TEMPLARS

CONSENT AS A BASIS FOR PROCESSING PERSONAL DATA OF DATA SUBJECTS IN NIGERIA: THE KEY ISSUES

Introduction

The exponential growth in Information, Communication, Technology, E-commerce and Social Media in recent times, has resulted in an extraordinary demand for the personal data of data subjects across the globe. From an economic perspective, it has been submitted that personal data has become the new oil, based on its rapidly increasing value in the global digital economy. Resultantly, the need to properly regulate the processing of personal data has attracted unprecedented attention nationally and internationally.

As the world continues to strengthen the regulation of personal data privacy and personal data processing, Nigeria, through the National Information Technology Development Agency (NITDA), issued her latest Data Protection Regulation in 2019 (the "Regulation"). The Regulation, among other considerations, prescribes consent as one of the primary bases for processing of personal data of Nigerian citizens, both within and outside the country.

Key Contacts

Sadiku Ilegieuno
Partner
sadiku.ilegieuno@templars-law.com

Kazeem Lawal
Associate
lawal.kazeem@templars-law.com

Akinyemi Akinniyi
Associate
akinyemi.akinniyi@templars-law.com

While the Regulation, (although, a subsidiary legislation), was a very timely legislative response to issues relating to the personal data of Nigerian citizens, it is important to note that the provision of the Regulation on the consent requirements seems patchy and inexhaustive. This is because, in our view, it merely provides general prescriptions on what should be, without addressing the specific and key issues which underpin consent as a concept. That being the case, the objective of protecting the personal data of data subjects from unlawful processing, which is the core of the Regulation, becomes more or less, ineffective.

This article considers the concept of consent as a basis for data processing, as well as the fundamental issues which underpin consent under the Regulation. In doing so, the meaning of consent as a key determinant for processing of the personal data of data subjects and the exceptions to the consent requirement will be considered. Further and more significantly, the article will also consider issues around consent in relation to a child within the context of data processing. The article also examines some subtle methods, such as the adoption of take it or leave it approach by data controllers in obtaining consent.

The consent requirement

The governing rule under the Regulation is that personal data of a data subject must be processed[3] primarily with the consent of the data subject and in accordance with the specific, legitimate and lawful purpose consented to by the data subject[4].

But the question is: what is consent? Generally, consent is a voluntary yielding to what another proposes or desires; agreement, approval, or permission regarding some act or purpose, especially given by a competent person; legally effective.[5] Under the Regulation, consent is described as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[6]. In essence, the grant of consent involves a contractual, voluntary agreement between the data processor and the data subject.

It is also important to note from the above description of consent that the person or data subject giving the consent must be such that is capable of giving consent so that if a data subject is under any form of legal disability, any consent purportedly obtained may not qualify as consent in reality. Furthermore, prior to obtaining the required consent, the data processor is required to inform the data subject of his or her right regarding the data sought to be processed, the specific purpose for which the data is required, as well as the method for withdrawing the consent at any given time[7].

Nonetheless, it must be borne in mind that the fact that a data subject's consent has been obtained, does not automatically make data processing lawful or justified. This is because the controlling factor is the purpose or motive for which the data is to be processed. Thus, consent cannot be sought, given or obtained in circumstances where the processing of personal data may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts[8]. This prohibition accords with the principle or rule of law that parties cannot contract to do that which is contrary to law or public policy. Any such contract, if at all executed, cannot and will not give rise to an enforceable right at law[9].

It should also be noted that the requirement for consent as a basis for processing personal data of data subjects has qualifications and exceptions. In other words, the concept of consent of the data subject is not the only legally recognized basis for processing personal data of data subjects. This is because of the recognition that in some instances or situations, it may be difficult, if not impossible, to obtain the needed consent. A good example is the case of the web search engines. Considering their automated nature, the volume of personal data processed and the speed at which they process such data, it would be a tough sell if the law, such as the Regulation under review, were to require that search engine operators or owners first obtain the consent of the relevant data subjects before searches are conducted through the search engines.

Perhaps, it is in realising the above challenge, that the draftsmen or makers of the Regulation, apart from the consent requirement, provided for other lawful bases for the processing of personal data, namely: where processing is necessary (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; (ii) for compliance with legal obligation by the data controller; (iii) in order to protect the vital interest of the data subject or another person; and (iv) for the performance of a task carried out in the interest or in exercise of official public mandate vested in the data controller[10].

As previously mentioned, the focus of this article is consent as a primary basis for data processing, as such, we will not explore these other considerations for processing data.

