



\$1.3 BILLION FINE ON META: THE COMPLEXITIES OF CROSS-BORDER DATA TRANSFER IN A DIGITAL WORLD

CHRISTIAN ANIUKWU | CHIZITEREIHE OTI | IBITOLA AKANBI



\$1.3 BILLION FINE ON META: THE COMPLEXITIES OF CROSS-BORDER DATA TRANSFER IN A DIGITAL WORLD

In today's world, data has become a valuable resource, fondly referred to as the new oil that drives businesses and industries forward as it can be used to deliver targeted advertising, improved services, and gain insights into consumer behavior. For instance, Airbus, the aircraft manufacturer, has

improved its supply chain by sharing design and engineering data, resulting in a reduction in supplier delivery times from several weeks to just a few hours¹. The proliferation of data in recent years has been greater than anything we have seen before. However, the collection, storage, and processing of personal


¹ <https://www.mondag.com/nigeria/data-protection/1278964/the-lowdown-on-data-privacy-and-data-protection-policy-for->

[startups#:~:text=Noncompliance%20or%20breach%20of%20the,case%20of%20a%20data%20controller">startups#:~:text=Noncompliance%20or%20breach%20of%20the,case%20of%20a%20data%20controller](#)

data also pose significant risks to individuals' privacy and security, especially when that data is transferred across borders as this data includes sensitive information such as financial details, health records, and personal identifiers that, if compromised, can lead to identity theft, fraud, and other forms of cybercrime.

issue to anyone (Individuals, organizations and corporations) who processes or handles personal data.

These strict regulations exist for adherence and failure to comply can result in legal and financial consequences, as evidenced by the recent \$1.3 billion fine imposed on Meta by the European Union (EU) for violating privacy laws.



"Data protection has become a critical issue to anyone (Individuals, organizations and corporations) who processes or handles personal data..."

To address these concerns, the European Union (EU) introduced the General Data Protection Regulation (GDPR) in 2018, which sets strict rules for the processing of data within the EU and the transfer of personal data outside the EU. Consequently, Data protection has become a critical

In this article, we will discuss the import of the decision of the Court of Justice of the European Union (CJEU) in the recent META case, likewise, the need for the Europe Union-United States (EU-US) and other countries of the world to have in place comprehensive Data Policy laws, regulations, frameworks on cross-

border data transfers that would provide legal clarity and certainty to companies and organizations engaged in cross border data transfers in today's interconnected world. We would also be juxtaposing the international/cross-border transfer regulations under the recently enacted Nigeria Data Protection Act and extant data protection laws in Nigeria, with the provisions of the General Data Protection Regulation 2018 (GDPR).

CASES OF FINES AND PENALTIES FOR DATA BREACHES AND NON-COMPLIANCE -META AS CASE STUDY

The inception of the GDPR brought about strict regulation in the data protection space, while imposing million-dollar worth of fines on erring companies. Some of these fines imposed over the years were

imposed on the following companies: Instagram, which was fined \$403 million by Ireland's Data Protection Commission for violating children's privacy; T-Mobile, which settled for \$350 million after a data breach impacting 77 million people; and the Irish regulator also imposed four fines against Meta's platforms Facebook, Instagram and WhatsApp ranging between €405 million and €225 million in the past two years. Also, Amazon was previously fined €746 million by Luxembourg's National Commission for Data Protection of which it is set to appeal. The Appeal will be heard at a Luxembourg Court in January 2024² However, one of the most recent is, the CJEU imposing a record fine of \$1.3 billion on Meta, the parent company of Facebook. The decision of the CJEU is a result of the case brought by the Australian privacy activist, Max Schrems, who argued that the mechanism in place for the transfer of EU citizen data to America

²

<https://mlexmarketinsight.com/news/insight/amazon-s-appeal-of-record-gdpr-fine-to-go-to-luxembourg-court-in-january-2024>

[n-s-appeal-of-record-gdpr-fine-to-go-to-luxembourg-court-in-january-2024](https://mlexmarketinsight.com/news/insight/amazon-s-appeal-of-record-gdpr-fine-to-go-to-luxembourg-court-in-january-2024)

did not protect Europeans from U.S surveillance. It is worth noting at this point that there have been various mechanisms implemented to regulate cross-border data transfer between the EU and US.

