BEYOND THE BREACH: CRAFTING EFFECTIVE DATA SECURITY MEASURES

By: Olayinka Alao & Chinelo Obiekwe

INTRODUCTION

In our increasingly digital world, data breaches have become a significant concern for businesses worldwide, and Nigeria is no exception. The surge in digital platform usage and data proliferation has heightens the risk of unauthorized access to personal data. To address these challenges and protect personal data, the Nigeria Data Protection Act 2023 ('NDPA" or "the Act') was enacted, building on the foundational principles set by the Nigeria Data Protection Regulation (NDPR) of 2019.

The NDPA and the NDPR outline stringent obligations for organizations to ensure both the lawful processing of personal data and its protection, along with outlining responsibilities in the event of a data breach. Given that data breaches can result in severe and irreparable financial, legal, and reputational harm to data subject, it is essential for data controllers[1] and data processors[2] in Nigeria to create and implement effective data breach response strategies to ensure confidentiality, integrity and availability of personal data.

This article explores the legal guidelines for managing data breaches and emphasizes the safeguards and best practices that businesses in Nigeria should adopt. By doing so, it aims to assist businesses in aligning their operational processes with the NDPA's provisions, thereby protecting their operations and maintaining the trust of their stakeholders.

DATA BREACH EXPLAINED

The Act specifically defines a 'Personal Data Breach' as any security breach involving a data controller or processor that results in, or is likely to result in, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that has been transmitted, stored, or otherwise processed.[3] Simply put, a data breach occurs when personal data is accessed

[1] Data controller is an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data (See, Section 65 of the NDPA, 2023).

[2] Data processor is an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor (See, Section 65 of the NDPA, 2023).

[3] Section 65 of the Nigerian Data Protection Act, 2023. See also Article 1.3 of the NDPR on the definition of Personal Data Breach.

unlawfully and/or without authorization, compromising the data's confidentiality, integrity, or availability.

Under the Act, data controllers are legally responsible for the personal data under their care and must implement strong and effective measures to protect this data during processing or storage.[4] Despite these precautions, data breaches can still occur, sometimes as a result of deliberate sabotage such as cyber-attacks, phishing or insider threats, and other times due to unintentional actions or negligence such as human errors, or system vulnerabilities.

According to Surfshark, a leading cybersecurity firm, the frequency of data breach incidents in Nigeria saw a significant increase of 64% in the first quarter of 2023, with the number of cases rising to 82,000 from 50,000 in the last quarter of 2022.[5]

RESPONSIBILITIES OF ORGANIZATIONS IN MANAGING DATA BREACHES

The NDPA and the NDPR provide detailed rules on how organizations should respond to and manage personal data breaches, as follows:

A. Surveillance

For effective data breach response and mitigation, time is of the essence. This is because prompt discovery of a data breach enhances the ability of the data controller to limit both the extent and the impact of the breach. Recognizing this critical factor, the NDPA and NDPR mandate that data controllers regularly review their data protection frameworks, implement multi-layered protection strategies, educate employees on data security, and establish policies that encourage staff to report any suspected data breaches.[6] Data controllers are required to invest in technology capable of monitoring access to and authorization of all personal data they hold, providing early alerts of any potential or actual breaches.[7]

B. Data Breach Report

In the event of a personal data breach, the data processor, upon becoming aware of the breach, must notify the data controller or the data processor that engaged it, and respond to all information requests from them.[8]

---

[4] See Sections 24(1)(f)

[5] < https://guardian.ng/business-services/nigeria-suffers-64-data-breach-in-q1-ranks-32-globally/> accessed June 13, 2024

[6] See Section 39(1) of the Act and Article 2.6 of the NDPR

[7] Ibid

[8] Nigerian Data Protection Act, Section 40 (1)

It is important to understand that within the framework of the Act, a data processor acts as an agent for the data controller, handling personal data on their behalf. While the data processor is accountable to the data controller for the personal data it processes, the data controller remains directly and personally accountable to both the data subjects and the Nigeria Data Protection Commission ("the Commission"). This includes data that the data processor handles on behalf of the data controller.

