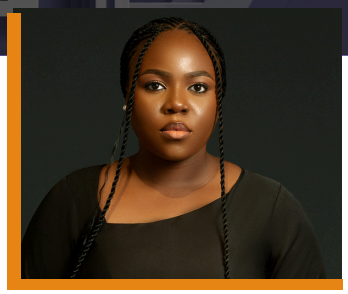
DATA PROTECTION INCIDENT READINESS: WHAT TO DO BEFORE, DURING, AND AFTER A DATA BREACH

March 2026



Oladiran Falore
Managing Partner



Precious Bassey
Associate Counsel

Abstract

The rapid expansion of Nigeria's digital economy has resulted in unprecedented levels of personal data generation and processing. Financial institutions, telecommunications providers, e-commerce platforms, health service providers and government agencies increasingly rely on digital infrastructure to deliver services to millions of users. While this transformation has improved efficiency and widened access, it has also heightened the risk of data breaches capable of exposing large volumes of sensitive personal information. Public concern has been sharpened by reports surrounding the alleged commercial access to National Identification Number (NIN), Bank Verification Number (BVN) and related identity data, even as the National Identity Management Commissiondenied that its core database had been compromised. These developments have raised serious questions about governance, access control and security safeguards across Nigeria's digital ecosystem.

In response, Nigeria enacted the Nigeria Data Protection Act 2023 (the "Act"), creating the country's first comprehensive statutory regime for data protection and establishing the Nigeria Data Protection Commission (the "Commission") as the primary supervisory authority. Yet legal compliance cannot be achieved through policy documents alone. It requires organisations to build operationally effective breach-response systems capable of identifying, containing, reporting and remediating personal data incidents in a manner that aligns with the expectations of the Commission. This article examines the concept of data protection incident readiness through a Nigerian lens and proposes a structured breach-response framework informed by Nigerian case studies and comparative insights from the General Data Protection Regulation 2025 ("GAID").

1. Introduction

In Nigerian parlance, many organisations still approach compliance with what can only be described as a fire-brigademental ity: action begins only when the flames are already visible. Data breaches, however, do not usually begin with noise. They often begin quietly, with weak governance, poor vendor discipline, careless access control and the dangerous assumption that privacy is a legal formality rather than an operational duty.

A common example illustrates the point. It is not unusual for Ministries, Departments and Agencies to issue demand notices or correspondence and inadvertently copy persons who have no business being part of the exchange. In other cases, broadcast emails are sent with every recipient openly copied, rather than using blind copy for multiple intended recipients. The usual reaction is often telling: the communications unit barely notices the mistake, the IT team hesitates or declines to take immediate steps to recall or contain the email, and management dismisses the matter with the view that no real harm has been done. By the time the organisation begins to treat the incident with the seriousness it deserves, unauthorized release of data have already been occasioned.

The Act was enacted to move organisations away from that culture of reaction and into a culture of accountability. The Act is not concerned only with breach notifications after the event. It is concerned with lawful, fair and transparent processing, adequate security, demonstrable accountability and meaningful remedies where rights are infringed. Incident readiness therefore sits at the heart of the Nigerian data protection framework. The real question is not whether an organisation has an incident response policy somewhere in a shared drive. The real question is whether it can detect, assess, contain, report and remediate a breach in a manner that reflects the duty of care demanded by Nigerian law

2. Incident Readiness under the NDPA and the GAID

Under section 24 of the Act, personal data must be processed fairly, lawfully and transparently, collected for specified purposes, limited to what is necessary, kept accurate and processed in a manner that ensures appropriate security, including protection against unauthorised processing, loss, destruction, damage or any form of data breach. The same section imposes a duty of care and requires controllers and processors to demonstrate accountability. Those provisions are the foundation of incident readiness. They make clear that breach preparedness is not merely an IT concern. It is a legal obligation flowing from the principles of processing themselves.

The governance burden becomes even clearer when the Act is read alongside the GAID. For data controllers of major importance, the Act requires the designation of a Data Protection Officer (‘DPO’) with expert knowledge of data protection law and practice. The GAID then strengthens that role by requiring the DPO to report directly to management, by requiring a semi-annual internal data protection report, and by expecting organisations to maintain internal privacy training schedules, basic privacy checklists and continuous monitoring arrangements for data security systems. In practical terms, that means an organisation that waits for a breach before deciding who owns the response has already failed the maturity test.