The latest was the Privacy Shield which was struck down by the CJEU in 2020. Since the overturn of the Privacy Shield in 2020, the officials of both the EU and US have been unable to produce a mechanism that replaces the Privacy Shield for over 2 years, thus making companies result to alternate measures to ensure the protection of data of EU citizens.

In this instance, META used a mechanism known as standard contractual clauses, an option available under Article 46(1) of the GDPR, to transfer personal data in and out of the EU. This was not blocked by any court in the EU and these clauses were adopted by the EU Commission in conjunction with other measures implemented by Meta. However, upon the institution of the case against Meta, it was held by the CJEU that these arrangements by Meta did not address the risks to fundamental rights and freedom of data subjects.³



"... the CJEU imposing a record fine of **\$1.3 billion** on Meta, the parent company of Facebook. The decision of the CJEU is a result of the case brought by the Australian privacy activist..."

³ [Meta fined a record \\$1.3 billion over EU user data transfers to the U.S. \(cnn.com\)](https://www.cnn.com/2023/07/04/tech/meta-fine/index.html)

This decision by the CJEU was then followed by the fine imposition that has now gained fame as the largest fine imposed under the EU's GDPR for violating privacy laws, in a matter that can be mistaken as a witch-hunt on big companies. Additionally, the Company was also given six months to suspend the transfer of data collected from Facebook users in Europe to the US.

This decision of the CJEU has resulted in a substantial penalty that could potentially affect American businesses. Some industry representatives have expressed their discontent with the ruling, claiming that the penalty increases the legal uncertainty that companies already face when transferring data across international borders while also asserting that such transfers are critical for everyday functions, such as collaborating with colleagues in

international offices and fulfilling orders for a global customer base⁴. The decision of the CJEU seems like punishing a child for not eating a meal that the parent did not prepare, the child in this case being Meta, and the Parent being the EU.

It is about that there is provision for a comprehensive framework by the government for cross-border data transfer between EU and US, as it seems that nothings besides from this would be sufficient to meet the GDPR's standards on data privacy of its citizens. Although this holds no certainty as the previous framework, Privacy Shield, was also a result of a consolidated efforts of both governments.

WHY IS A CONSOLIDATED EFFORT REQUIRED?

In March 2022, to remedy the tussle, President Biden implemented more

4

<https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>

measures to protect Europeans' personal data from being collected by U.S. intelligence agencies, giving individuals the ability to seek legal action for any illegal interception of their data. However, these measures seem not be ever sufficient as Data protection Activists, specifically Max Schrems who won the lawsuit nullifying the US-EU data sharing agreement (Privacy Shield), still believes that unless U.S surveillance laws are amended, Meta will need to significantly restructure its systems. One solution he suggested was a "federated social network," where most personal data remain within the EU, with only necessary transfers made⁵.

Fortunately, the EU-US Data Privacy Framework is anticipated to be ratified by this Summer, which will offer stability and legal assurance for companies, while ensuring robust privacy safeguards for individuals. In

the meantime, businesses may continue utilizing standard contractual clauses (SCCs), which undergo individual evaluation by EU regulators. In this interim, it is suggested that the EU commission works hand in hand with the regulators in approving these SCCs, in order to avoid a repeat Meta situation where international companies are penalized for implementing SCCs already adopted by the EU Commission.

SCCs are standardized templates that have been approved by the European Commission and can be adopted by companies engaged in cross-border data transfers. This was adopted as a temporary mechanism in place for EU-US cross border transfer of data after the Privacy Shield was upturned in 2020. It is thus important that the U.S and the EU bring back certainty to data flows between the two region since this

⁵ <https://www.politico.eu/article/eu-hits-meta-with-record-e1-2b-privacy-fine/>

cross-border data transfer has implications that are bigger than just META and has a significant impact on the transatlantic economy, society, and international cooperation, if not addressed appropriately.

CROSS BORDER TRANSFER OF PERSONAL DATA: THE NIGERIAN CONTEXT

Whilst in Europe the GDPR prevails as it aims to harmonise data protection laws across the EU, and it also provides enhanced rights for individuals over their personal data.

