DATA PROTECTION LAW AND/OR AN INDEPENDENT DPA ARE PREREQUISITES FOR A POSITIVE ADEQUACY DECISION IN NIGERIA: A REVIEW OF IKIGAI V. NITDA

Data Protection Law and/or an Independent DPA are Prerequisites for a Positive Adequacy Decision in Nigeria: A Review of Ikigai V. NITDA

Chukwuyere Ebere Izuogu

Introduction

On 28 November 2023, the Federal High Court (the Court) delivered its judgment in the case of Ikigai v National Information Technology Development Agency Suit No. FHC/ABJ/CS/1246/2022. The Plaintiff, Ikigai, a non-profit organisation, requested the Court to interpret the provisions of the Nigerian Data Protection Regulations 2019 (NDPR) and the Nigerian Data Protection Regulations 2019: Implementation Framework (Implementation Framework) concerning international data transfers.

In this article, I analyse this case and discuss its possible ramifications for international data transfers from Nigeria and the criteria to be used when assessing the adequacy of the level of protection of personal data in a third country.

Why adequacy assessment

Personal data is a critical input in the global digital economy and its international transfer is essential for the provision of various services and benefits to individuals. However, such transfers also pose significant challenges and risks for the protection of personal data and the rights of data subjects, especially when the data is intended to be processed in countries that have different or lower standards of data protection than the country of origin. Consequently, international data transfers are subject to rigorous oversight by privacy regulators and Data Protection Authorities (DPAs) due to these privacy risks. An example of this scrutiny is the decision of the Court of Justice of the European Union (CJEU) in CJEU Case C-311/18 *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, which invalidated the European Commission's Privacy Shield Decision, the international data transfer framework between the US and EU, due to the invasive nature of US surveillance programmes, thus rendering transfers of personal data based on the Privacy Shield Decision unlawful.

Adequacy assessment is a mechanism to ensure that international data transfers are conducted in a way that respects the privacy and security of personal data and the fundamental rights and freedoms of data subjects. It involves the evaluation of the level of data protection in a third country by a DPA, to determine whether it is comparable to the level of data protection provided in the country of origin. If a third country is deemed to have an adequate level of data protection, data can be transferred to that country without any additional safeguards or authorisations. This simplifies international data transfers and reduces the

administrative and legal burden for the data exporters and importers.

Adequacy assessment is important for several reasons. First, it promotes the harmonisation and convergence of data protection standards and practices across different jurisdictions, which can enhance the trust and cooperation among DPAs, consumers and other stakeholders. Second, it eliminates digital trade restrictions to the free flow of data in cross-border business transactions, which can benefit the economy and society. Third, it safeguards the rights and interests of data subjects, who can enjoy the same level of data protection regardless of where their data is transferred or processed.

However, adequacy assessment is beset with some challenges and limitations. For example, it requires a comprehensive and rigorous analysis of the legal and institutional framework, the enforcement and oversight mechanisms, and the international commitments and obligations of the third country. In some cases, it requires continuous monitoring and review of the adequacy decision, which can be revoked or suspended if the level of data protection in the third country changes or deteriorates. Moreover, it may be affected by political and diplomatic factors, as well as by judicial interpretations and decisions, such as the judgement under review in this article and the EU case of *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (supra).

Legal framework for international data transfers under the NDPR and Implementation Framework

Under the NDPR, there are, in principle, two ways in which the transfer of personal data to third countries or international organisations is permissible. International transfers of personal data may take place on the basis of: an adequacy decision (art. 2.11); or, in the absence of such an adequacy decision, where an exemption applies (art. 2.12). Under the Implementation Framework, Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) are introduced under art. 7.3 as an international data transfer mechanism where an organisation seeks to transfer personal data to another entity within its group of companies or an affiliate company.

According to art. 2.11 a) of the NDPR, the Attorney General of the Federation (AGF) supervises the transfers of personal data from Nigeria to a third country or an international organisation, which can only take place if the National Information Technology Development Agency (the Agency or NITDA) determines that the third country ensures an adequate level of protection for the personal data. The Agency has not yet defined what constitutes an 'adequate level of protection' for personal data. However, when evaluating the adequacy of protection, art. 2.11 b) of the NDPR requires the AGF to take into account the legal system of the third country, particularly in relation to rule of law, human rights and fundamental freedoms, relevant legislation in various areas, such as public security, defence, national security and criminal law, and the access of public authorities to personal data.