---

[4]The Data Protection Regulation, 2019 (the "Regulation") paragraphs 2.1 (a) and 2.2 (a).
[5]Black's Law Dictionary, 11 Ed., page 380.
[6]paragraph 1.3 of the Regulation.
[6]Paragraph 2.3 (1) & (2) (c) of the Regulation.
[8]Paragraph 2.4 of the Regulation.
[9]S.D.C. Cementation (Nigeria) Ltd & Anor v Nagel& Company Ltd & Anor (2003) LPELR-9167 (CA).

The concept of consent as a rule for data processing seems straight forward, however, its practical application within the context of children as data subjects, raises some fundamental questions. Such questions include: (i) determining who a child is for the purpose of consent; (ii) whether a child can validly give consent for the purpose of data processing; (iii) whether the consent of a child may be given by proxy for the purpose of data processing under the Regulation or how can a child validly give consent for the purpose of data processing; and (iv) whether consent obtained by subtle coercion may be said to be valid.

Who is a child for the purpose of consent?

A child undoubtedly qualifies as a data subject under paragraph 1.3 of the Regulation, which defines a data subject as any person who can be identified either directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. Surprisingly, while the Regulation imposes an obligation on a data controller to demonstrate that a data subject has the capacity to give consent[11] prior to the processing of his or her personal data, it is however silent on those who, like children, may not be able to give consent on their own. The Regulation also does not give any indication regarding who will qualify as a child and whether a child will have the capacity to give consent, and if so, in what circumstances.

It is the view of the authors that since the grant of consent for data processing presupposes an agreement or some sort of contractual arrangement, the general rule regarding the contracting age in Nigeria may be a helpful basis for determining the age of contractual consent. That said, we note that under Nigerian law, a child can either be a person below the age of 18 or 21 years, depending on the applicable legal regime that operates in the particular State. In States where the Child Rights Act has been adopted[12], a child is a person under the age of 18 years and to be able to contract and thus give consent, the child must be at least 18 years and above. However, for States that are yet to adopt the Child Rights Act as part of their body of laws, and in which case, the common law[14] still holds sway[15] , a child is a person below the age of 21 years[16]. Thus, for such States, to be able to contract and thus give consent, the data subject must be above 21 years.

The implication of the above legal limitation on the ages of data subjects is that, until a data subject is above 18 years or 21 years depending on where they are, such a data subject may not be able to validly give consent for the processing of his or her data.

Even so, it is important to note that these age stipulations may be far from the 21st century realities in which 14-year-olds (and younger) already understand the workings of the information and communication technology better than some adults, and thus, arguably, possess a better understanding of the dynamics of data processing.

It is, therefore, not a surprise that the Data Protection Bill, 2020 (the "**Bill**") defines sensitive data to include the personal data of a child who is under the age of 16 years[17]. Although, this innovation of the Bill is not a clear stipulation of the age of contractual consent, it however demonstrates the new legislative thinking in Nigeria regarding the need to adopt a liberal approach to the contracting age of a child and which is completely in accord with the reality of the digital age. It is hoped that when the Bill is finally passed into law, 16 years would be adopted as the age of contractual consent for data processing of the personal data of data subjects in Nigeria.

[10] Paragraph 2.2 (b-e) of the Regulation.
[11] Paragraph 2.3 (2)(a) of the Regulation.

How can a child validly give consent for the purpose of data processing?

Next, we consider: Can a child validly give consent for the processing of his or her data? Unfortunately, the Regulation is equally silent on the procedure for obtaining the consent of a child before the processing of his or her data. It is the opinion of the authors that this is a serious omission in the Regulation.

Fortunately, this omission seems to have come to the attention of the relevant Nigerian Authorities as this issue appears to have been equally dealt with or considered in the Bill, which aims to fill this obvious gap in the law. Thus, a provision in the Bill generally seeks to prohibit the processing of personal data which relates to a child who is under parental guidance or control unless the prior consent of the parent or guardian is obtained. Simply put, a child cannot validly give direct consent for data processing, but indirectly through his or her parent or guardian.

Away from the above theoretical prescriptions, it must be acknowledged that it is practically difficult for parents to be available at every conceivable time to give consent to the processing of their children's personal data. For instance, online consent request and approval more often than not requires a data subject to instantly approve or reject the data controller's privacy policy which has the consent request embedded in it. A potential, albeit difficult to implement, solution could be to require a data controller to directly request consent from the parent or guardian by mandating the child to supply his or her parent's email address or phone number at the time consent is required to be given. The request for consent is then routed to the concerned parent or guardian who approves it regardless of his or her location. That way, the challenges associated with having to always wait for a parent or guardian for their consent on behalf of the child or ward will be significantly reduced.

