

An Overview Of Data Protection And Data Privacy Under The Nigerian Law

Introduction

Data is considered to be the ‘oil’ of the digital era. The 21st century, commonly dubbed "the information age" with its greatest invention, the internet and social media have brought about fast and easy dispensation of personal information or data. Social media is the greatest accomplice to the speedy dispensation of personal information around the world as every internet user dispenses personal data such as name, address, pictures, email address, bank details, or medical information online. These details are mostly required before access can be granted to social media users or for electronic financial transactions. Although, social media users are often, advised of data privacy terms, the advice do not necessarily preclude the use or sharing of such personal data in specified circumstances. This introduces the risk of having personal sensitive information shared with or sold to high-level security agents or blue-chip companies to enable surveillance and data gathering. In 2008, there was widespread information regarding how top brands such as Facebook, Panera Bread and Sacramento Bee experienced data breaches that exposed several millions of personal records to abuse by criminals.

Being a lucrative venture, hackers tend to sell stolen data to internet fraudsters or professional scammers. In 2018, Cambridge Analytica Limited, a British political consulting and strategic communication firm shook the world when it was found to have illicitly collected the personal data and information of about 87 million Facebook users without their consent for political advertising purposes (especially in the run-up to the 2016 US Presidential elections). This scandal amongst other previous data privacy breaches signalled the urgent need to protect personal data. It prompted the immediate implementation of the EU General Data Protection Regulation (GDPR) in 2018.

The world biggest companies including Google, Apple, Facebook, Amazon, Baidu, and Tencent have contributed significantly to making data more valuable, available and abundant, as users are required to provide personal information to facilitate access. These personal information if not adequately protected can be exploited to harm users unscrupulously for economic gain. Therefore, it has become important to protect and regulate collection and use of these data.

This paper examines the differences between Data Protection and Data Privacy, the legal frameworks of data protection and privacy in Nigeria and key provisions of Nigeria Data Protection Regulation (NDPR) 2019.

Definition of Data, Data Protection and Data Privacy

Data is an individual unit of information which may be measured, collected and reported, stored and analysed. It is an information, which is being processed by means of equipment operating automatically in response to instructions given for that purpose. In computing, data is information that has been translated into a form that is efficient for movement or processing.

Data protection refers to the safeguarding of important personal data or information from loss, corruption or compromise by external attackers and mischievous insiders.

Data privacy: refers to privacy rights of individuals, how their personal data or information is collected, used and shared.

Understanding the Distinction between Data Protection and Data Privacy

Data breaches cause tremendous problems, not only for the company affected, but also for its clients. Depending on the company, stolen data can range from relatively benign information to extremely personal details. In any case, a breach can result in extensive monetary damages and significant loss of goodwill for the Company.

Despite the frequency of data breaches and their attendant publicity, not many people actually understand the difference between data privacy and data protection. The distinction are as outlined below:

1. Data Protection is focused on protecting assets from unauthorized use, while data Privacy defines who has authorized access.
2. Data privacy is the regulations or policies that governs the use of data when shared, while data protection is the mechanism, that is, the tools and procedures to enforce the policy and regulation, including the prevention of unauthorized access or misuse of the data that the user agreed to share.
3. The important distinction between data protection and data privacy is "who controls which part". Data privacy controls are mostly given to users. Users can usually control which data is shared. Data Protection is mostly a company's responsibility. Companies need to make sure that the privacy settings of users are implemented and data protected.
4. Data privacy is about keeping your information from being sold or shared, while data protection focuses on keeping that information from hackers.
5. Data privacy regulates the use of data lawfully collected by people, how they are required to use the data; and control the data subject have over that retention and use of the data. Data protection ensures that your personal data is safeguarded from unlawful access by unauthorized parties.
6. Data protection focuses on protecting organizations' assets. It is mostly about keeping threats out, while data privacy is all about what is done with people's data. It deals with how data is handled and managed inside the organization.

Legal Frameworks of Data Protection and Data Privacy in Nigeria.

Nigeria is one of the few countries that have initiated data privacy and protection laws across the globe. Despite the array of laws and regulations in this subject area, the only law that specifically and comprehensively deals with this phenomenon is the Nigeria Data Protection Regulation (NDPR) issued in 2019 by the National Information Technology Development Agency (NITDA).

Prior to the NDPR, most laws on data privacy and protection in Nigeria were industry specific. For instance, the various NCC regulations were made to protect consumers in the telecommunications sector; the provisions in the Child Rights Act protects persons under the age of 18 and the Freedom of Information Act protects personal data in records of public institutions. Therefore, the establishment of the NDPR, a data privacy and protection law, which transcends industries and category of persons is highly commendable.

