THE
TRUSTED
ADVISORS

Data Protection and Privacy Laws for Telecom Companies: Compliance Strategies

Authors

Grace Eniyandunmo
Associate

Adeife Omolumo
Associate

www.trustedadvisorslaw.com

Swipe

INTRODUCTION

In today's digital economy, telecom businesses are vital to data exchange, supporting everything from voice communication to internet access, mobile banking, and location monitoring. In Nigeria, where mobile and internet adoption is quickly increasing, telecom providers deal with massive amounts of personal and sensitive data on a daily basis. As a result, they are crucial stakeholders in the discourse around data protection and privacy.

WHAT IS DATA PROTECTION?

Data protection is the process of safeguarding data and restoring important information in the event that the data is corrupted, compromised or lost due to cyberattacks, shutdowns, intentional harm or human error. Protecting sensitive data is essential for maintaining client trust, especially for data-driven sectors like telecoms.

As Nigeria advances toward a digital economy, the volume of information transmitted online continues to grow, increasing the risk of cybercrime, fraud, and identity theft. To operate effectively and comply with laws like the Nigeria Data Protection Act, organizations must implement robust data protection plans that safeguard against threats.

IMPORTANCE OF DATA PROTECTION FOR TELECOM COMPANIES IN NIGERIA

Data protection and privacy laws are intended to govern how personal data is gathered, processed, kept, and disseminated while upholding individuals' privacy rights. Compliance with these laws is not just a legal responsibility for Nigerian telecom businesses, but it is also a strategic need in a data-driven economy.

The telecommunications industry, due to the sheer volume of data it handles, sits at the heart of the data protection debate in Nigeria. Telecom companies collect everything from names, addresses, and call logs to biometric information during SIM registration. This positions them as key data controllers under the law, with heightened responsibilities.

Telecommunication companies found in violation of data protection laws can face penalties ranging from tens of millions to billions of naira, depending on the severity and impact of the breach.

NIGERIA DATA PROTECTION ACT (NDPA) 2023

The Nigeria Data Protection Act (NDPA) 2023 is at the heart of Nigeria's data protection system as it establishes a comprehensive legal framework for personal data protection in Nigeria and is consistent with international standards such as the EU's General Data Protection Regulation (GDPR). It establishes the Nigeria Data Protection Commission (NDPC), tasked with overseeing the enforcement of data privacy laws nationwide.

The NDPA provides a coherent legal structure for how personal data should be collected, processed, and safeguarded. It sets out the conditions under which data can be lawfully processed. This is whether it is based on consent, contract, legal obligation, or public interest. It also guarantees the rights of individuals to access their data, request corrections, object to processing, or demand deletion, giving consumers much-needed control over how their personal information is used.

Telecom providers must acquire and use personal data on one of the permissible bases specified in the NDPA, such as user consent, contractual requirement, or legal obligation. Individuals have the right to access, correct, delete, or object to the processing of their personal data, and telecom providers must have methods in place to react to these requests within a specific timeframe. They must also establish suitable technical and organizational safeguards to protect personal data from unauthorized access, loss, or misuse. In the event of a data breach, telecom companies must notify the Nigeria Data Protection Commission (NDPC) and affected persons within a certain timeframe.

The NDPA imposes restrictions on the transfer of personal data outside Nigeria, requiring that such transfers occur only to countries with adequate data protection laws, appropriate safeguards in place or the company uses mechanisms like standard contractual clauses. This provision is especially relevant in a globally connected industry like telecommunications. Given the sensitive nature and volume of data handled by telecom companies, strict compliance with these legal provisions is essential. Failure to adhere to the NDPA can result in significant penalties, reputational damages, and loss of customer trust.

NIGERIAN COMMUNICATIONS ACT, 2003

The Nigerian Communications Act, 2003 provides a framework aimed at promoting fair competition and universal access to communications services. It establishes the Nigerian Communications Commission (NCC) as an independent regulatory authority with the power to grant and enforce licenses, manage the frequency spectrum, and set industry standards.

