



**THE LEGAL FRAMEWORK FOR THE TRANSFER OF PERSONAL  
DATA OF NIGERIAN CITIZENS TO FOREIGN COUNTRIES:**

**EXPLORING THE CASE IN SUIT NO. FHC/ABJ/CS/1246/2022  
BETWEEN INCORPORATED TRUSTEES OF IKIGAI INNOVATION  
INITIATIVE AND NATIONAL INFORMATION TECHNOLOGY  
DEVELOPMENT AGENCY (NITDA) IN THE LIGHT OF THE  
NIGERIA DATA PROTECTION ACT 2023**

 **LAGOS | ABUJA**



## BACKGROUND

The Federal High Court recently made a decision in the case of *Incorporated Trustees of Ikgai Innovation Initiative v. National Information Technology Development Agency (NITDA)*<sup>1</sup> nullifying the provisions of the whitelist set out in Annexure C of the Nigeria Data Protection Regulation Implementation Framework (“the framework”) which wrongly whitelisted some countries lacking an adequate data protection framework in their respective jurisdictions. The decision came shortly after the signing of the Nigeria Data Protection Act 2023 (NDPA). It is a landmark case which contributes to the reinforcement of data protection in Nigeria particularly the area of transfer of personal data of Nigerian citizens to foreign countries.

In the above case, Justice Obiora Ekwuatu of the Federal High Court, Abuja held that ***“where a country neither has a data protection law nor establish an independent data protection authority, measuring the adequacy of its data protection laws and regime is not possible. This violates the spirit of Article 2.11 of the NDPR AND Article 7.0 of DPIF on transfer of personal data abroad...The right of privacy guaranteed under section 37 of the Constitution is not one to be toyed with. For a citizen to be deprived of this right, such deprivation must be in accordance with the law. Therefore, a breach of the mandatory duty to whitelist countries that afford an adequate level of protection as enjoined by the provisions of NDPR and indeed DPIF is not one to be ignored as ignoring same may translate by extension as failure to comply with the constitutional stipulations to the right of privacy as enshrined in section 37 of the Constitution”***.



This judgement implies that where a foreign country lacks data protections laws, enforcement agencies and judicial redress mechanisms, it cannot be rightly whitelisted as a country where the personal data of Nigerian citizens can be transferred to without their consent as that will go against the Article 2.11 of the NDPR, Article 7.0 of the DPIF and section 37 of the Constitution which guarantees the right to privacy.

## BRIEF FACTS

The Plaintiff, an incorporated non-profit organization set up to advance information technology policy in Africa by undertaking diverse research on technology policy and legal frameworks across Africa, filed an originating summons against the Defendant which is a government agency created under the National Information Technology Agency Act 2007. The Plaintiff sought amongst other reliefs:

- i. a declaration that there is no basis for the introduction of Binding Corporate Rules and Standard Contractual Clauses through the DPIF as it is not conceived under the provisions of Article 2.11 and 2.12 of the NDPR;
- ii. a declaration that by virtue of the combined provisions of Article 2.11 of

<sup>1</sup> Suit No: FHC/ABI/CS/1246/2022

**the NDPR and Article 7.0 of the DPIF, the Defendant is obliged to whitelist only countries that have adequate level of protection of personal data;**

- iii. **a declaration that the whitelist set out in Annexure C of the DPIF is contrary to the combined provisions of Article 2.11 of the DPIF and thereby ultra vires, null and void.**

The plaintiff contended that the Defendant failed to comply with the spirit of its self-made NDPR and DPIF as Annexure C of the DPIF goes against the relevant provisions of the two laws (NDPR and DPIF) and endangers the constitutional right to privacy of the Nigerian citizenry including the Plaintiff's members. In reference to Article 2.11 of NDPR and Article 7.0-7.2 of DPIF, the Plaintiff argued that any transfer of personal data undergoing or intended for processing to an alien country shall only take place where such country has an adequate level of data protection. An adequate level of data protection in this sense implies that the country has a comprehensive data protection law, an independent data protection enforcement agency and a judicial mechanism for redress.

The whitelist countries compiled in Annexure C of the DPIF were ordinarily conceived by the framework to have an adequate level of data protection. The United Nations Conference on Trade and Development (UNCTAD) data protection legislative tracker revealed that some of these whitelist countries such as India, Togo, Comoros, Guinea-Bissau and Sierra Leone do not have data protection laws and independent data protection agencies despite the fact that some of these countries are signatories to the Malabo Convention but failed to ratify and implement its provisions. Although countries such as Algeria, Mauritania and Zambia and Mozambique had data protection laws but the laws failed to establish an independent data protection agency to enforce the provisions of the laws. These countries were therefore argued to be unfit for the whitelist contained in Annexure C of the DPIF and their inclusion was a blatant violation of the provision of Article 2.11 of the NDPR and therefore ultra vires, null and void.