Furthermore, the Act stipulates that a data controller must notify the Commission within seventy-two (72) hours of becoming aware of a breach that poses a potential risk to the rights and freedoms of individuals. This notification should, where feasible, detail the nature of the personal data breach, including the categories and approximate number of data subjects and personal data records affected.[9]

Communication with Data Subjects After a Data Breach

When a personal data breach presents a high risk to the rights and freedoms of a data subject, the Act mandates that the data controller must quickly inform the affected individuals in plain and clear language.[10] This communication should include guidance on steps the data subject can take to mitigate the potential adverse effects of the breach. If direct communication with the data subjects is impractical due to disproportionate effort or expense, the data controller may opt for a public announcement via one or more widely used media platforms to ensure the affected individuals are likely to become aware of the breach.[11]

In determining whether a personal data breach could likely pose a risk to the rights and freedoms of a data subject, the Act allows both the data controller and the Commission to consider various factors. These include:

(a) The effectiveness of existing technical and administrative measures to mitigate harm, such as data encryption or the de-identification of data.
(b) Any additional measures taken by the data controller post-breach to reduce risk.
(c) The nature, scope, and sensitivity of the personal data involved in the breach.[12]

[9] Ibid. Section 40 (2).
[10] Ibid. Section 40(3) and Paragraph 12 of the Implementation Framework issued pursuant to the NDPR
[11] Ibid. Section 40 (3) & (4)
[12] Ibid. Section 40 (7)

C. Data Breach Register Requirements

The Act requires data controllers to maintain a comprehensive register of all personal data breach incidents.[13] This record must include:

(a) facts relating to the personal data breach;

(b) effects of the breach; and

(c) remedial actions taken by the controller after the breach.

Maintaining a detailed record of data breaches serves two crucial purposes. Firstly, it provides the Commission with valuable information about the nature and scale of the breach, which is essential during regulatory investigations. Secondly, it allows organizations to learn from past incidents, helping them enhance their data protection strategies and mitigate future risks.[14]

ENHANCING DATA BREACH RESPONSE AND MITIGATION: PRACTICAL RECOMMENDATIONS

To effectively meet the demands of the NDPA and NDPR, organizations should put in place thorough data breach detection and response mechanisms. Here are some practical steps that can be taken:

- **Periodic Data Protection Impact Assessment and Audits**: Conducting Data Protection Impact Assessments (DPIAs) for activities involving high-risk data processing is crucial. These assessments help businesses proactively pinpoint and address potential vulnerabilities. Similarly, regular data protection audits, typically conducted annually, allow organizations to consistently evaluate their compliance with the NDPA and NDPR, identify any shortcomings, and take necessary corrective actions.
- **Development of a Response and Mitigation Strategy**: It is advisable for businesses to develop and implement detailed incident response plans that clearly define employees' roles and responsibilities in the event of a data breach. This ensures adherence to the NDPA and NDPR requirements. The breach response strategy should be documented and disseminated among staff to ensure their understanding and compliance. Regular reviews and updates of this data breach policy are essential to accommodate regulatory changes and evolving security threats.

[13] Ibid. Section 40 (8)

- **Staff Training and Capacity Building**: In today's digital landscape, where data breaches are increasingly common, educating employees about data protection principles, breach detection, and their specific responsibilities during an incident is vital. Ongoing training and education improve staff awareness and preparedness, equipping them to better handle potential breaches.
- **Professional Advisory and Support**: Data privacy is a specialized area that often requires expert advice and guidance. Businesses might find it beneficial to consult with licensed Data Protection Compliance Organizations (DPCOs). These organizations are recognized under the NDPA and NDPR as licensed entities authorized to offer advisory and compliance services to businesses, helping them navigate the complexities of compliance.[15]

CONCLUSION

While many data breaches are preventable, they remain a stark reality in the digital age. Even with the most stringent security measures in place, breaches can still occur. Therefore, beyond just safeguarding personal data, businesses must also have effective data breach response and mitigation strategies ready to deploy when needed.

As a licensed Data Protection Compliance Organization (DPCO), we understand the complexities that businesses face in managing data breach responses and mitigation. For more information on data audits, compliance training, or to discuss data protection compliance needs, please reach out to us at info@scp-law.com.

[15] See Section 33 of the NDPA and Article 1.3 of the NDPR