In Nigeria, the recently passed Nigeria Data Protection Act (NDPA) 2023 is the extant law that governs and regulates the processing of personal data of individuals, protection of the privacy rights of data subjects in Nigeria and it also applies to any organizations that processes personal data of individuals located in Nigeria regardless of where the organization is based and data controllers/processors domiciled, ordinarily resident or ordinarily operating.



"...Nigeria Data Protection Act (NDPA) 2023 is the extant law that governs and regulates the processing of personal data of individuals..."

The NDPA was enacted in response to the need for a comprehensive data protection law in Nigeria. The objective of the Act, amongst other things, is to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution. True to its objectives, the Act enacts more precise and comprehensive provisions in accordance with its objectives. It ensures to also put stricter mechanisms in place that assures data subjects of the protection of their rights.

Although the provisions of the NDPA attempts to include robust provisions on the regulation of cross-border transfer, there still exists loopholes and inadequacies in the provisions covered in section 42-44 of the Act. The provisions on cross-border transfers are based on the adequacy provisions of the receiving country. Thus, section 42 of the Act provides that cross-border transfer of data can occur where the recipient of the

personal data 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 section 43. Following the provisions of section 43, the Nigeria Data Protection Commission may approve such binding rules, codes of conduct or certification mechanisms proposed to it by a data controller. The NDPA further provides that the Commission is required to make guidelines and regulations that will determine the adequacy of the recipient, as well as determine from time to time whether any country, region or specified sector within a country, or standard contractual clauses, afford an adequate level of protection, as is seen under the Nigeria Data Protection Regulation as the 'Whitelist'.

On face value, it might seem that the provisions on cross-border data

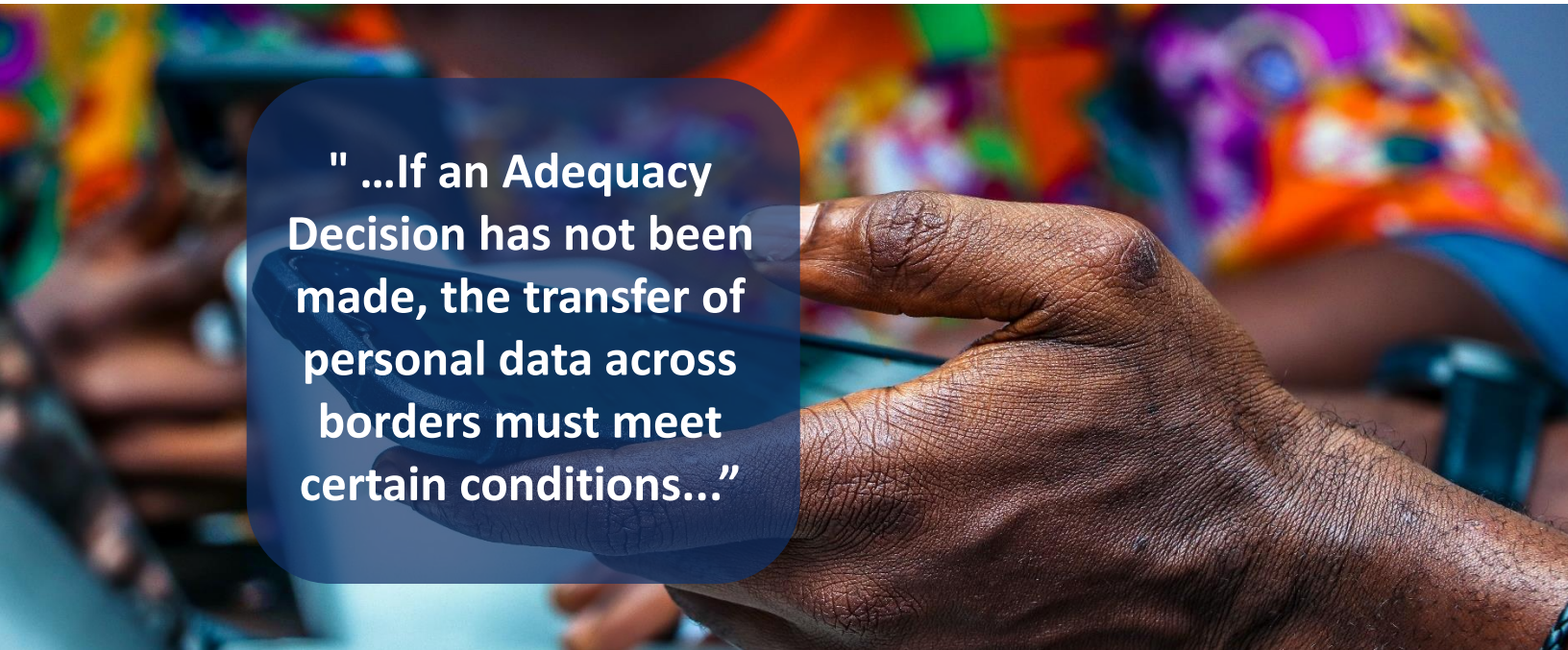
transfer of the NDPA as opposed to the Nigeria Data Protection Regulation, as provided for under the Nigerian Data Protection Implementation Framework, are more elaborate. However, the authors of this article are of the opinion that the provisions of the NDPA contain subtle loopholes that might affect the strict regulation of cross-border transfer. Considering the digitalization of the world and the consistent movement of data and high-risk, the provisions of cross-border transfer should be clearer, specific, and more stringent. The Law should have clearly provided for a Binding Corporate Rule or Standard Contracting Clause as a major requirement, while proffering a stringent template or proposed content of what should be of the BCR or SCC. Also, where the law intended to leave gaps to be filled by regulations and guidelines, then a timeline should have been provided for or the Act could have ordinarily made these provisions, this would see

