Challenges of Cross-Border Data Transfer and Privacy Protection

- *Temiloluwa Koya and Monsurat Lamina*

Introduction: The Path of Data Across Borders

Today, personal data doesn't stay in one place. It moves—fast and often—across countries. Each transfer brings new legal responsibilities for businesses that handle such data.

Imagine Amina, a Nigerian professional. Her day starts under Nigeria's Data Protection Act (NDPA), which governs how her data should be collected, stored, and shared. But the moment she orders shoes from a UK-based store, her personal details—name, address, payment information—are processed under the EU's General Data Protection Regulation (GDPR). Later, she uploads a file to a U.S.-based cloud provider, with the data stored in Germany and Japan. That file may still be subject to U.S. laws like the CLOUD Act, which gives American authorities access under specific conditions. At night, she video-calls a colleague in Kenya and posts a photo online—further extending her digital footprint across multiple jurisdictions.

For businesses handling such cross-border data, knowing which law applies at each stage—and complying with it—is essential. While the NDPA sets a foundation for data governance in Nigeria, international transactions often trigger other legal frameworks. This overlap demands a deliberate and well-informed compliance approach. Businesses, data controllers and data processors must no longer treat data protection as a background concern. Clear policies and responsible data practices are no longer optional; they are necessary to meet legal obligations and maintain customer trust.

The Global Data Odyssey: Legal Risks and Business Realities

Cross-border data transfers are a central part of how businesses serve customers, manage operations, and grow internationally. But with every transfer, legal risks arise—especially when different national laws impose conflicting obligations. Navigating these challenges is essential to staying compliant and building trust across markets.

Managing Legal Conflicts: GDPR vs. the U.S. CLOUD Act

The EU's General Data Protection Regulation (GDPR) is widely regarded as one of the strictest data privacy frameworks globally. It requires that any personal data leaving the EU be given "essentially equivalent" protection wherever it goes (Articles 44–49). This includes robust safeguards around consent, accountability, and individual rights. By contrast, the U.S. CLOUD Act allows American law enforcement to compel U.S.-based companies to provide access to data, even if the data is stored outside the United States. This creates tension. For example, in 2013, U.S. authorities requested access to emails held by Microsoft on servers in Ireland.

Microsoft refused, citing privacy obligations under Irish and EU law. Although the case was eventually overtaken by the CLOUD Act—which clarified U.S. government powers—the underlying tension remains: how can companies comply with one country's law without breaching another's? This legal tug-of-war forces businesses to think carefully about how and where they store and transfer data.

Practical Strategies for Cross-Border Compliance

To reduce legal exposure, businesses must act proactively. Many rely on Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to lawfully transfer data across borders. These tools provide a legal basis for transfers and help demonstrate that data is handled with sufficient protection—even in jurisdictions without similar privacy laws.

SCCs are pre-approved contractual terms that require both parties—the sender and the recipient of the data—to meet strict obligations. These include limiting the use of data to clearly defined purposes, maintaining appropriate security safeguards, and protecting the rights of individuals whose data is transferred. They are commonly used in commercial relationships between unrelated organizations, such as when a Nigerian company outsources data processing to a foreign service provider.

BCRs, by contrast, are internal rules adopted by multinational companies to regulate the movement of personal data within the same corporate group. They are legally binding and apply across all entities in the group, regardless of where each entity is located. Although they take more time and resources to develop and implement, BCRs offer greater operational flexibility, particularly for large businesses with complex data flows between offices or subsidiaries in different countries.

Both SCCs and BCRs provide legal assurance that personal data is not left unprotected when it crosses borders. However, they must be backed by internal systems that ensure day-to-day compliance—through clear policies, regular audits, staff training, and close oversight of service providers. Managing cross-border data responsibly requires a balance of legal formality and operational discipline.

Cross-Border Risks: Lessons from the Flutterwave Case

In 2024, Flutterwave—a major fintech player in Nigeria—suffered a security breach that led to unauthorized transfers of funds. Flutterwave operates in multiple countries, so the breach raised concerns beyond Nigeria. The breach revealed a key lesson: meeting local data compliance standards is not enough. Businesses must anticipate and address risks that arise from global data movement. Gaps in security and governance can expose companies to

liability and reputational harm beyond Nigeria's borders. The Flutterwave case highlights the need for coordinated data protection strategies that align with international best practices, not just national regulations.