The following are the existing legal frameworks regulating data protection and data privacy in Nigeria;

1. **Nigeria Data Protection Regulation (NDPR) 2019**

NDPR is the principal data protection legislation in Nigeria. The National Information Technology Development Agency (NITDA) issued it on 25th January 2019 pursuant to Section 32 of the NITDA Act 2007. This robust regulation was issued to regulate the comprehensive use and control of data in Nigeria.

The Regulation applies to all transactions intended for the processing of personal data in respect of natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent. It is instructive to note that in outlining its scope, the Regulation does not contemplate protection of entities. It applies only to natural persons and not artificial persons. Whilst the intention of the NITDA to protect the personal data of persons of Nigerian descent regardless of their country of residence is laudable, extending the scope of the Regulation to such persons is somewhat overreaching, due to the potential challenges which would be encountered in enforcing the Regulation outside Nigeria.

It is important to point out that the Regulation contemplates collaboration with regulatory and law enforcement authorities in other jurisdictions in order to safeguard the privacy of data subjects, however the provision in this regard is limited to “transfer of personal data to a foreign country or an international organization”. Also, the Regulation is intended to operate as an added layer of protection to existing data protection legislation locally and internationally. Thus, persons who process or control personal data of individuals are also expected to comply with existing obligations in other legislation (as applicable) in addition to those imposed under the Regulation. Furthermore, the Regulation expressly distinguishes between personal data and sensitive personal data. The import of the foregoing is that the Regulation requires the same degree of protection to be accorded to the various components, which constitute personal data and sensitive personal data.

2. **Constitution of the Federal Republic of Nigeria, 1999 (as amended)**

Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) makes provision for data protection and data privacy. The section guarantees and protects the right of privacy of Nigerians with respect to their homes, correspondence, telephone conversations and telegraphic communications.

3. **Consumer Code of Practice Regulation 2007** –

The Nigerian Communications Commission (NCC) issued the regulation. Regulation 35 requires licences in the telecommunications sector to ensure adequate protection of customer data.

4. **The Freedom of Information Act 2011**

Section 14 of the Freedom of Information Act protects personal data. Public institutions are prevented from disclosing data containing personal information except where the data subject consents to its disclosure or where the information is publicly available. The Act also provides that a public institution may deny the application for disclosure of information that is deemed privileged by law (e.g. Attorney-client privilege, doctor-client privilege).

5. **The Central Bank of Nigeria Act 2007**

Pursuant to this Act, CBN issued the Consumer Protection Framework 2016, which requires financial institutions to ensure adequate protection of consumer data.

6. **The Child's Right Act 2003**

Nigeria adopted the Child Rights Act (CRA) in 2003 to domesticate the United Nations Convention on the Rights of the Child. This is a human rights treaty designed to guarantee the civil, economic, political, social, health and cultural rights of children. The CRA is a legislation to provide for and protect the rights of a Nigerian Child or a person under the age of 18 years.

Section 3 of Part II CRA incorporates by reference the provisions of Chapter IV of the Constitution, which deal with the fundamental rights of citizens. Also, section 8 of the CRA which covers a child's rights to private and family life states that a child is entitled to his privacy, family life, home, correspondence, telephone conversations and telegraphic communication.

7. **The National Identity Management Commission (NIMC) Act 2007**

Section 26 of this Act requires the approval of the Commission before a corporate body or anybody can have access to data stored in their database. The Act also empowers the NIMC to collect, collate and process data of Nigerian citizens and residents.

8. **The National Health Act 2014**

This Act requires health establishments to maintain and ensure the confidentiality of health records of every users of health services.

9. **The Cybercrime (Prohibition, Prevention, etc) Act 2015**

The CPPA fundamentally established a framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It imposes an obligation on mobile networks; computer and communications service providers to store and retain subscriber information for a period of two years. Significantly, it requires such service providers to accord premium to an individual's right to privacy as enshrined in the Constitution and to take steps

towards safeguarding the confidentiality of data processed. It is the Nigeria's foremost law on cybercrimes. See Sections 12, 14, 16 and 19 thereof.

10. **The HIV and AIDS (Anti-Discrimination) Act 2014**

Section 13(1) of the Act grants all persons living with HIV or affected by AIDS the right to protection of data with respect to their health and medical records.