The take it or leave it approach of data controllers

As seen above, a key component of a valid consent under the Regulation is that it must be freely given and devoid of any undue influence or coercion. This is apparent in paragraph 1.3 of the Regulation, which, as already mentioned above, defines consent to mean "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". Further, paragraph 2.3 (2) of the Regulation obligates a data controller to ensure that consent is obtained without fraud, coercion or undue influence.

Realistically speaking, however, individuals do not really have a plausible choice when given a consent request and are left with a non-negotiable 'take it or leave it' scenario, which in our view amounts to nothing but subtle coercion or coercion in disguise, and which does not amount to consent.

The reason for this is apparent. Most internet-based service providers make the grant/approval of consent request a pre-condition for accessing their services. Thus, when a data subject declines consent, he or she is exposed to the inevitable consequence of being denied access to the internet-based services of the service provider. The reality of the 21st century and the exceptional circumstances foisted on humanity by Covid-19 triggered the migration of most activities online. Taking advantage of this exponential growth in online activities, virtually all internet-based service providers now engage in subtle coercion thus aggravating the problem.

---

[12]These includes Lagos, Ondo, Ekiti, Osun, Rivers States, etc. See Child Rights Act Tracker, "States that have Passed the Child's Right Law in Nigeria" <www.partnersnigeria.org/childs-rights-law-tracker/> accessed 17 March 2021.
[13]Child Rights Act 2003, section 277.
[14]It is instructive to note that, most often than note, reference is wrongly made to the Infant Reliefs Act 1874, which is a Statute of General Application, as the statutory basis for the common rule on the definition of a child. Infant Reliefs Act contains no such stipulations, rather it merely void contracts made with a child, except for necessaries. Besides, in the United Kingdom, the Family Reform Act 1969 has reduced the age of majority to 18 years. Regardless, the common law rule continues to apply in Nigeria in view of the cut-off date of 1st January 1900 for the application of Statutes of General Application.
[15]These are Bauchi, Yobe, Kano, Sokoto, Adamawa, Borno, Zamfara, Gombe, Kastina, Kebbi and Jigawa States. See Nike Adebowale, "Updated: 11 States in Northern Nigeria yet to pass the Child Rights
[16]The applicability of this Common Law rule was confirmed by the Full Court, the equivalent of the present-day Supreme Court in Labinjoh v. Abake (1924) 5 N.L.R 33. Law-UNICEF Official" Premium Times (11 May 2019) < www.premiumtimesng.com/news/more-news/329511-12-states-in-northern-nigeria-yet-to-pass-child-rights-law-unicef-official.html> accessed 17 March 2021.
[17]Section 66 of the Data Protection Bill, 2019.
[18]Section 26 (1) & (2) of the Bill.
[19]Schermer, Custers & Van der Hof, Ethics Inf Technol 2014/16, p. 177-178.

Although, paragraph 2.3(2)(c) of the Regulation provides that when assessing whether consent was freely given or not, utmost account shall be taken to see if the performance of contract or the provision of services is conditional on consent to the processing of personal data that is not necessary (or excessive), it does not contain express provision which prevents internet-based service providers from denying data subject access to their services for the failure to give consent. Thus, a valid argument could be made that the Regulation tacitly permits subtle coercion. This runs counter to the clear objective of the Regulation, which is to ensure that consent is freely given without fraud, coercion or undue influence.

Although, paragraph 2.3(2)(c) of the Regulation provides that when assessing whether consent was freely given or not, utmost account shall be taken to see if the performance of contract or the provision of services is conditional on consent to the processing of personal data that is not necessary (or excessive), it does not contain express provision which prevents internet-based service providers from denying data subject access to their services for the failure to give consent. Thus, a valid argument could be made that the Regulation tacitly permits subtle coercion. This runs counter to the clear objective of the Regulation, which is to ensure that consent is freely given without fraud, coercion or undue influence.

Therefore, to ensure that data subjects are neither unduly pressured into granting consents for the processing of their personal data, nor denied essential internet-based services for declining consents, it is imperative for legislative or regulatory interventions to prohibit or minimise the take it or leave it approach currently being adopted by some data controllers and replace it with a more flexible and balanced approach. For instance, the Regulation could introduce a "limited access" regime, which will entitle data subjects to only have limited access to internet-based services in the event of failure to grant consent.

Conclusion

We have discussed the concept of consent as a basis for processing personal data and some practical issues associated with the concept of consent including: the determination of the age of contractual consent; how a child can validly give consent; and the take it or leave it approach of data controllers.

We have recommended some steps that could make complying with consent requirements in the context of data processing more effective. It is hoped that the law makers will find these recommendations useful and take them on board in their consideration of the Bill before it is passed into law. This is to ensure that the ultimate goal of safeguarding the right of persons to data privacy in a more robust fashion in Nigeria.