to an efficient data privacy ecosystem. Where strict provisions of the mechanisms required to ensure adequate cross-border data transfer are provided, then it would be clear the data controller's obligations and very little would be left to presumptions.

It is worth noting that the provisions of the NDPA does not repeal the provisions of the NDPR or its subsidiary regulations but rather adopts them as though made under the Act, thus making applicable conflicting provisions on cross-border data transfer, including the requirement of the approval of the Attorney General of the Federation for cross-border data transfer requests, including the adoption of countries listed on the Whitelist as countries with appropriate level of adequacy provision. If an Adequacy Decision has not been made, the transfer of personal data across borders must meet certain conditions. These include:

- a. Obtaining express consent from the data subject,
- b. Transferring the data for the performance of a contract,
- c. Transferring it for public interest reasons,
- d. Transferring it for legal claims or transferring it to protect the vital interests of the data subject or other persons who cannot give consent due to physical or legal incapacitation.

behind in terms of the protection of citizen's personal data as opposed to its European counterpart, as the latter provides for clauses in a BCC to make it sufficient for use in cross-border transfer, empowers the regulators to make a clear decision as to what countries ensure an adequate level of protection, provide stricter safeguards for cross-border data processing in the absence of a adequacy provision⁶.



"...If an Adequacy Decision has not been made, the transfer of personal data across borders must meet certain conditions..."

Despite the provisions for cross-border data transfers, the NDPA is steps

In a world that currently runs on various international data transfers, it

⁶ Article 44-46 General Data Protection Regulation 2018.

has become imperative to bolster up its provisions on cross-border data transfer, such that will perhaps take into accounts specific mechanisms or frameworks in place for cross-border transfer of data both within and outside Africa and strict provisions or templates of SCCs adopted by the Nigerian Data Protection Commission to be adopted by Data Controller Processors.

Millions of data are processed daily all over the world and thus it is imperative that countries are proactive and efficient in the protection of the rights of their citizens. It has also become crucial for Nigeria and other African countries to develop a comprehensive data protection framework for cross-border transfer in Africa that considers the specific needs and challenges of their populations. This includes engaging with stakeholders

such as civil society organizations, academics, and industry players to ensure that data protection laws are effective, comprehensive, and in line with international best practices.⁷

