WHY CBN'S DIRECTIVE TO FIs TO OBTAIN THE SOCIAL MEDIA HANDLE OF CUSTOMERS POTENTIALLY VIOLATES THE DATA PROTECTION ACT

Why CBN's Directive to FIs to Obtain the Social Media Handle of Customers Potentially Violates the Data Protection Act

Chukwuyere Ebere Izuogu

On 31 May 2023, the Governor of the Central Bank of Nigeria (CBN) in exercising powers granted under the Banks and Other Financial Institutions Act 2020 (the Act) issued the Central Bank of Nigeria (Customer Due Diligence) Regulations 2023 (the CDD Regulations). One of the objectives of the Regulations is to provide additional customer due diligence (CDD) measures to enable Financial Institutions (FIs) to comply with the Money Laundering (Prevention and Prohibition) Act 2022, Terrorism (Prevention and Prohibition) Act 2022, CBN (Anti-Money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction in Financial Institutions) Regulations 2022 and international best practices.

The CDD Regulations require FIs to among other things, obtain the social media handle of customers for the purpose of identification. In this article, I argue why this requirement imposed on FIs by the CDD Regulations potentially violates the Data Protection Act 2023 (DPA).

What exactly is customer due diligence

According to the CBN Guidance Note on Anti-Money Laundering and Combatting the Financing of Terrorism for Other Financial Institutions 2022 (the Guidance Note), CDD 'involves customer identification, information gathering, and monitoring'. Under the CDD Regulations, FIs are required by regulation 5 (1) to carry out CDD in the following circumstances: when business relationships are established; when carrying out transactions above the CBN designated threshold; carrying out occasional transactions that are wire transfers; when there is suspicion of money laundering, terrorist financing, proliferation financing; or when there are doubts as to the veracity or adequacy of previously obtained customer identification data.

Among other things, the CDD measures to be implemented by a FI must include the means for customer identification and verification of customer identity. Customer for the purpose of this article refers to only natural persons that are customers of a FI, thus one of the key elements of CDD is customer identification and verification through credible evidence such as original and valid identification issued by government agencies.

Are social media handles personal data

As an initial matter, the DPA is triggered every time personal data is processed. The simple act of collecting, storing or retrieving personal data constitutes a data processing operation. Personal data on the other hand is defined by the DPA as:

> any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual.

Online identifier as used in this definition is a phrase borrowed from the General Data Protection Regulations (GDPR) regulating data protection in the European Union. Recital 30 of the GDPR clarifies that '[n]atural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags'. According to the Information Commissioner's Office (ICO), the data protection authority in the United Kingdom, social media handles may be personal data because their use may leave traces which, when combined with unique identifiers and other information received by servers, may be used to create profiles of individuals and identify them.

For illustration, the ICO explains that:

> An individual's social media 'handle' or username, which may seem anonymous or nonsensical, is still sufficient to identify them as it uniquely identifies that individual. The username is personal data if it distinguishes one individual from another regardless of whether it is possible to link the 'online' identity with a 'real world' named individual.

Having established that social media handles are indeed personal data, I now turn to how their collection by FIs as part of CDD measures is violatory of the DPA.

Excessive personal data collection is contrary to the principles of personal data processing

Under the DPA, one of the principles of data personal data protection provided in section 24 (1) (c) is to ensure that the personal data processed is 'adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed'. This principle is otherwise referred to as data minimisation under the GDPR and in most jurisdictions with a data protection framework. This principle (and others provided for in section 24 of the DPA) must be complied with whenever personal data is processed irrespective of the lawful base, unless such data processing operation is exempt from the application of the DPA.

Data minimisation means that data controllers and processors must only collect and process personal data that is directly relevant to the specific purpose pursued by the processing operation. Thus, data controllers and processors must ensure not to obtain more personal data than is necessary from the data subject (in this case the customers) in relation to the purpose the data processing operation seeks to accomplish. Under the CDD Regulations, the purpose of collecting personal data from customers by FIs is for identification and verification of the customer's identity.

For the purpose of identifying customers, regulation 6 (a) of the CDD Regulations requires FIs to in addition to collecting the social media handles of customers, also collect the following types of personal data: legal name; permanent address (full physical address); residential address (where the customer can be located); telephone number; e-mail address; Bank

Verification Number (BVN); Tax Identification Number (TIN); and an official personal identification number or other unique identifier contained in an unexpired document issued by a government agency, that bears a name, photograph and signature of the customer such as a passport, national identification card, residence permit, social security records or drivers' license.

While these personal data are required to be collected by FIs to enable the proper identification of customers, it is respectfully submitted that they are excessive in relation to the purpose of the processing operation and potentially violate the data minimisation principle in the DPA. As a matter of fact, only the BVN, TIN and/or official unexpired identity document issued by a government agency is required to properly identify the customer, anything more than this would be excessive data processing. In terms of verifying such official documents when provided by customers, the principle of regularity may be relied upon absent any compelling evidence challenging the validity of these documents. Thus, it goes without saying that data collection in this case is excessive and therefore unnecessary in light of the purpose of the collection since a customer's identification and verification can easily be accomplished by excluding certain other types of personal data mentioned in the CDD Regulations.