Processor governance is equally important. Section 29 of the NDPA requires a controller engaging a processor, or a processor engaging another processor, to ensure that the engaged party complies with the Act, assists with compliance obligations, implements appropriate technical and organisational measures and operates under a written agreement. In the breach context, that provision matters enormously. Many of the most serious personal data incidents do not start in the controller's own environment. They begin with a payroll vendor, cloud host, call centre, digital identity partner, collection agent or software service provider. A breach-response framework that does not speak clearly to third-party escalation, contractual notification timelines, evidence preservation and access to forensic support is incomplete from the outset.

The Act also frames incident response through security and breach notification obligations. Section 39 requires appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data, including resilience, restoration and regular evaluation of controls. Section 40 then requires notification to the Commission within seventy-two hours of becoming aware of a breach that is likely to result in a risk to the rights and freedoms of individuals, while affected data subjects must be notified immediately where the breach is likely to result in a high risk. The GAID develops those duties further by explaining that high risk may arise where a breach could expose a data subject to fraud, identity theft or exposure of sensitive personal data, and by expecting immediate information to relevant authorities where early escalation may help contain harm on a national, sectoral or public scale.

3. Nigerian Case Studies of Data Breach and Exposure

3.1 The NIMC / AnyVerify controversy

One of the most widely discussed data privacy controversies in Nigeria involved allegations that certain third-party platforms were offering access to identity-related records of Nigerian citizens for a fee. Paradigm Initiative reported in 2024 that unauthorised websites were allegedly providing access to personal and financial information for as little as ₦100 per search, following earlier reporting on XpressVerify and similar platforms. The National Identity Management Commission publicly denied that its core database had been compromised and urged the public to disregard those claims.Whether viewed as a direct compromise of the official database or as an ecosystem failure involving uncontrolled verification channels, the controversy exposed a serious governance problem: once third-party access to sensitive identity information becomes weakly supervised, citizens bear the risk long before the regulator is informed.

3.2 The Flutterwave incident

A second example arose from the widely reported unauthorised movement of funds linked to Flutterwave in 2024. TechCabal reported that approximately ₦11 billion was diverted through unauthorised transactions, while the company maintained that customer funds were not compromised in the manner publicly alleged. Whatever label one gives the event, the lesson for incident readiness is straightforward. Not every damaging privacy or security incident will look like a textbook external cyberattack. Workflow abuse, insider collusion, weak approvals and poor segregation of duties can create the same regulatory exposure as a direct technical compromise.

3.3 Government portal exposures

Another area of concern relates to public-facing portals. Investigative reporting in 2025 documented instances in which government-linked websites exposed personal information, including names, addresses, phone numbers, BVNs, bank account details and attendance records. These reports pointed not to sophisticated adversaries alone, but to basic failures of website hygiene, file exposure controls and institutional oversight. In the Nigerian context, that is a sobering point. Sometimes the breach is not hidden in a dark corner of the internet. Sometimes it is sitting in plain sight, indexed by search engines because no one thought carefully enough about what should never have been publicly accessible.

3.4 Compromised digital accounts affecting Nigerian users

The broader threat landscape also matters. Cybersecurity reporting carried by Channels Television in 2025, relying on Surfshark data, stated that at least 119,000 Nigerian user accounts had already been compromised in that year and that Nigeria had recorded more than 23 million compromised accounts since 2004. Even where such figures reflect a mix of domestic and global exposures, they underline a wider point,data breaches affecting Nigerians are not isolated oddities. They are now a recurring feature of the digital environment.

Taken together, these examples reveal an important reality. Data breaches in Nigeria are no longer rare or exceptional events. They are now predictable operational risks embedded in modern information systems.

4. Comparative Insights: Lessons from the GDPR Incident Response Model

Any serious examination of Nigeria's emerging data protection regime benefits from a comparative glance at the Global Data Protection Regulation (GDPR), which remains one of the most influential privacy frameworks in the world. One of its most notable features is the structured breach notification regime in article 33, which requires notification to the relevant supervisory authority within seventy-two hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Article 34 complements that duty by requiring communication to affected data subjects where high risk arises.

