

NDPR? DATA PRIVACY FOR NIGERIAN BUSINESSES



Introduction

Start-Ups, SMEs and small companies are replete with personal information obtained from customers through their platforms, mobile applications or online websites. They are hence easy prey in relation to data breaches. Apart from helping boost investor and consumer trust in any company and its products, companies should understand data privacy and the Nigeria Data Protection Regulation (NDPR) to avoid falling victim to data breaches and heavy fines by the National Information Technology Development Agency (NITDA). For instance, NITDA recently fined Electronic Settlements Limited (parent company of Paypal and CashEnvoy) N5,000,000 for violating the NDPR.¹ Data is essential to the operations of many companies, which emphasises the need for them to be privacy compliant.

Personal Data?

This is simply any personally identifiable information e.g. a person's name, home address, phone number, age, bank details, passwords, etc. It includes all information a person may be identified with.

¹ Techpoint Africa, “[-NITDA fines fintech company, Facebook and COVID-19 Vaccines, Kenyas drone registrations Techpoint Africa](#)” (16th March 2021)



Data Privacy/Protection?

Data Privacy relates to a person's right to control how their personal data is used or processed. Data Protection refers to the measures related to protecting personal data from unauthorised access, including legal and technological measures to safeguard a person's data privacy. Data Protection laws safeguard personal data privacy. Both concepts are Siamese twins that cannot function without the other.

The right to privacy of citizens, their homes, correspondence, telephone conversation and telegraphic communications is a fundamental right guaranteed by the Nigerian constitution² and persons may choose to enforce this right in the event of an infringement. A data subject is any person whose personal data is obtained or processed by controllers and processors.

NDPR?

The NDPR³ is Nigeria's foremost data protection regulation aimed at controlling the collection, use, storage and processing of the personal data of persons residing in Nigeria and Nigerians residing outside Nigeria. It safeguards the data privacy rights of Nigerians and persons residing in Nigeria. NITDA is the agency that enforces this regulation. The regulation touches on principles of data processing, the requirements for guaranteeing data subjects' consent for collecting and processing data, the procedure for international transfers of data, rights of data subjects, and penalties for non-compliance.



² Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended).

³ [NigeriaDataProtectionRegulation.pdf \(nitda.gov.ng\)](https://nitda.gov.ng/NigeriaDataProtectionRegulation.pdf)

Some Terms and Compliance Requirements Under the NDPR

Data Controllers/Processors: Data controllers are persons or organisations that collect personal data and decide how and what these data will be used for, e.g. Facebook, Banks, Telcos, Twitter, etc. Data processors use, analyse, compute and transfer these data on the instructions of the controllers. Controllers and processors could be the same or different entities. Many fintech companies and other start-ups are both data controllers and processors, e.g. Paystack.

Consent: Before obtaining or processing the data of data subjects, their explicit consent must be sought. The NDPR provides that consent must be specifically obtained freely, clearly, unambiguous without fraud, undue influence, or coercion of the data subject.⁴ Mostly, consent is obtained through clearly and simply drafted privacy policies. Although not the only lawful ground, consent is the most common basis to obtain or process data.

Privacy Policy/Notices: Privacy Policies under the NDPR are clear and unambiguous statements that detail how the controller obtains and processes data, the purpose for collection, the type of information collected, etc.⁵

Data Protection Compliance Organisations (DPCOs) and Data Protection Officers (DPOs):

DPCOs are organisations licensed by NITDA to provide data compliance and auditing services to data controllers. DPCOs ensure their clients are privacy and NDPR-compliant. They also provide data privacy training, advisory services and prepare data protection documents like Data Protection Policies and Privacy Policies.



⁴ Article 1.3, 2.2, and 2.3 of the NDPR 2019.

⁵ Article 2.5 of the NDPR 2019.

DPOs are employed by organisations to create and ensure adequate data protection mechanisms within those organisations and to ensure compliance with data protection regulations. DPO functions can be outsourced to a competent person or firm.

Data Protection Audits: The NDPR mandates all organisations to carry out periodic audits of their data protection processes. Organisations that process the data of more than 1000 data subjects within a six-month period or the data of more than 2000 data subjects within a 12-month period are required to submit their data protection audit reports to the NITDA on or before the 15th of March of every year. Most start-ups fall within this category.

Penalty for Non-Compliance and Breach: Organisations that flout the NDPR or experience a data breach shall be liable to a fine of between 1% and 2% of Annual Gross Revenue of the preceding year or payment of the sum of 2 or 10 million Naira, whichever is greater; (depending on whether the data subjects involved are fewer or more than 10,000 respectively).

Conclusion

If you are a small company, SME or start-up, your reputation is very integral to building investor and consumer trust. Data breaches and lawsuits have adverse effects on your brand. It is therefore important to engage the services of a competent DPCO to provide data compliance and auditing services to your organisation.

Francis Ololuo
ulawteam@uubo.org

Disclaimer

Disclaimer: This article is for general information purposes only, does not constitute legal advice and does not purport to be comprehensive. If you have any questions, require any clarification on how the subject of this article applies to you or your business, or require the services of our U-LAW team, please contact info@u-law.org.