11. **The Nigerian Communications Commission (NCC) Act 2003**

Pursuant to section 70 of the Nigerian Communications Act 2003 (NCA 2003), the NCC is empowered to make and publish regulations concerning multiple subjects including but not limited to permits, written authorisations, licenses, offences and penalties relating to communication offences. Drawing from this authority, the NCC issued the NCC Regulations, which apply to telecommunications companies. Regulation 9 of the NCC Regulations specify that, in furtherance of the rights guaranteed by section 37 of the Constitution and subject to any guidelines issued by the NCC or a licensee, any subscriber whose personal information is stored in the Central Database is entitled to request updates; to have the data kept confidential; not to have subscriber information duplicated except as prescribed by the NCC Regulations or an Act of the National Assembly; and to preserve the integrity of the subscriber's information. Also, licensees are required to utilise subscriber's information in accordance with the law; likewise, licensees and other named parties are required not to retain biometrics of any subscriber after transmission to the Central Database. Regulation 10 of the NCC Regulations is to the effect that any release of the personal information of a subscriber must be subject to the consent of the subscriber or in accordance with the provisions of the Constitution of the Federal Republic of Nigeria or any other Act of the National Assembly or the NCC Regulations as may be amended from time to time.

12. **The Credit Reporting Act 2017**

Section 9 thereof guarantees the right of data subjects under the Act to privacy and confidentiality with respect to their credit information held by credit bureaux.

13. **The NCC's Registration of Telephone Subscribers Regulation 2011**

Regulations 9 and 10 provide for confidentiality of records of telephone subscribers maintained in the NCC's central database.

14. **The Federal Competition and Consumer Protection Act 2019**

Section 34(6) stipulates that the Federal Competition and Consumer Commission shall ensure that business secrets of all parties concerned in investigations conducted by it are adequately protected during all stages of the investigation or inquiry.

Key rights of Nigerians (Data Subjects) under the Nigeria Data Protection Regulation 2019

The key rights that individuals with respects to their personal data are as follow;

1. Right to request access to his personal data. **See Section 3.1(7)(h) of the NDPR**
2. Right to rectify his personal data. **See Section 3.1(7)(h) of the NDPR**
3. Right to request the deletion and erasure of his personal data. **See Section 3.1(7)(h) and 3.1(9) of the NDPR**
4. Right to object to processing of his personal data. **See Section 2.8 of the NDPR**
5. Right to restrict processing of his personal data. **See Section 3.1(7)(h) & (11) of the NDPR**
6. Right to have his personal data transmitted directly from one controller to another, where technically feasible. **See Section 3.15 of the NDPR**
7. Right to be informed of his right and method to withdraw his consent at any time. **See Section 2.3(2)(c) of the NDPR & Section 8.3 of NDPR**.
8. Right to object to marketing of his personal data. **See Section 2.8 (a) of the NDPR**
9. Right to complain to the relevant data protection authorities or seek redress in a court of law. **See Section 2.10 and 4.2 of the NDPR**
10. Right to receive his personal data which has been provided to a data controller, in a structured, and machine-readable format. **See Section 3.1(14) of the NDPR.**

Key Principles applicable to the Processing of Data under the Nigeria Data Protection Regulation 2019

1. Data controllers must have a lawful basis for processing personal data. **See Section 2.2 of the NDPR**
2. The purpose for which personal data is processed must be clearly stated by the data controller. **See Section 2.1 of the NDPR**
3. The data controller should limit the processing and/or collection of personal information to achieving the specific purpose for which the information is collected or processed. **See Section 2.1(1) (b)&(c) of the NDPR**.

4. The data controller shall not use the information without taking steps to ensure with reasonable certainty that the data is accurate and up-to-date.
5. Personal data shall be kept in a form which permits identification of data. **See Section 2.1(1)(c) of the NDPR**
6. There must be a lawful basis for processing. **See Section 2.2 of the NDPR**
7. Data Security - Section 2.1(d) of the NDPR provides that personal data should be secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, and dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements. Also, Section 19.3 of the Cybercrime Act requires financial institutions to put in place effective counter-fraud measures to safeguard sensitive information.

The conditions under which Personal Data would be deemed to have been lawfully processed.

1. Where consent of the Data Subject has been procured
2. Where processing is necessary for the performance of contract to which the Data Subject is a party
3. Where it is required for compliance with a legal obligation which the Data Controller i.e. the person or body of persons who determine the purposes for which and manner in which Personal Data is being or to be processed, is required to discharge
4. Where it is required to protect the vital interests of the Data Subject
5. Where it is required for carrying out a task in the public interest or in the exercise of an official public mandate imposed on the Data Controller.