Equally important is the GDPR's accountability principle. The expectation is not merely that an organisation should obey the law in substance, but that it should be able to demonstrate compliance through documentation, internal measures, governance structures and records. The European Data Protection Board's guidelines on personal data breach notification reinforce this by stressing the need to document all breaches, assess risk carefully arnd act promptly even where all facts are not yet fully available. That logic is plainly reflected in the Act and the GAID, particularly in their emphasis on duty of care, internal reporting, breach records, DPO governance and demonstrable organisational controls.

The same is true of privacy by design and by default. Article 25 of the GDPR requires controllers to integrate data protection safeguards into systems and processing activities from the earliest stages of development and, by default, to process only the personal data necessary for each purpose.

5. Regulatory Trends and the Evolving Enforcement Posture of the NDPC

Since the enactment of the Act, Nigeria's data protection landscape has moved from basic awareness-building into a more visibly enforcement-oriented phase. The statute itself gives the Commission substantial powers to investigate, issue compliance orders, make enforcement orders and impose sanctions, including remedial fees that may reach the greater of ₦10 million or 2% of annual gross revenue for controllers or processors of major importance.

Recent reporting suggests that the Commission is increasingly willing to use that architecture. In August 2025, African Law & Business reported that the Commission had initiated investigations targeting over 1,000 organisations for suspected breaches of the Act. In February 2026, Reuters reported that the Commission had opened a probe into Temu over alleged data protection violations, while also noting the Commission's earlier fine against Multichoice Nigeria. Even if Nigeria's enforcement record is still developing compared with mature European regulators, the direction of travel is now clear enough. Organisations should assume that the era of soft-touch privacy compliance is ending.

That shift matters for breach readiness. When enforcement becomes more active, undocumented response processes, untested incident playbooks and casual vendor oversight become far harder to defend. In other words, breach-response maturity is no longer a matter of best practice alone. It is increasingly a matter of regulatory prudence.

6. Risk-Based Incident Readiness Strategies for Organisations

If incident readiness is to meet the Commission's expectations, it must be riskbased, not cosmetic.

First, organisations need a clear data classification framework that separates routine personal data from higherrisk categories such as biometrics, identity credentials, financial information, health records, and children's data. Without proper classification, incident triage becomes guesswork.

Secondly, organisations should run incident response simulations. Tabletop exercises reveal hesitation, confusion, and hidden weaknesses in a way no policy document ever can. A response plan that has never been tested is, in reality, no plan at all.

Thirdly, third-party risk management must sit at the centre of incident readiness. Processor contracts should contain explicit obligations on escalation timelines, cooperation, preservation of evidence, visibility over subprocessors, and audit support. Due diligence should not end at onboarding; it must continue throughout the relationship.

Fourthly, organisations should adopt continuous monitoring and audit practices. The GAID does not envisage a oneoff compliance effort followed by institutional sleep. It expects ongoing monitoring, evaluation, and maintenance of security controls, alongside continuous privacy training and practical guidance for staff and contractors.

Finally, data protection must be embedded within enterprise risk management and overseen at board level. The most effective organisations do not treat privacy as a narrow legal issue. They recognise it as a governance matter that touches operations, technology, procurement, HR, customer trust, and regulatory exposure.

7. What to Do Before, During and After a Breach

A practical Nigerian breach-response framework can be understood in three stages:

7.1 Before the breach

Before any incident occurs, the organisation should know what data it holds, where it is stored, which systems and vendors touch it, which processing activities are high risk, and who has authority to make breach decisions. The DPO, legal team, security function, operations owners and senior management should have defined roles. Notification templates, escalation paths, media holding lines, processor contacts and evidence-preservation steps should be settled in advance. Staff should know that where personal data is misdirected, exposed or unlawfully accessed, silence is not caution; silence is delay.

7.2 During the breach

Once an incident is suspected, the immediate priorities are containment, fact-finding and risk assessment. Access may need to be suspended, credentials revoked, systems isolated and vendors contacted. The organisation must establish what happened, what data is involved, who may be affected, and whether the incident creates risk or high risk to rights and freedoms. The statutory seventy-two hour window should be treated as a hard outer boundary, not a comfortable planning period. If early notice to the Commission or other relevant authorities may help to contain imminent harm, the GAID points towards prompt escalation.

