

# RIGHTS OF DATA SUBJECTS AND THEIR ENFORCEMENT UNDER THE NIGERIA DATA PROTECTION REGULATION 2019

TSEDAQAH  
ATTORNEYS



# 01

## INTRODUCTION

With the inception and increase in the use of information technology, there has been a need to protect the collection and processing of personal data used for social and economic purposes.

Many public and private bodies have migrated their respective businesses and other information systems online. Information solutions in both the private and public sectors now drive service delivery in the country through digital systems. These information systems have thus become critical information infrastructure which must be safeguarded, regulated and protected against atrocious breaches<sup>1</sup>.

The protection of personal information dates back to the establishment of the Tort of Breach of Confidence by the English Court in the case of *Prince Albert v Strange (1849) 18 LJ CH. 120*. In that case, The High court of Chancery awarded Prince Albert an injunction restraining Mr. Strange from publishing a catalogue describing Prince Albert's etchings.

On the 25<sup>th</sup> day of January 2019, the National Information Development Technology Agency (NITDA), which is statutorily mandated to develop Regulations for electronic governance and monitor the use of electronic data interchange and other

---

<sup>1</sup> Preamble to the Nigeria Data Protection Regulation, 2019

# 02

forms of electronic communication transactions, issued the "Nigeria Data Protection Regulation, 2019" (NDPR).

The Regulation is considered the most comprehensive data protection framework in Nigeria which is set to achieve some underlining objectives, *inter alia*: to safeguard the rights of natural persons to data privacy; to foster safe conduct for transactions involving the exchange of Personal Data; to prevent manipulation of Personal Data; and to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

The bulk of this work is centered around Data Privacy Challenges in Nigeria, the Rights of Data Subjects and enforcement of same under the Nigeria Data Protection Regulation

## WHAT IS DATA AND PERSONAL DATA?

Under the NDPR, "Data" means characters, symbols and binary on which operations are performed by a computer. Which may be stored or transmitted in the form of electronic signals, is stored in any format or any device<sup>2</sup>.

---

<sup>2</sup> Article 1.3d of the Nigeria Data Protection Regulation, 2019

# 03

What then is Personal Data? Personal Data is defined as any information relating to an identified or identifiable natural person (referred to as '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<sup>3</sup>.

Simpliciter, Personal Data can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others<sup>4</sup>.

## DATA PRIVACY AND DATA PROTECTION DEFINED

Overtime, the term "Data Privacy" has been used interchangeably with the term "Data Protection". While both terms are related, it must be noted that they are not the same.

Data Privacy, also called information privacy, is the aspect of information technology that deals with the ability an organization or individual has to

---

<sup>3</sup> Article 1.3q

<sup>4</sup> supra

# 04

determine what data in a computer system can be shared with third parties<sup>5</sup>.

Data Protection, on the other hand, is the process of safeguarding important information from corruption, compromise or loss<sup>6</sup>.

To show the distinction between both terms, an analogy of a child is given: When a child is born, he or she does not have the consciousness of his/her right to privacy or even infringement of it, compared to when he/she becomes an adult wherein the consciousness for privacy becomes eminent. No adult will intentionally allow another human to invade his/her privacy without consent sought and obtained and will as such seek to guard against “trespassers”.

Having had a sneak peek, we shall now look at the issue of Data Privacy in Nigeria, Rights of Data Subjects, and how they can be enforced under the NDPR.

## DATA PRIVACY CHALLENGES IN NIGERIA AND THE RIGHTS OF DATA SUBJECTS UNDER THE NDPR

Until the recent case of *Emerging Market Telecommunication Services v Godfrey Nya Eneye*<sup>7</sup>,

<sup>5</sup> <https://searchcio.techtarget.com/definition/data-privacy-information-privacy>. Accessed on the 9<sup>th</sup> of July, 2020.

<sup>6</sup> <https://searchdatabackup.techtarget.com/definition/data-protection> Accessed on the 9<sup>th</sup> of July, 2020.

<sup>7</sup> (2018) LPELR-46193

# 05

hardly can one cite a case with regards to the violation of data privacy of citizens in Nigeria. In that case, the Plaintiff, a legal practitioner sued the operators of Etisalat mobile line for sharing his telephone number to third parties which sent him unsolicited text messages thereby breaching his right to privacy enshrined under Section 37 of the Constitution of the Federal Republic of Nigeria 1999 as amended (Constitution).

Both the Trial Court and the Court of Appeal held that by giving those unknown persons and organizations access to the Respondent's Etisalat GSM phone number to send unsolicited text messages into it, led to violation of his right to privacy guaranteed by Section 37 of the Constitution.

A very common instance of Data privacy challenge in Nigeria occurs where website user's personal information/data are collected by the use of cookies and stored in the browser history and websites visited. Such information will thereafter be shared with advertisers to send unsolicited messages to such users without their consent first sought and obtained.