Conversely speaking, another question is whether a FI has the technological means to verify a customer's identity through a social media account. While another third party may be able to do so, this is unlikely to be the case for FIs considering the technical resources available to them. It is also unlikely that such a third party would be willing to disclose the identity of an individual associated with a social media account, at the request of the FI in the absence of proper authorisation under the applicable law or data protection legislation. In other words, social media handles serve no customer identification purpose as they cannot enable a FI to ascertain the identity of the individual behind that social media account.

When assessing what personal data may be collected to accomplish the purpose pursued by the processing operation, data controllers and processors are also minded to consider the adverse impact of the means of processing as well as verifying whether an alternative or less intrusive means of processing is available and has fewer adverse effects on the data subject. While the collection of social media handles may seem reasonable to the CBN, it does pose a significant privacy risk since social media handles are now considered to be an extension of the private sphere of an individual. And any processing in this regard would be deemed to be quite invasive. An example of this is when the Agencia Española de Protección de Datos (AEPD), the Spanish data protection authority, in an administrative determination ruled that the use of biometric data (fingerprints in this case) for access control by students on the premises was excessive when a less intrusive alternative like the use of identity cards would have served the same purpose.

In addition, legitimate concern exists that the disclosure of social media handles pursuant to the CDD Regulations could have a chilling effect on social media use by interfering with freedom of expression, especially if that social media handle is active and/or has a massive followership. This chilling effect is a significant impediment to the fundamental rights and freedom of the data subject which the DPA seeks to safeguard in section 1(a). As I have stated elsewhere, the necessity of the personal data collected

and its proportionality in relation to the purpose pursued by the processing operation must be taken into consideration by a data controller in its assessment of what personal data may be collected.

Conclusion

While the extant Nigerian Data Protection Regulations 2019 (NDPR) issued by National Information Technology Development Agency (NITDA) which predates the DPA saw minimal enforcement, probably due to stakeholders' concerns questioning its legal basis. The DPA on the other hand is an Act of the legislature that derives legitimacy from the constitutional power of the National Assembly to make laws. On this basis, it becomes pertinent to mention that where a conflict exists between an Act of the National Assembly such as the DPA and a subsidiary legislation such as the CCD Regulations, the law is that a subsidiary legislation cannot over-rule the law, see *Akanni v. Odejide* (2004) All FWLR pt. 218 pg. 827 at 853; *Kennedy v. INEC* (2009) 1 N.W.L.R (Pt. 1123). Thus, the aspect of the CCD Regulations that infringes the data minimisation principle of the DPA can be declared null and void if challenged in court.

In any case, identity verification is a delicate matter that essentially involves the disclosure and dissemination of personal data which in turn triggers the DPA. While note should be taken that the main argument made in this article is that collecting social media handles in accordance with the CDD Regulations serves no customer identification and/or verification purposes and as such violates the data processing principle of data minimisation under the DPA. However, no assumption should be made that other requirements in the CDD Regulations do not implicate other provisions of the DPA such as purpose specification, lawful bases, transparency and information provisions and the obligation to conduct a data privacy impact assessment, the extent of which can only be determined after a comprehensive data protection analysis of the CDD measures to be implemented by FIs.

It, therefore, becomes important for organisations that regularly process personal data and/or implement identity verification processes to ensure compliance with the DPA in every aspect. As of the time of this writing, there has also been a public uproar against the collection of social media handles by FIs in compliance with the CDD Regulations. In particular, the Socio-Economic Rights and Accountability Project (SERAP), a civil society organisation that regularly engages in public interest litigations has written to the CBN asking it to 'immediately delete the patently unlawful provisions in the Central Bank of Nigeria (Customer Due Diligence) Regulations directing banks to obtain information on customers' social media handles for the purpose of identification'. It would be interesting to see the final conclusion of this matter and whether this would be the first test of the enforcement bite of the DPA to protect the rights and freedoms of data subjects in Nigeria.

Contact person for this article
Chukwuyere Izuogu, LL.M (Hannover), CIPP/E
chukwuyere@sskohn.com

WHY CBN'S DIRECTIVE TO FIs TO OBTAIN THE SOCIAL MEDIA HANDLE OF CUSTOMERS POTENTIALLY VIOLATES THE DATA PROTECTION ACT

STREAMSOWERS & KÖHN is a leading commercial law firm providing legal advisory and advocacy services from its offices in Lagos, Abuja, and Port Harcourt. The firm has extensive experience in acting for Nigerian and international companies, government, and industry regulators in the firm's various areas of practice.

Contact us at:
16D Akin Olugbade Street
(Off Adeola Odeku Street)
Victoria Island, Lagos
Tel: +234 1 271 2276; **Fax:** +234 1 271 2277
Email: info@sskohn.com; **Website:** www.sskohn.com