7.3 After the breach

After containment and notification comes the phase that often determines how the incident will be judged. The organisation should conduct a root-cause analysis, verify the effectiveness of remedial measures, review any processor failure, update relevant DPIAs, retrain staff where necessary and document lessons learned. Breach logs, management reports and DPO reporting should show not merely that the incident occurred, but that the organisation responded in a way consistent with accountability and duty of care. If the same weakness is left in place after the event, the organisation has not really remediated anything.

8. Conclusion

The expansion of Nigeria's digital economy has created valuable opportunities for innovation, financial inclusion, administrative efficiency and improved service delivery. At the same time, it has generated complex privacy risks associated with large-scale personal data processing by both public and private institutions. The real test of Nigeria's data protection regime will therefore lie not only in the strength of the statute, but in the

willingness of organisations to internalise privacy governance as part of day-to-day operations.

Institutions that invest in strong breach-response systems, clear governance lines, tested incident playbooks, disciplined vendor management and risk-based monitoring will be better placed to navigate the Commission's evolving expectations. More importantly, they will be better placed to preserve trust. In the digital economy, trust is no longer a soft value. It is a hard regulatory asset.

References

• Nigeria Data Protection Act 2023.
• General Application and Implementation Directive 2025 (20March 2025).
• Nigeria Data Protection Commission, Guidance Notice on the Registration of Data Controllers and Data Processors of Major Importance (19 December 2024).
• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
• European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under GDPR (Version 2.0, 4 April 2023).
• National Identity Management Commission (NIMC), 'Press Statement - NIMC Denounces Allegations of Data Compromise' (NIMC, 2024).https://technext24.com/2024/06/22/nimc-denounces-data-compromise/ accessed 20th March 2026
• African Law & Business, 'Nigeria Launches Widespread Probe into Data Protection Violations' (28 August 2025).https://www.africanlawbusiness.com/news/nigeria-launches-widespread-probe-into-data-protection-violations/accessed 20th March 2026
• Paradigm Initiative, 'Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira' (20 June 2024).https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/ accessed 20 March 2026
• TechCabal, 'Exclusive: Flutterwave Loses ₦11 Billion in Security Breach' (16 May 2024) https://techcabal.com/2024/05/16/exclusive-flutterwave-loses-%E2%82%A611-billion-in-security-breach/ accessed 20 March 2026.
• Foundation for Investigative Journalism, 'How CBN, Edo, Other Govt Sites Leak BVNs, Personal Data of Nigerians' (28 July 2025) https://fij.ng/article/how-cbn-edo-other-govt-sites-leak-bvns-personal-data-of-nigerians/ accessed 20 March 2026.
• Channels Television, 'Nigeria Records at Least 119,000 Data Breaches in Q1 2025 - Report' (10 May 2025) https://www.channelstv.com/2025/05/10/nigeria-records-at-least-119000-data-breaches-in-q1-2025-report/ accessed 20 March 2026.
• Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
• European Data Protection Board, Guidelines 9/2022 on Personal Data Breach Notification under General Data Protection Regulations (Version 2.0, 4 April 2023)https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf accessed 20 March 2026.

• African Law & Business, 'Nigeria Launches Widespread Probe into Data Protection Violations' (28 August 2025) https://www.africanlawbusiness.com/news/nigeria-launches-widespread-probe-into-data-protection-violations/accessed 20 March 2026.
• Reuters, 'Nigeria Opens Probe into Temu over Suspected Data Protection Breaches' (18 February 2026) https://www.reuters.com/sustainability/boards-policy-regulation/nigeria-opens-probe-into-temu-over-suspected-data-protection-breaches-2026-02-17/ accessed 20 March 2026.

Disclaimer:

The information provided in this publication does not, and is not intended to constitute legal advice. It is intended for general informational purposes only. Please contact us for further information.

Lagos Office: No 13, Mustapha Street, Off Olanrewaju Street, Billingsway, Oregun, Ikeja, Lagos.
Abuja Office: No. 16, Nkwere Street, Area 11, Garki, Abuja, FCT.
Email: info@syntegrallp.com
Telephones: 08025754547, 08023007172, 07015694060

© Copyright 2026 - Syntegral Legal Practice