Additionally, art. 2.11 c) – e) of the NDPR requires the AGF and/or the Agency to consider other matters, such as: the implementation of the legislation, data protection rules, professional rules and security measures, including the rules for the onward transfer of personal data to another country (or recipient); the case-law, the effective and enforceable data subject rights and the effective administrative and judicial redress for the data subjects whose personal data are transferred; the existence and effective functioning of one or more independent supervisory authorities in the

third country or organisation, with the responsibility for ensuring and enforcing compliance with the data protection rules, assisting and advising the data subjects in exercising their rights and cooperating with the relevant authorities in Nigeria; and the international commitments or obligations of the third country or organisation arising from legally binding conventions or instruments or from its participation in multilateral or regional systems, particularly in relation to the protection of personal data.

In transferring personal data abroad, art. 7.1 of the Implementation Framework stipulates that the following information is required: the list of countries where the personal data of Nigerian citizens and residents is transferred in the regular course of business; the data protection laws and the relevant data protection office/administration of those countries; the NDPR-compliant privacy policy of the data controller; an overview of the encryption method and data security standards; and any other detail that ensures the adequate protection of the privacy of personal data in the target country. Art. 7.2 also states that the Agency shall coordinate transfer requests with the AGF. To implement this provision, a positive adequacy decision in the form of a White List containing a list of countries that provide an adequate level of protection for personal data was established in Annexure C to the Implementation Framework. If the international data transfer is to a third country that is not on the White List, the data controller must ensure the lawfulness of such transfers, either by obtaining the consent of the data subjects or by relying on one of the exceptions provided in art. 2.12 of the NDPR. After the Agency determines that a third country provides an adequate level of protection for personal data, the transfer of personal data from Nigeria to that country becomes lawful and unrestricted.

Facts of Ikigai v NITDA and the decision of the Court

Ikigai filed a lawsuit against the Agency on 28 July 2022, seeking the interpretation of several provisions of the NDPR and Implementation Framework pertaining to international data transfers. One of the questions that the Plaintiff raised for the determination of the Court was whether the Agency, as the Defendant, was subject to the NDPR and Implementation Framework with respect to the international transfers of personal data from Nigeria to a third country and whether the NDPR and Implementation Framework mandated the Agency to grant a positive adequacy decision in the White List to only to countries that ensured an adequate level of protection for the personal data. On this basis, the Plaintiff among other reliefs, sought a declaration from the Court that Algeria, Comoros, Guinea Bissau, India, Mauritania, Mozambique, Sierra Leone, Togo and Zambia, which were included in the White List, did not provide an adequate level of protection for personal data, due to the lack of a data protection law and/or a data protection authority (DPA) in those countries. The Plaintiff also sought from the Court a declaration invalidating the BCRs and SCCs, and the White List as specified in Annexure C of the Implementation Framework.

In the main hearing, Ikigai among other things contended (and I agree) that it is impossible to assess the adequacy of protection for personal data in a country that lacks both a data protection law and an independent data protection authority. This according to Ikigai is violatory of art. 2.11 of the NDPR and art. 7.0 of the Implementation Framework. The Court sided with Ikigai by stating that the Agency, when conducting an adequacy assessment for the purpose of international data transfers, must consider the third

country's 'Data Protection Law, Rule of law, respect for human rights, implementation of data protection rules, the existence of an independent data protection authority and its international commitments'.

Moreover, the Court held that, according to the NDPR and the Implementation Framework, the Agency had to consider the third countries contained in the White List as offering an adequate level of protection for personal data. The Court asserted that this was a mandatory condition of art. 2.11 of the NDPR and art. 7.0 – 7.2 of the Implementation Framework. In the light of this, the Court concluded that the inclusion of Algeria, Comoros, Guinea Bissau, India, Mauritania, Mozambique, Sierra Leone, Togo and Zambia in the White List is null and void since these countries lacked a data protection law or a DPA, and thus did not ensure an adequate level of protection within the meaning of art. 2.11 of the NDPR and art. 7.0 of the Implementation Framework that govern the process of international data transfers from Nigeria. The Court also stated that non-compliance with these provisions deprived the data subjects in Nigeria whose personal data were transferred to these countries of their enforceable data subject rights and their effective administrative and judicial redress mechanism. This consequently violated the right of privacy of Nigerians under section 37 of the Constitution of the Federal Republic of Nigeria (the Constitution).

Finally, the Court held that the use of BCRs and SCCs as mechanisms for international data transfers, as established under art. 7.3 of the Implementation Framework, was invalid since they were not provided for in arts. 2.11 – 2.12 of the NDPR, and thus exceeded the powers of the Agency under the NDPR. The Court based its decision on the case of *Amasike v Registrar General Corporate Affairs Commission* (2010) 13 NWLR (Pt. 1211) at 399, where the Supreme Court of Nigeria stated that 'a public body or authority with statutory powers must act lawfully and avoid exceeding or abusing its powers. It must remain within the boundaries of the authority granted to it'.