It was further contended that the Defendant through Article 7.3 of the DPIF introduced two mechanism, Standard Contractual Clauses and Binding Corporate

Rules, for international data transfer which the Plaintiff argue was not within the contemplation of Articles 2.11 and 2.12 of the NDPR and the Defendant therefore has no power to introduce such provisions neither through the NDPR nor through the DPIF which was merely issued to provide clarifications on the provisions of the NDPR.

The Defendant though served with the originating summons and hearing notices failed to file any process in opposition of the suit. The court after considering the argument of the Plaintiff entered judgement in its favour by granting all the reliefs sought.

### **BASIS OF THE COURT'S DECISION**



In arriving at its decision, the Court made reference to the case of *Amasike v. Registrar General Corporate Affairs Commission*<sup>2</sup> where the Supreme Court held that

***“a public body or authority vested with statutory powers must act within the law and take care not to exceed or abuse its powers. It must keep within the authority given to it. It must act in good faith and reasonably. Where a person or body or authority claims to have acted pursuant to a power granted by a statute, such person or authority must justify the act, if challenged, by showing that the statute applied in the circumstances and that he or it was empowered to act under it”.***

The Court in applying this decision to the instant case held that the Defendant had failed to justify the use of its powers by including certain provisions in the DPIF. Since the facts set out in the Plaintiff's Affidavit were not denied, they were deemed admitted by the Court.

As regards the failure of the Defendant to file any process in response to the suit, the court held that

<sup>2</sup> (2010) 13 NWLR (Pt. 12110 @ 399.



**“It is trite also that the law is that where an appellant fails to file a reply brief when it is necessary to do so, he will be deemed to have conceded the points arising from the respondent’s brief.”** The court therefore rightly interpreted the failure of the Defendant to respond to the points and arguments raised by the Plaintiff to mean concession with same.

#### **COMMENTARY**

The right to data privacy emanates from the right to privacy enshrined in Section 37 of the Constitution as earlier mentioned. The Constitution remains the supreme law in Nigeria and every other law that contradicts any of its provisions is null and void to the extent of the contradiction. Therefore, any provision in the DPIF, which is a subsidiary legislation, which unjustly intercepts with the protection of the right to privacy of the Nigerian citizenry is therefore null and void. Similarly, no agency is empowered to enact any law, regulation or framework that contravenes the constitution.

As earlier stated, the implication of wrongly whitelisting a country lacking an adequate legal framework for data protection will imply that the personal data of Nigerian citizens transferred to such countries will be endangered and will put citizens at the risk of violation of their right to privacy enshrined in Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) and frustrate the goal of the Nigerian data protection laws. The decision in the case therefore provides a judicial precedence in the area of data protection to the extent of its compliance with the new NDPA.

It is worthy to note that this judgement did not make reference to the NDPA due to the fact that the law was not in force at the time the matter was brought before the court and new law are not meant to be retroactive. The decision is however in line to some extent with the provisions of Section 41 to 43 of the NDPA which provides for cross-border transfers of personal data. However, Section 41 r of the NDPA permits the transfer of data to a foreign country where the recipient is subject to binding corporate

rules and contractual clauses. This provision therefore modifies the aspect of the judgement that declared the introduction of Binding Corporate Rules and Standard Contractual Clauses through the DPIF void and by implication revives the provisions of Section 7.3 of the Framework.

Section 41 clearly provides that personal data can be transferred to country where the recipient ***“is subject to a law, binding corporate rules, contractual clauses, code of conduct, or certification mechanism that affords an adequate level of protection with respect to the personal data in accordance with this Act”***. Section 42 of the Act provides a guideline for determining the adequacy of a country’s law by providing a country’s level of protection is deemed adequate if it has a framework that upholds principles that are substantially similar to the conditions for processing of personal data enshrined in the Act. The rest of the provisions of the NDPA on data transfer to foreign countries serve similarities with what is contained in the 2019 regulation which is still in force.

In a nutshell, the above case provides a good precedence in the area of data protection which is still a novel and developing area of law in Nigeria. The aspect of the judgement that declared the introduction of Binding Corporate Rules and Standard Contractual Clauses through the DPIF is however nullified by the provisions of the NDPA Act as stated earlier. It is also worthy to note that by virtue of Part II of the NDPA, the new agency in charge of the enforcement of the NDPA is the Nigeria Data Protection Commission.

## CONTACTS



**LAZARUS KALU**

lazarus.kalu@advocaat-law.com



**TEMITUOPE KEKEMA**

temituope.kekema@advocaat-law.com