Telecom companies are regulated by the Nigerian Communications Commission (NCC), which enforces specific privacy-related obligations through various guidelines. Notably, the Consumer Code of Practice Regulations require operators to ensure the confidentiality of customer information and to obtain explicit consent before sharing data with third parties. The SIM registration framework also imposes strict obligations for protecting biometric data, reinforcing the need for secure storage and limited access.

CYBERCRIME (PROHIBITION, PREVENTION ETC) ACT 2015

The Cybercrime (Prohibition, Prevention, etc.) Act 2015 mandates service providers to retain traffic data and subscriber information for two years and release it to law enforcement agencies upon request.

When sharing this information, service providers must balance the need for disclosure with the individual's right to privacy, taking measures to protect data confidentiality.7 The Act also prescribes penalties, including fines and imprisonment, for offenses such as unlawful interception of electronic messages; computer fraud and forgery; unauthorized modification of data and systems interference.

COMPLIANCE STRATEGIES FOR TELECOMMUNICATION COMPANIES

Telecommunication companies in Nigeria can adopt several strategies to ensure compliance with data protection and privacy laws. These strategies include:

1. Creating and Implementing Data Protection Policies:
Telecommunication companies should develop and implement comprehensive data protection policies that outline procedures for collecting, storing, and processing personal data. Privacy policies should be clearly communicated to users, and data processing activities must be documented and justifiable. These policies should be regularly reviewed and updated to ensure they remain effective and compliant with changing regulations.

2. Appointing a Data Protection Officer:
Companies classified as data controllers of major importance, a category that includes telecom operators are mandated to appoint a Data Protection Officer (DPO).8 A Data Protection Officer (DPO) should be appointed to oversee data protection and privacy compliance. The DPO can provide guidance to the company on data protection issues.

3. Conducting Regular Audits:
Telecommunication companies are required to conduct regular audits to ensure continued compliance with data protection regulations and identify areas for improvement. They should also conduct data protection impact assessments to identify potential risks and mitigate them.

4. Implementing Data Security Measures:
Telecom companies are expected to implement appropriate technical and organizational measures such as encryption, firewalls, and secure access protocols—to prevent unauthorized access or data breaches. In the event of a breach, the law requires prompt notification to the NDPC and affected individuals, reflecting global best practices.9

5. Training Employees:
Telecom companies are advised to provide regular training to employees on data protection best practices and principles as it relates to transparency, data minimization, data retention and respect for subscribers rights.

6. Obtaining Consent:
Telecom companies must obtain explicit consent from subscribers before collecting and processing their personal data. Consent must be freely given, specific, informed, and unambiguous.

EFFECT OF NON-COMPLIANCE

Non-compliance with Nigeria's data protection regulations can have severe consequences. The Nigerian Data Protection Act, 2023, outlines significant legal sanctions for violations. If the Commission determines that a data controller or processor has breached or is likely to breach compliance orders, it may issue a written order. This order can include a warning, a requirement to comply with data protection provisions, or a cease and desist order.

The Act also empowers the Commission to impose penalties, such as compelling the offending party to remedy the violation, pay compensation to affected data subjects, account for profits made from the breach, or pay a penalty or remedial fee.

Beyond legal penalties, non-compliance poses significant reputational risks. Breaches of data protection obligations can severely damage consumer trust, leading to a decline in customer confidence and revenue.

Operational disruptions are another consequence of non-compliance. Regulatory authorities may impose mandatory audits and increased scrutiny on organizations found in breach. These measures can disrupt normal business operations, diverting critical resources away from innovation and service improvement.

The cumulative effect of legal penalties, reputational damage, and operational interruptions can hinder a telecommunication company's ability to operate effectively and sustain long-term growth. Therefore, implementing robust data protection strategies is essential for telecom companies operating in Nigeria.

CONCLUSION

Given the sensitive nature and volume of data handled by telecom companies, strict compliance with data protection and privacy laws is essential. Failure to adhere to the data protection and privacy obligations as provided under these laws can result in significant penalties, reputational damages, and loss of customer trust.

At The Trusted Advisors, we help telecom companies navigate their data protection obligations with confidence. Our experienced team offers tailored guidance to ensure compliance, minimize risks, and build customer trust.