CONCLUSION

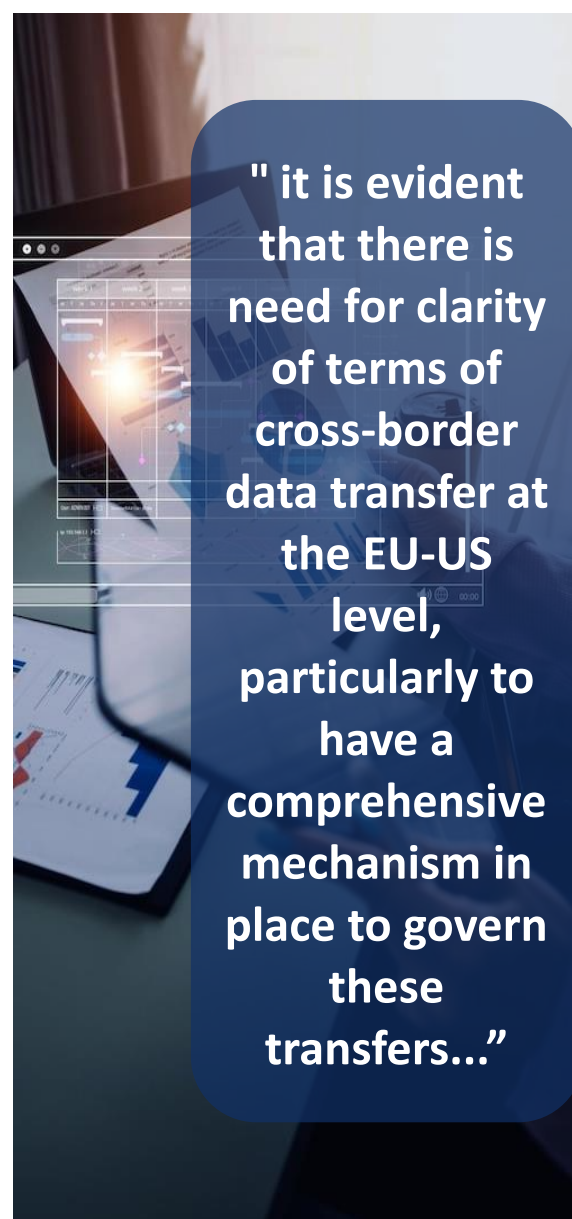
In conclusion, it is evident that there is need for clarity of terms of cross-border data transfer at the EU-US level, particularly to have a comprehensive mechanism in place to govern these transfers. It is worth noting that a continuous lack of such a mechanism would be detrimental to the transatlantic economy, society, and international cooperation. In a fast-growing digital world, cross-border data transfer is essential for efficiency. Thus, the government and regulators are required to implement uniform mechanisms in place, as the lack of

⁷ <https://www.linkedin.com/pulse/draft-data-protection-bill-2022-interesting-approach-oloni-cipp-e>

this only seems like a trap for bigger fines on global corporations. Lessons from the Meta case are highly instructive and relevant in the Nigerian context. These lessons revolve around principles such as generating SCCs. Although, there exists an apparent conflict arising from the regulations guiding data protection in Nigeria, companies and organizations are advised to ensure strict compliance with the provisions of the NDPA, NDPR and err on the side of caution by liaising and working with the Commission, especially in terms of cross-border transfer.

It is also suggested that the Nigeria Data Protection Commission adopts more comprehensive mechanisms for cross-border data transfer that assures the citizens of the protection of their data that are transferred outside the country. In terms of cross-border data transfer in Africa, the writers are of the opinion that it has become pertinent that with the rise of

various African start-up companies servicing various companies within the region, Africa adopts a comprehensive cross-border data transfer framework as has been done over the years between the US and the EU.





AUTHORS



Christian Aniukwu
Managing Partner



Chizitereihe Oti
Associate



Ibitola Akanbi
Associate

THE FIRM

Stren & Blan Partners is an innovative and dynamic law firm with a compelling blend of experienced lawyers and energetic talents. Our lawyers are available to provide you with guidance and innovative solutions on complex business and legal issues across a variety of sectors.

This is a publication of Stren and Blan Partners and it is for general information only. It should not be construed as legal advice under any circumstances. For more information about the firm and its practice areas, please visit www.strenandblan.com. You can also contact us via contact@strenandblan.com or call +234 (0) 702 558 0053.