Privacy Please – Digital Age of Consent for Children – Series 6

Introduction

The pervasiveness and the allure of the internet continues to hold sway and wax stronger amongst different age groups, more so with the younger generation. A huge outcome of this, is the readiness of a number of users in sharing their personal data on various platforms. One of the rising challenges amidst all this, is children's data, studies have shown that more than 83% of children will have regular access to a smartphone in their pre- and early teens. Business organizations unknowingly sometimes are therefore exposed to processing the data of a child for several purposes, whether commercial or administrative. In view of this, it is important that the right privacy principles are adopted when dealing with child data. This instalment of our Privacy Please series will examine the provisions relating to the protection of child data under Nigerian law and offer guidance to business organisations.

Processing Personal Data of a Child

Prior to the enactment of the Nigeria Data Protection Act (NDPA) 2023, the processing of the personal data of a child was primarily regulated by the Nigeria Data Protection Regulation (NDPR) and its Implementation Framework. For the purposes of the NDPR, a child was categorized as a person below 13 years of age. Data controllers or processors whose processing activity targeted children were required to ensure that their privacy policy is made in a child-friendly form with the aim of making children and their guardians have a clear understanding of the data processing activity before granting consent. Under the NDPR, information relating to a child is to be provided in writing or by other means, including electronic means where appropriate.

However, the NDPA has established a new regime with respect to the processing of personal data belonging to a child and persons lacking legal capacity.

Age - The NDPA increases the age requirement for data protection purposes[1]. A child is now **considered as any person below 18 years of age**[2] a significant increase from the provisions of the NDPR highlighted above

Consent - Whilst the NDPR and its Implementation Framework were silent on whom to obtain consent from, the NDPA explicitly states that a data controller shall obtain the consent of the parent or legal guardian, as applicable. However, this consent will not be required where:

a) It is necessary to protect the vital interests of the child or person lacking the legal capacity to consent;
b) It is carried out for purposes of education, medical, or social care, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality; or
c) It is necessary for proceedings before a court relating to the individual.

Protection - The NDPA provides an additional layer of responsibility on data controllers as it requires them to apply appropriate mechanisms to verify age and consent, taking into consideration available technology. For this purpose, presentation of any government-approved identification document is deemed as an appropriate mechanism.

Finally, the NDPA authorizes the Nigeria Data Protection Commission (NDPC) to make regulations for the protection of children that are **13 years** and above in relation to the provision of information and services by electronic means at the specific request of the child. This means that we should expect specific guidelines from the regulators specifically as it relates to the processing of data from children in the aforementioned age group (13 years and above but below 18) via the internet and other electronic means.

The above provisions clearly show that the NDPA has given significant attention to the processing of child data. It goes further to state *that nothing within the Act shall be construed as authorising data processing in respect of a child in a manner that is inconsistent with the provisions of the Child's Right Act.*

[1] Section 65 of the NDPA
[2] Section 277 Childs Rights Act 2003

Key Considerations for Business

Processing the personal data of a child is a very sensitive issue. In view of the provisions of the NDPA there are a few considerations that businesses must pay attention to, some of which include:

A. **Develop Best Practices**: Business organizations must develop data privacy best practices that illustrates how it intends to obtain consent from the parent or legal guardian of a child or person lacking capacity. This may include revising your terms and conditions or privacy policies to specifically highlight your approach to children's data in line with the NDPA. It is also pertinent that this type of information is easy to read and understand by all age groups.

B. **Age and Consent Verification Technology:** Data Controllers and processors often indicate that they have no way of ascertaining when they are processing personal data belonging to a child. However, the NDPA has now mandated them to employ available technology to ensure verifications. Businesses must ensure that their IT set up is such that the right technology is being deployed for the purpose of verifying a person's age. An easy way to start is to adopt the recommended government ID mechanism referred to above. Businesses may also engage with the NDPC to ascertain if there are any other recommended age and consent verification technology that it needs to adopt.

C. **Application of Child Right Act**: Businesses would also need to be mindful of the data privacy concerns under the Child Right Act in developing their practices around the dealings involving processing children's data.

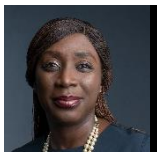
D. **New/Special Regime for Data Processing for Children Age Below 13 Years**: Businesses are encouraged to pay close attention to the regulators especially in view of any upcoming regulations that may be applicable to the processing of personal data of children aged 13 and above via online products.

Conclusion

The protection of personal data belonging to a child during processing is a salient point for any business organizations. According to the United Nations International Children's Emergency Fund (UNICEF), there is widespread belief that standards of data protection and security concerning children should be set at a higher level, but currently, there is no agreed global data governance framework addressing key concerns related to children's data. Businesses must ensure that they pay attention to the provisions of the NDPA and also adopt available international best practices when processing child data.

Aluko & Oyebode is a registered Data Protection Compliance Organisation (DCPO), and we are able to assist organisations facilitate their data protection compliance plans in line with the prevailing practices.

Contact Details



Sumbo Akintola
Partner

M +234 803 403 5122
E Sumbo.Akintola@aluko-oyebode.com

Emmanuel Ido
Associate

M +234 916 834 4310
E Emmanuel.Ido@aluko-oyebode.com