Considering this and other factors, the Court granted all the reliefs requested by the Plaintiff Ikigai.

Implications for the future of international data transfers in Nigeria

The Court's decision implies that under the NDPR, any international data transfers from Nigeria to third countries can no longer be made based on the White List. Moreover, any other country that lacks a data protection law and/or a DPA would also likely fail to meet the adequacy requirement and, therefore, any transfer of personal data from Nigeria to that country would be unlawful as well unless an exemption provided for in art. 2.12 applies. Therefore, it is recommended that before transferring personal data to third countries, data controllers in Nigeria must first confirm that a positive adequacy decision has been made by the Agency in respect of that country, or alternatively rely on any one of the exemptions provided in art. 2.12 of the NDPR. Otherwise, the transfer may be contested by data subjects as unlawful. Moreover, if such a legal challenge succeeds, the data subject may also claim compensation if there is a clear showing that the transfer breaches the constitutional right to privacy.

Furthermore, data protection compliance organisations (DPCOs) should be aware that, without any guidance from the Nigerian Data Protection Commission (the Commission), they must properly justify the legal basis of any international data transfers conducted by the companies they audit in the data protection audit report to be filed with the

Commission annually. It should also be noted that the NDPR remains in force alongside the Nigeria Data Protection Act 2023 (NDPA), which led to the Agency's transformation into the Commission. Therefore, any reference to the Agency in this article should be interpreted as a reference to the Commission for the purposes of the NDPA and NDPR.

Under the NDPA, the procedure for international data transfers is similar in some parts to the NDPR, and the lawfulness of such transfers depends on whether the third country or recipient complies with a law, BCRs, SCCs, code of conduct, or certification mechanism that ensures an adequate level of protection for the personal data (section 41 (1) (a)), or if an exemption applies (section 43 (1)). Section 42 (2) requires the Commission to consider the following factors when assessing the adequacy of the level of protection: the availability and enforceability of data subject rights, the possibility of a data subject to seek administrative or judicial redress, and the rule of law; the existence of a suitable instrument between the Commission and a competent authority in the recipient jurisdiction that guarantees adequate data protection; the access of a public authority to personal data; the existence and effectiveness of a data protection law; the existence and operation of an independent, competent data protection, or similar supervisory authority with sufficient enforcement powers; and the international obligations and agreements binding on the relevant country and its participation in any multilateral or regional organisations.

As of the date of this writing, the Commission is yet to exercise its power under the NDPA to designate any third country as providing an adequate level of protection, nor has it endorsed any BCRs, SCCs, codes of conduct, certification mechanisms or other instruments for international data transfers. Consequently, to ensure the legality and permissibility of international data transfers under the NDPA, the data controller (and/or processor) must rely on one of the exemptions provided for in section 43 (1).

Conclusion

Following the Court's judgment in this case, the Commission is expected to conduct adequacy assessments of third countries and issue positive adequacy decisions that will enable unrestricted data transfers from Nigeria to these countries. Unfortunately, adequacy assessment was not mentioned in the Nigeria Data Protection Strategic Roadmap and Action Plan (NDP-SRAP) 2023-2027.

To this end, the Commission should as a matter of priority adopt a proactive and cooperative approach to adequacy assessments, by consulting with data controllers, processors, DPAs of the third countries, data subjects and other concerned stakeholders, and by reaffirming its adherence to the principles and standards established in both the NDPA and NDPR. A positive adequacy decision by the Commission must rely on core data protection principles present in the legal framework of that third country that align with those stipulated in the NDPA and the NDPR. It must also indicate the scope of its applicability, whether national or sectoral, and the identity of an independent public authority in charge of enforcing the data protection rules. It is further recommended that the Commission establish a robust framework to oversee and evaluate its adequacy decisions on an ongoing basis and be ready to respond to any changes or challenges that may emerge.

In conclusion, international data transfers are a vital component of the global digital economy and digital society. Therefore, DPAs must conduct adequacy

assessments for international data transfers, in compliance with the applicable legislative frameworks. Adequacy assessments are a means of ensuring that the personal data of data subjects is safeguarded throughout its transit, irrespective of its destination. Finally, it must be emphasised that adequacy assessment is not only a legal requirement, but also of strategic importance for the Commission, as it can enhance its reputation, influence, and impact in the global data protection landscape.

chukwuyere@sskohn.com

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