As more Nigerian businesses scale internationally, compliance with the NDPA and investment in stronger data security are not just legal requirements—they are business priorities. A clear, well-managed data strategy helps reduce risk and strengthens Nigeria's standing as a credible player in the global digital space.

What's Ahead: Trends in Cross-Border Data Privacy

Several key trends are shaping the future of global data management:

1. **Data Sovereignty and Localization**: More countries are introducing laws that restrict how and where certain categories of personal data can be stored or processed. For instance, India's data protection law limits the transfer of sensitive personal data outside its borders, while Brazil has introduced similar restrictions. These rules often mean companies must build local infrastructure/data centres and adjust their global data practices. For businesses operating across multiple countries, navigating these requirements is becoming a key part of compliance planning.

2. **Privacy-Enhancing Technologies (PETs):** To stay compliant while still using data, companies are turning to tools that protect privacy. These include techniques like differential privacy and federated learning, which help extract insights without exposing individual data. As privacy laws tighten, these tools are becoming part of standard data management strategies.

3. **Push for Global Harmonisation:** Efforts are underway to reduce the regulatory fragmentation that currently complicates international data transfers. Initiatives led by organizations like the Organisation for Economic Co-operation and Development (OECD) aim to create common standards that promote consistency across legal systems. While meaningful convergence has yet to be achieved, businesses should monitor these developments, which may eventually simplify compliance across borders and reduce legal uncertainty.

4. **Expanding Consumer Rights and AI Oversight:** As artificial intelligence becomes more common, regulators are introducing new obligations on how personal data is used in automated systems. These include enhanced rights for individuals—such as the ability to access, delete, or move their data—and requirements for transparency in algorithmic

processing. Companies using AI must now consider not only how they collect data, but also how their systems explain and justify automated decisions.

5. **Rising Standards for Corporate Responsibility:** Beyond legal compliance, there is growing public pressure for companies to act responsibly in their use of personal data. Consumers expect transparency, fairness, and ethical handling of their information. Businesses that take clear positions on data ethics and demonstrate accountability are more likely to earn trust and protect their reputations in the long term.

Navigating the Data Landscape: Practical Steps for Businesses

For businesses involved in cross-border data transfers, legal compliance and operational readiness must go hand in hand. The following steps offer a practical roadmap:

- **Understand Applicable Laws**: Identify all data protection laws relevant to operations and data flows. Monitor regulatory developments across jurisdictions and update internal policies accordingly.
- **Develop Clear Internal Policies**: Establish practical rules for how personal data is collected, stored, accessed, and shared. Ensure alignment with both national regulations and international standards.
- **Strengthen Data Security**: Implement safeguards such as encryption, access controls, and breach detection systems to protect sensitive data and support compliance obligations.
- **Raise Internal Awareness**: Train employees on data protection responsibilities. A well-informed workforce reduces risk and ensures day-to-day compliance.
- **Coordinate Legal and Technical Expertise**: Involve legal, compliance, and IT professionals in designing and reviewing data strategy. Cross-functional collaboration is essential to managing legal and technical risks effectively.
- **Use Legal Transfer Mechanisms**: Adopt tools like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to lawfully transfer data across borders and ensure adequate protection throughout the data lifecycle.

By following these steps, companies can reduce legal exposure, reinforce stakeholder confidence, and stay competitive in an increasingly regulated global data environment.

Conclusion: Building Trust Through Smart Data Practices

As data moves across borders, businesses must manage a growing set of privacy rules. Adapting to these rules is not just about compliance—it is an essential part of sustainable, ethical operations. Nigeria's data protection laws, alongside global shifts in privacy and security expectations, highlight the importance of clear strategy and strong governance. Businesses that are proactive, follow the law, and respect individual rights will be better placed to compete and grow. For tailored guidance on navigating cross-border data compliance, please contact us at info@scp-law.com.

REFERENCES

1. George Yijun Tian (2017): Current Issues Of Cross-Border Personal Data Protection In The Context of Cloud Computing and Trans-Pacific Partnership Agreement: Join Or Withdraw.
2. https://www.reedsmith.com/en/perspectives/2018/06/potential-conflict-and-harmony-between-gdpr-and-the-cloud-act
3. United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2016).
4. Nigerian Data Protection Act 2023.
5. https://panfinance.net/flutterwave-suffers-7m-security-breach/#
6. Digital Personal Data Protection (DPDP) Act, 2023.
7. Data Privacy Day 2024 – Key Global Developments in Data Privacy and Cybersecurity in 2023 and What to Expect in 2024 | Covington & Burling LLP