

After the *Breach*

Legal Strategies for Response,
Recovery, and Resilience



Contributors



**Okechukwu
Ekweanya**

Partner, Dispute
Resolution & ADR



Sonia Onyia

Associate, Dispute
Resolution & ADR



Okenna Onyelu

Associate, Dispute
Resolution & ADR

For further information on the issues discussed in this article,
contact our legal team at counsel@kennalp.com

Introduction

A data breach is described as unauthorised access, disclosure, or theft of private and sensitive information. Data breaches may take various forms, such as cyberattacks, internal threats, and accidental data releases. In summary, data breaches result in the compromise of the confidentiality and integrity of the information concerned, and the consequences may extend beyond the actual data itself. In modern times, where technology is used extensively for commercial purposes, data plays a critical role in strategic planning and development, and as such serves as a source of market power. Nonetheless, the use of technology has brought with it major cyber threats, resulting in the leak of sensitive information about the individuals concerned and, as such, posing great dangers to their finances and reputations.

In light of the foregoing, this article explores data breaches and analyses the requisite procedures for responding to breaches in accordance with applicable data protection laws in Nigeria, as well as the preventive measures necessary to safeguard controlled personal data.

"In a digital economy, data is market power — and its compromise is no longer a remote risk, but a predictable cost of doing business."

Responding to Data Breaches

There are various stringent data protection requirements that organisations must comply with, such as ensuring fair processing, employing a data protection officer when required, and implementing necessary measures after a data breach. All these requirements aim at protecting the constitutional right to privacy and the rights of other data subjects. In case of data breach, time becomes an enemy. Organisations need to be proactive in containing damage, protecting data subjects, and meeting legal requirements as per the provisions of the Nigeria Data Protection Act (NDPA) and the General Application and Implementation Directive (GAID). After a data breach in an organisation, the organisation must implement the following steps immediately:

Initial Notifications: When a breach is detected, the organisation involved is expected to promptly notify the data controller, describing the nature of the personal data breach, including, where possible, the categories and approximate numbers of data subjects and personal data records concerned¹ Furthermore, the law prescribe that an additional notification must be made to the Nigeria Data Protection Commission within 72 hours of becoming aware of the breach if the breach is likely to pose a risk to the rights and freedoms of individuals.²

Additional Notifications: Data breaches may escalate to circumstances where it is likely to result in a high degree of risk to the rights and freedoms of data subjects. In such an instance, the organisation is required to notify the data subject without delay, including information on how the data subject can mitigate the risk of harm. Where direct notification is not feasible, the organisation can notify the public through widely used media.³ This is an important step to enable data subjects to promptly change passwords, delete sensitive data or take other protective measures to guard their personal data.

Record Keeping: Organisations are mandated to maintain adequate records of all personal data breaches and the effects and remedial actions taken.⁴ This is important to analyse the impact when rectified and take steps to prevent future occurrences.

Statutory Reporting Threshold

72h

Maximum time from awareness of breach to mandatory notification of the Nigeria Data Protection Commission, where risk to data subjects is likely.

Source · NDPA & GAID

Preventive Measures to Safeguard Data

In 2021, popular social media platform LinkedIn experienced a data breach involving the large-scale scraping of publicly accessible user data affecting approximately 700 million users of LinkedIn, where information such as names, emails, phone numbers, and professional details was aggregated and circulated online.⁵ LinkedIn responded by investigating the incident, blocking scraping activities, and improving detection systems, but faced criticism for prioritising technical classification over user-centred protections such as prompt notification and enhanced privacy controls. The breach had reputational consequences, weakened user trust, and intensified regulatory scrutiny of data practices. Critically, the case highlights the evolving nature of data breaches beyond traditional hacking and underscores the need for proactive safeguards under the *privacy by design* principle to prevent foreseeable misuse of personal data.

Given the nature of current data breaches, which not only affect information but also reveal inherent weaknesses within organisations, present-day laws have made it compulsory for businesses to adopt a forward-looking approach to information security rather than merely focusing on compliance. This means adopting a privacy by design strategy, in which privacy considerations and measures are embedded within systems and technology itself in order to ensure effective processing of personal data as per regulatory norms. This model relies upon the high standards of legal and regulatory regimes, considering factors like data minimisation, data protection, transparency, and consent while increasing privacy, building up consumer confidence, and complying with regulations. Some of the difficulties associated with adopting privacy by design include high initial costs, complex implementation processes, limited use of legal data, and mere compliance without achieving intended objectives. Nevertheless, the model may be implemented through:

Pillars of Privacy by Design

Data minimisation · data protection · transparency · consent.