With the issuance of the Nigeria Data Protection Regulation, there are several outlined rights of Individuals called Data Subjects<sup>8</sup>. Data Subjects have the right to obtain information about the processing of their personal information (Personal Data)<sup>9</sup>. When a Data Subject visits a website, there are several options that will appear on the use of

---

<sup>8</sup> Part 3 of the NDPR

<sup>9</sup> No data shall be obtained except the specific purpose of collection is made know to the Data Subject (Article 2.3)

# 06

cookies in collecting their personal data. An information like the one shown below pops up to such a website user with an option to either agree or disagree:

***We use cookies to help promote our services and improve your site experience. If you continue to use our web site, we will assume you are ok with our use of cookies. You can use the settings tool to change your cookie settings for this site at any time.***

Also, as mandated by the NDPR, all organizations who determine how personal data is processed (called Data Controllers) must ensure that any medium through which personal data is being collected or processed displays a simple and conspicuous privacy policy that the class of Data Subjects being targeted can understand<sup>10</sup>.

The privacy policy shall in addition to any other relevant information contain the following: a) what constitutes the Data Subject's consent; b) description of collectable personal information; c) purpose of collection of personal data; d) technical methods used to collect and store personal information, cookies, JWT, web tokens etc.; e) access (if any) of third parties to personal data and purpose of access; f) a highlight of the principles governing data processing g) available remedies in the event of a violation of the privacy policy; h) the

---

<sup>10</sup> Section 9 of the NDPR

# 07

time frame for remedy and i) any limitation clause, provided that no limitation clause shall avail any Data Controller who acts in breach of the principles of lawfulness.<sup>11</sup>.

Further, where the consent of the data subject is sought and obtained, the Data Controller is under obligation to ensure that consent has been obtained without fraud, coercion or undue influence. Where processing is based on consent, the Controller shall be able to demonstrate that the Data Subject has consented to processing of his or her personal data and the legal capacity to give consent<sup>12</sup>.

If the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the NDPR shall not be binding on the data subject<sup>13</sup>.

The Data Subject must be informed of his/her right and the ease to withdraw his consent at any time prior to giving consent. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

---

<sup>11</sup> Supra

<sup>12</sup> Article 2.3 of the NDPR

<sup>13</sup> Supra



# 08

In addendum to the right to withdraw consent, the data subject has the right to request that his/her personal information is deleted without delay and the Controller shall delete personal data where one of the following grounds applies: a) the personal data is no longer necessary in relation to the purposes for which it was collected or processed; b) the Data Subject withdraws consent on which the processing is based; c) the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing; d) the personal data have been unlawfully processed; and e) the personal data have to be erased for compliance with a legal obligation in Nigeria<sup>14</sup>.

The data subject shall have the right to receive his/her personal data which was provided to a data controller and shall have the right to transmit those data to another data controller without hindrance from the data controller to which the personal data has been provided. This right can only be exercised in circumstances where the processing is based on consent, or on a contract, and the processing is carried out by automated means. However, this right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller<sup>15</sup>.

It must be noted that the exercise of the foregoing rights shall be in conformity with constitutionally guaranteed principles of law for the general protection and enforcement of fundamental rights<sup>16</sup>.

---

<sup>14</sup> Article 2.13.8 of the NDPR

<sup>15</sup> Part 3 of the NDPR

<sup>16</sup> Article 2.13.15 of the NDPR

# 09

## **ENFORCEMENT OF THE RIGHTS OF DATA SUBJECTS UNDER THE NDPR**

Data Privacy and Protection are guaranteed under the Right to Privacy enshrined in Section 37 of the Constitution. The constitution guarantees the right to privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.

Although the Constitution does not mention data or even personal data, it can still be gleaned from the grundnorm. Thus, any person who alleges that his right has been, is being or is likely to be contravened in any State in relation to him may apply to a High Court in that State for redress<sup>17</sup>. A "High Court" in this case has been defined to mean both the High Court of a State, High Court of FCT and the Federal High Court<sup>18</sup>.

The NDPR also makes provisions for *Administrative Redress Panel (ARP)* where a Data Subject may seek redress for the contravention of his/her rights. The ARP is set up to act as a quasi-court for investigating allegations of any breach of the provisions of the NDPR and determination of appropriate redress within 28 working days.

Nevertheless, the establishment of the ARP does not restrict the right of a Data Subject to seek redress in a court of competent jurisdiction.

---

<sup>17</sup> Section 46(1) of the Constitution of the Federal Republic of Nigeria, 1999 (as amended)

<sup>18</sup> Order 1, Rule 2 of the Fundamental Rights (Enforcement Procedure) Rules 2009

# 10

## CONCLUSION

The NDPR makes provisions for data subjects to lodge their complaints with the NITDA or another relevant regulator and any person who is found to be in breach of the data privacy rights of any Data Subject shall be liable to a fine in addition to any other criminal liability. For a Data Controller dealing with more than 10,000 Data Subjects, a fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million naira whichever is greater shall be levied.

While in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 2 million naira whichever is greater has been prescribed.

With the full knowledge of the enormous rights of Data Subjects and the consequences for breach, Data Controllers are enjoined to comply with the provisions of the NDPR and ensure that the objectives are realized.



Elfrida **Igbikiowubo**  
Is an Associate at  
Tsedaqah Attorneys

