ADVOCAAT
LAW PRACTICE

OBLIGATIONS OF A DATA CONTROLLER UNDER THE NIGERIA DATA PROTECTION REGULATION 2019:

A REVIEW OF INCORPORATED TRUSTEES OF DIGITAL RIGHTS V. MINISTER OF INDUSTRY, TRADE, AND INVESTMENT & 2 ORS - FHC/AWK/CS/116/2020.

LAGOS | ABUJA

www.advocaat-law.com | Advocaat Law Practice | advocaatlawpractice

INTRODUCTION

The personal data of millions of persons residing in Nigeria are regularly collected, stored and disseminated by government agencies or corporate entities and the collection and use of such data is now governed by the Nigeria Data Protection Regulation 2019 (NDPR). ***Article 1.3 of the NDPR*** defines a data controller as any person or statutory body that ***"determines the purposes for and the manner in which personal data is processed."*** The most important consequence of being a controller is the legal responsibility for complying with the obligations under the NDPR. The NDPR regards the obligations of the data controller as serious and provides that:

a. No limitation clause shall avail any data controller who acts in breach of the principles set out in the NDPR;[1] and

b. Data controllers are liable to pay penalty for breach of the principles set out in the NDPR.[2]

Despite the provisions of the NDPR on the protection of personal data by data controllers, many data controllers do not comply with the NDPR. The non-compliance with the provisions of the NDPR was recently challenged in the case of ***Incorporated Trustees of Digital Rights v. Minister of Industry, Trade and Investment & 2 Ors.***[3] In this case, the Court reiterated that only compliance with the NDPR by all stakeholders, including government agencies, would bring about a true data protection regime in Nigeria.

BRIEF FACTS

The Federal Ministry of Industry, Trade, and Investment set up a Micro, Small and Medium Enterprises (MSME) Survival Funds on an online portal hosted as www.survivalfund.gov.ng and www.survivalfundapplication.com on which personal data of applicants of the survival fund were collected including data such as the names, addresses, telephone numbers and Bank Verification Number (BVN) of the applicants. The Incorporated Trustees of Digital Rights (the Applicant) alleged that one of its members sought to apply for the survival fund and discovered that the process of collection and processing of these personal data were done in contravention of and without regard to the duties and obligations of data controllers under the NDPR.

In particular, the Applicant alleged that a.) the 1st Respondent did not publish its privacy notice as required by ***Article 2.5 of the NDPR***; b.) the 1st Respondent did not appoint a Data Protection Officer for the portal; c.) the 1st Respondent did not adopt security measures to protect the personal data collected on the portal.

The Applicant commenced this action at the Federal High Court against the 1st Respondent for the violation of the requirements of ***Article 1.1(a), 2.2 and 2.3 of the NDPR.*** In determining this case, the Federal High Court formulated a sole issue for determination thus: ***"Whether or not from the circumstances of this present case, the Respondent had failed to comply with the Nigeria Data Protection Regulation, 2019, resulting in the likely infringement of the Applicant's member's right to private and family life provided for in Section 37 of the Constitution of the Federal Republic of Nigeria as amended."*** The Court held that the 1st Respondent breached the provisions of the NDPR.

[1] **See Article 2.5(j) of the NDPR**
[2] **Article 2.10 of the NDPR**
[3] **FHC/AWK/CS/116/2020**

BASIS OF THE COURT'S DECISION

In resolving the issue for determination, the Court relied on ***Articles 1.1(a), 2.2, 2.3, and 3.1 of the NDPR*** as well as the interpretation of ***Section 37 of the 1999 Constitution of the Federal Republic of Nigeria, 1999 (as amended).*** These principal provisions imposed obligations on anyone or organization responsible for collecting personal data of Nigerian residents. In defining who a data controller is, the Court relied on the definition in ***Article 1.3(x) of the NDPR***, which provides that a data controller "***means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and how Personal Data is processed or is to be processed.***"

The Court further held that since the 1st Respondent was responsible for determining the purpose and manner in which the personal data submitted on the online Survival Fund portal were to be processed, the 1st Respondent is a data controller within the meaning of the NDPR and therefore under the obligation to comply with the duties and obligations imposed on data controllers by the NDPR in ***Articles 1.1(a); 2.1(d); 2.5; 2.6; and 3.1(7) (a) and (b) of the NDPR***. These provisions sum up the responsibilities of a data controller, which are summarized below:

1. ***To safeguard the rights of natural persons to data privacy.***
2. ***Secure personal data against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire, or exposure to other natural elements.***
3. ***To display a simple and conspicuous privacy policy that the class of data subject being targeted can understand.***
4. ***To develop security measures to protect data. Such measures include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specifically authorized individuals, employing data encryption technologies, developing organizational policy for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.***
5. ***To provide their identities and contact details as controllers and the contact details of the Data Protection Officer.***

According to the Court, the 1st Respondent was unable to show its compliance with the above obligations of the data controllers and therefore held that the failure of the 1st Respondent to adopt security measures towards protecting the data privacy of the citizens, taking into account the vital information required from the data subject such as BVN, names, addresses, and phone numbers, posed a threat to the right to family and private life of the data subjects and

contravened the provisions and objectives of the NDPR.

The Court used the opportunity to strengthen the importance of compliance with the obligations and duties imposed by statutes and regulations and held that ***"When there is a statute or regulation stipulating the manner that a thing or act is to be done or carried out, such legislation must be complied with strictly, otherwise such legislation becomes cosmetic."***

COMMENTARY

Corporate organisations as data controllers must take heed of the requirements of NDPR to insulate themselves from laws suits as citizens and interested non-government organisations are now litigating to seek enforcement of their rights under the NDPR. Given the pervasive nonchalance around the collection and use of personal date, we envisage more lawsuits seeking redress for data privacy breaches by non-complying data controllers. Hopefully, the National Information Technology Development Agency will continue with the implementation of the provisions of the NDPR and strengthen the enforcement procedures under same.

CONTACT

JACOB FAMODIMU
jacob.famodimu@advocaat-law.com

LAZARUS KALU
lazarus.kalu@advocaat-law.com

TOBILOBA BANKOLE
tobiloba.bankole@advocaat-law.com