed 07.06.2021).

ii. Incorporated/unincorporated data

The definition of PD and DS[13] narrows it down to 'information relating to natural person'. A natural person as distinguished from a legal person means a living human being. Therefore any pieces of information relating to companies, business names, clubs, associations and other similar institutions are not PD. Therefore company's registration number (RC No.), email such as info@company.com, the name of the company, address, etc are not PD. But the data of its directors, shareholders, and employees are PD which are protected under ***NDPR.***

According to a learned author:[14] "*Although the European Commission states that company registration is not considered a personal data this writer thinks that such a blanket waiver betrays the principle of unique identifier and context of identification and/or processing. It may be favourably argued that, where a person's identity and other personal data are linked to his/her company's registration number, then it may necessarily follow that, an unlawful processing of such company registration number will impact on the person's privacy and data protection rights.*" Therefore, where corporate data relates to individuals, in terms of: *'content'*, *'purpose'* or *'result'*, such will amount to PD.

iii. Data of Deceased Person

Data of a deceased person is not PD because **NDPR** covers only data of "*identified or identifiable natural person*". However, where deceased data relates to a living identifiable person, such data may amount to PD protected under ***NDPR.***

iv. Structured/Unstructured Data

NDPR recognises two means of processing PD: automated and non-automated (manual filing system). Non-automated processing which forms part of a filing system is PD. "*Filing system means any structured set of Personal Data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis*".[15] An example are papers or file arranged in alphabetical order. A structured paper file constituted PD under **NDPR.**[16] However, an unstructured manual filing data are set of raw and disorganised data not held as part of a filing system. This type of data are not regarded as PD. This is because it might be impossible to identify data subject from the data.

v. Pseudonymised/Anonymised Personal Data

These terms are not provided in the **NDPR**. However, **European General *Data Protection Regulation* (GDPR)** defined it as: "*pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".[17] It simply allows the original data to be redacted to conceal the identity of the data subject. For instance, Key-coded data are good example of pseudonymised data. Pseudonymised data are still PD since the process is reversible.[18] However, when data are irreversibly altered to de-identify data subject it can no longer become PD and it is called anonymisation.

[13] ***Article 1.3(xiv).***
[14] Olumide Babalola, **'Understanding The Elasticity And Scope of "Personal Data" In The Context of Nigeria Data Protection Regulation (NDPR)'**, *Mondaq*, 06.04.2021: https://www.mondaq.com/nigeria/data-protection/913848/understanding-the-elasticity-and-scope-of-personal-data-in-the-context-of-nigeria-data-protection-regulation-ndpr (last accessed 07.06.2021).
[15] ***Article 1.3 (xvi).***
[16] ***Article 1.3(xvi).***
[17] ***Article 4(5) GDPR 2018.***
[18] **Recital 26 GDPR 2018.**

vi. *Volunteered, Observed and Inferred data*

Volunteered data are data willingly provided by individuals such as creating social media profiles or using credit card to purchase something online.[19] Observed data are data generated by recording activities of an individual and it includes data generated from security camera, facial recognition, browser cookies etc.[20] Majority of the data generated from Internet of things are deemed to be observed data.[21] Inferred data or metadata are data inferred from analysing volunteered and observed data and it is used for predictive purpose.[22] Both the observed, volunteered and inferred data are PD.[23]

vii. *Fictitious social media account name*

Social media accounts are replete with fictitious usernames or information about an individual. For instance, it may not be unusual to find *Facebook*, *Instagram* or *Twitter* account name like *'kingmaker', 'Lilsexy' etc.* These data although not real names of the users are regarded by ***NDPR*** as PD, since they are information capable of identifying their users if combined with other factors. However, where the fictitious name is such to make identification impossible, it will not amount to PD.

Conclusion

Understanding the concept of PD is very fundamental in complying with the provisions of the ***NDPR.*** Where it becomes difficult to determine whether or not a set of data amounts to PD, it is advisable as a matter of good practice (or erring on the side of caution), to treat such data with care, and observe the provisions of ***NDPR.***

LeLaw Disclaimer:

Thank you for reading this article. Although we hope you find it informative, please note that same is not legal advice and must not be construed as such. However, if you have any enquiries, please contact the authors at: s.ngwu@lelawlegal.com or email: info@lelawlegal.com

[19] World Economic Forum and A.T Keaney, ***'Rethinking Personal Data: A New Lens For Strenthening Trust'***, *May 2014, p.16:* https://reports.weforum.org/rethinking-personal-data/near-term-priorities-for-strengthening-trust/ (accessed 03.06.2021).
[20] ***Ibid.***
[21] ***Ibid**, footnote 16.*
[22] Dara-Agnes Ubia, ***'Exclusive Data Exploitation in Data Driven Markets: The Competition And Data Protection Conundrum'***, Streamsowers and Kohn, 26.05.2021: https://www.youtube.com/watch?v=UwA3N135gQU (last accessed 03.05.2021).
[23] ***Article 1.3 xix.***