Embedded security into data:

Data is capable of restricting access to itself if ringfenced with encryption structures that ensure that any attempt to infiltrate an organisation's data system is rendered useless because the data itself cannot be accessed. A good example of such a preventive measure is encryption, which converts original data into complex text that can only be deciphered with the right key/ password. It ensures the confidentiality, integrity, and availability of information required to protect against illegal cyber threats. Without encryption, critical data may be easily accessible to cyber attackers who can then use the information as they see fit. The 2017 Equifax attack serves as an example of how a lack of strong encryption standards led to massive personal and financial information breaches of more than 150 million users. The company incurred heavy losses of up to \$400 million due to this attack.⁶

Organisational culture shift:

Prevention of data breaches cannot be achieved by technology alone. Organisational culture is one of the most important factors that influence success or failure in the security domain. Even the most advanced encryption methods can be compromised by insecure credential handling, weak passwords, and susceptibility to phishing attacks. Hence, it is important that organisational leadership is committed to security. In accordance with Article 39 of the General Data Protection Regulation (GDPR), Data Protection Officers are expected to provide training to data processing personnel to ensure they understand their roles in safeguarding the data they process. Moreover, efforts aimed at ensuring the employees remain aware and educated about the need to safeguard data, as well as the risks associated with the breach of data, even in minute ways, will help prevent such breaches.

Case in Point · Equifax · 2017

A lack of strong encryption standards led to one of the largest financial-data breaches on record.

Users Compromised

150M+

Personal & financial records exposed.

Direct Losses Incurred

\$400M

Borne by Equifax following the attack.

Data minimisation practices:

Organisations are typically fond of collecting as much data as possible to store, monetise or exploit in the future. At its core, data minimisation is a practice that requires organisations to collect only the data necessary to provide their services. Minimising data is collecting data only for an immediate and necessary purpose, not hoarding the data on the “off-chance that it might be useful in the future.”⁷ This does not mean companies should not collect data at all; rather, it makes them responsible for adhering to the principles of adequacy, relevance, limitedness and timeliness.⁸ While collecting personal data, the organisational responsibility comes with ‘data classification’ that helps better define the data, and decide which personal data is commensurate with the intended purposes or services. For example, in the case of a medical service, gender may be more relevant than religion or ethnicity. Consequently, the determination of what data is absolutely necessary is the first step in a successful data minimisation strategy. This practice is equally consistent with the NDP Act, GAID, and GDPR, which provide that only data necessary and relevant to the purpose for which it is processed should be collected from data subjects.⁹

Appointment of a Data Protection Officer (DPO):

It is mandatory for data controllers of major importance to employ or appoint a DPO who will serve as a chief advisor and compliance monitor regarding data protection in the organisation. In essence, the data controller must interact with their appointed DPO on all matters related to data protection and guarantee that the latter does not carry out their mandate under coercion or fear of punishment. It is recommended that organisations capitalise on this regulation by utilising the expertise of professionals to inform them about measures necessary in terms of prevention and reaction to any data breaches.

Data Deletion:

Where the purpose for which personal data was collected has been fulfilled, organisations should adopt data deletion practices, which involve the permanent removal of digital data from storage in order to protect privacy and ensure compliance with applicable legal obligations.

Chief Advisor

Counsels leadership on legal obligations.

Compliance Monitor

Tracks adherence to NDPA & GAID.

Independent

Acts without coercion or sanction.

Conclusion

Data breaches can no longer be considered a rarity; rather, they are a predictable consequence of operating within a growingly digital commercial environment. With the continued adoption of data as a means of catalysing innovation and efficiency, the legal and practical consequences of data breaches have become more evident. The provisions stipulated by the NDP Act and GAID require strict adherence to certain obligations, particularly during the first 72 hours following a breach.

However, compliance cannot be pursued only reactively. Effective data protection is proactive, holistic, and should be embedded into the organisation's culture. Data protection is more than just complying with regulations; rather, it represents a strategic requirement, since organisations that take proactive steps in governance and breach prevention put themselves in a favourable position to protect the rights of their data subjects, earn their trust, and succeed in an ever-changing digital world.

“Effective data protection is proactive, holistic, and should be embedded into the organisation's culture.”

1. NDP Act, Section 40(1)(a).
2. NDP Act, Section 40(2).
3. NDP Act, Section 40(3).
4. NDP Act, Section 40(8).
5. Lizzi Danielson, 'LinkedIn Data Scraping Incident', (2021), <https://www.huntress.com/threat-library/data-breach/linkedin-data-breach> accessed April 23 2026.
6. Data Guard, 'Cyber security and encryption: Best practices for your business', (2026) <https://www.dataguard.com/blog/cyber-security-measures-secure-your-business-with-encryption/>, accessed February 19, 2026
- 7.
8. Joe Maurer, "What is data minimisation? Definition, benefits and best practices", (2025), <https://matomo.org/blog/2025/10/data-minimisation/>, accessed April 10, 2026.
9. NDP Act, 2023, Section 24(1)(c), GAID, Article 4(1)(c), GDPR, Article 5(1)(c).



CONTACT US

LAGOS

KENNA Place
8, Ogunyemi Road, Palace Way,
Oniru PO Box 73002,
Victoria Island, Lagos

ABUJA

1st Floor, Novare Central
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285,
Abuja

ENUGU

Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner,
400211 Enugu State.

+234 811 395 1052, +234 811 395 1053 | counsel@kennalp.com