Procuring Consent from a Data Subject

The NDPR prescribe the circumstances under which consent may be extracted from a Data Subject as follows

1. The specific purpose of collection of Personal Data must be made known to the Data Subject before his consent may be secured and deemed lawful
2. The Data Controller is obliged under the law to ensure that consent of the Data Subject is obtained without fraud, coercion or undue influence; and in doing so, regard must be had to the legal capacity of the Data Subject
3. The Data Subject must be aware of his right to withdraw his consent at any time (provided that he is bound by acts carried out pursuant to initial consent before withdrawal), and also, the nature of the consent must be examined, to determine whether it is conditional or excessive for the performance of the contract, and whether data is transferable to a third party under a contract.

4. Privacy Policy to be displayed. All media through which Personal Data is being collected must display in a simple, conspicuous and understandable manner, their applicable privacy policy.

The Online Tracking Technologies by Online Platforms to capture Personal Data.

The online technologies include;

1. Web-bugs
2. Cookies
3. JavaScrip
4. Device fingerprinting.

Types of Information Collected by Online Platforms

The personal information or data includes;

1. Internet Protocol (IP) address
2. Click stream data
3. Name, Birth date and Location information
4. Email address and Telephone number
5. Photos
6. Credit/Debit Card details
7. Search queries
8. Social security number and device identifies
9. sexual preferences and Racial or ethnic origin

Data Controller/Processor in Nigeria and Purpose of Collecting Personal Data

1. **The National Identity Management Commission (NIMC) -** for creation of national identification number (NIN), issuance of the national electronic identity card, issuance of multipurpose identity card (e-ID card), and issuance of multi-purpose identity card.
2. **Providers of mobile telecommunications services; Independent Registration Agents; and Subscriber Registration Solution Providers -** for

activation of mobile telecommunications services and to verify the identity of owner of a SIM card used in connection with the commission of a crime.

3. **Independent National Electoral Commission (INEC)** - for issuance of voter card and to authenticate the identity of registered voters.
4. **Nigerian Immigration Service (NIS)** - for issuance of e-Passport.
5. **Deposit Money Banks (DMBs) and Other Financial Institutions (OFIs)** – for issuance of bank verification number (BVN) and bank account opening.
6. **Federal Road Safety Corps (FRSC)** – for issuance of driver's license and issuance of vehicle license.
7. **National Population Commission (NPC)** – for census calculation.
8. **Central Criminal Registry of the Nigerian Police Force (NPF)** – for issuance of police clearance certificate.
9. **Airline operators; Travel agencies; Hotels service providers; and Transportation service providers** – for airline flight booking/reservation.
10. **Credit bureaux** – for credit information of individual borrowers.
11. **Federal Inland Revenue Service (FIRS); Joint tax board (JTB)** – for issuance of tax identification number (TIN).
12. **Corporate Affairs Commission (CAC)** – for registration of a company or business name.
13. **Health Establishments; Health Management Organizations (HMOs); National Health Insurance Scheme (NHIS)** – for medical diagnosis and treatment.
14. **Central Motor Registry of NPF** – for vehicle registration.
15. **Educational institutions** – for registration and attendance at classes.
16. **Pension Fund Administrator (PFA)** – for registration for pension.
17. **The Nigerian Social Insurance Trust Fund (NSITF); Private and public sector employers** – for registration under the workmen's compensation scheme for the payment of compensation to employee or their dependants for any death, injury, disease or disability arising out of or in the course of the employee's employment.
18. **Private and public sector employers Recruitment agencies** – for employment.
19. **Federal Civil Service Commission (FCSC)** – for employment.
20. **Marriage registries** - issuance of a marriage certificate.

Conclusion

The issuance of the NDPR shows NITDA's seriousness towards protecting the privacy of individuals by protecting their personal data. Some organizations in Nigeria have already begun compliance with the provisions of the NDPR by putting up data security measures and fulfilling other compliance requirements. However, a number of organizations are yet to comply with the provisions of the NDPR.

It is imperative for all Data Controllers to engage the services of DPCOs, which are authorized by the NITDA, to review their data privacy policies and practices and help them navigate through the compliance requirements provided under the NDPR.

References

https://webfoundation.org/research/personal-data-protection-in-nigeria/

https://www.mondaq.com/nigeria/privacy-protection/834202/data-privacy-regulations-under-the-nigerian-data-protection-regulation-2019

https://home.kpmg/ng/en/home/insights/2019/08/the-nigeria-data-protection-regulation.html

https://www.dlapiperdataprotection.com/index.html?t=law&c=NG

https://www.aelex.com/wp-content/uploads/2019/05/An-overview-of-Big-Data-and-data-protection-in-Nigeria-1-compressed.pdf