



UDO UDOMA &
BELO-OSAGIE



DATA BREACHES:
COMPLIANCE OBLIGATIONS
UNDER THE NIGERIAN DATA
PROTECTION ACT 2023



Introduction

Data breaches are now a regular occurrence in the modern data-driven and digital global economy that the world has now become. A number of organisations have suffered data breaches in the course of their operations with differing degrees of seriousness. These breaches have resulted in the personal information under the custody of these organisations becoming compromised and unduly exposed to third parties with malicious motives, thereby creating potential risks for the affected individuals. Nigeria, a country with an estimated population of over 200 million people making it a fertile ground for data breaches, has also experienced cyber incidences that have affected both government institutions and corporate entities. Such cyber-attacks have led to the unauthorised exposure of personal data under the control of such institutions or corporate organisations. Surfshark, a cybersecurity firm, reported that data breach incidences in Nigeria increased by 64% in Q1 of 2023, recording 82,000 cases of data breaches in Q1 2023, up from 50,000 recorded in Q4 2022.¹

A data breach occurs when the data under an organisation's control suffers a security incident that results in a breach of the confidentiality, availability, or integrity of such data- including personal data.

In this article, we will examine the legal framework governing personal data breaches under the data protection laws in Nigeria.

What is a Data Breach?

In Nigeria, data protection and privacy are governed by the Nigerian Data Protection Act 2023 ("NDPA" or "Act"), which was signed into law on 12th June 2023.

The NDPA contains provisions that govern data breach events and stipulates the steps organisations are required to take when they suffer data breaches.

Personal data breach under the NDPA is defined to mean a breach of security of a data controller or data processor leading to or reasonably likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

¹ Adeyemi Adepotun, 24 May 2023, "Nigeria suffers 64% data breach in Q1, ranks 32 globally", *The Guardian*, <https://guardian.ng/business-services/nigeria-suffers-64-data-breach-in-q1-ranks-32-globally/>



This infers a situation where, due to a breach in security, an organisation (either as a controller or processor) suffers some form of unlawful destruction, loss, alteration or disclosure of the personal data under its control. Where an organisation suffers a data breach, the NDPA stipulates certain obligatory steps such organisations must take. We will closely examine the various steps as we go further in this article.

How do organisations suffer data breaches?

Organisations can suffer data breaches directly, that is, where the data breach occurs on personal data in the organisation's possession whilst it is undergoing processing, storage or in transit. Organisations can also suffer data breaches indirectly, where, though the data is not in the organisation's possession, such data is breached in the course of being processed by a third party acting on the controller's instruction. In this instance, while the data processing or storage infrastructure of the controller has not in itself been compromised, the personal data that is under the control of the data controller has been impacted by a breach since the data processor processed the personal data on the controller's instruction. The two scenarios mentioned above are envisaged under the NDPA, and the NDPA has provisions stipulating what organisations should do in such circumstances.

What are the obligations of the data processor in the event of a data breach?

In relation to the instances where a data controller suffers a data breach indirectly, that is, where the breach is suffered by a data processor who processed the personal data on the controller's instruction, the data processor is required to assess the situation and provide adequate information to the controller. Section 40 (1) (a) and (b) of the NDPA provides that where a personal data breach has occurred concerning personal data being stored or processed by a data processor, the data processor shall, on becoming aware of the breach-

- (a) notify the data controller or data processor that engaged it, describing the nature of the personal data breach, including, where possible, the categories and approximate numbers of data subjects and personal data records concerned; and
- (b) respond to all information requests from the data controller or processor that engaged it, as they may require such information to comply with their obligations under the NDPA.



What steps should organisations that have suffered a data breach take?

Where an organisation suffers a data breach, it is expected that, as a first step, the organisation will take all steps necessary to stop the breach where possible. This means that the organisation must first take steps to address the personal data breach and mitigate the adverse effects of the personal data breach to reduce the likelihood of harm to individuals or data subjects whose personal data has been breached. The appropriate remedial action would depend on the nature of the breach. For instance, the controller could typically try to make the data inaccessible or unintelligible for third parties where they have accessed such data unauthorisedly. Where the data has been altered or compromised, the controller would typically take steps to restore the availability and accuracy of the data.

Is there any reporting obligation to a data protection authority?

Where a data controller suffers a data breach, there are specific reporting obligations that such data controller must carry out depending on the perceived impact of the personal data breach. Where the data breach is such that is required to be reported, such notification is to be made by the data controller to the Nigeria Data Protection Commission (“NDPC”). The NDPC, which was established under the NDPA, is now the data protection authority for Nigeria and has taken over the function of the Nigeria Data Protection Bureau (as it was formerly known).

What types of personal data breach should be reported?

Under the Nigeria Data Protection Regulation 2019 (“NDPR”), there was an obligation on data controllers to report all types of personal data breaches to the data protection authority. The NDPA has moved away from this position. Under the NDPA, data controllers are now only required to report data breaches where such data breaches will result in a risk to the rights and freedoms of the data subjects. There is no obligation to report a data breach that will not result in a risk to the rights and freedoms of the data subjects.

What can be considered to be a risk to the rights and freedoms of data subjects?

There are three factors that data controllers and processors are required to consider in determining whether a data breach will result in a risk to the rights and freedoms of data subjects. These are (a) the likely effectiveness of the measures (technical and administrative) that are implemented to mitigate the likely harm or adverse effect of the personal data breach; (b) any subsequent measures taken by the data controller to mitigate such risk; and (c) the nature, scope, and sensitivity of the personal data that was involved in the breach.



Where, based on these considerations, the data controller is of the view that the personal data breach will result in a risk to the individuals whose data have been disclosed, the controller is required to report to the NDPC.

Is there a timeline for reporting a data breach?

Under Section 40 (2) of the NDPA, data controllers are required to notify the NDPC within 72 hours after they become aware that they have suffered a breach that is required to be reported under the Act. Where it is impossible for the data controller to provide all the required information regarding the data breach to the NDPC within the said timeline, the data controller may provide the information to the NDPC in phases.

Is there an obligation to communicate with the affected data subjects?


Based on the provisions of section 40 (3) of the NDPA, where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the data controller is required to communicate the personal data breach to the data subjects immediately. The communication should also include the measures the data subject could take to mitigate the possible adverse effects of the data breach. Where direct communication to the data subject would involve disproportionate effort or expense, the data controller may make public communication using one or more widely used media channels.

The NDPC also has the power to make public communication about a personal data breach that has been brought to its notice, where it considers the steps the data controller has taken to inform data subjects of the breach are inadequate.

Is there an obligation to keep records of data breach incidents?

To demonstrate compliance with their obligations under the NDPA, data controllers must keep a record of all personal data breach incidents. The record should include the facts relating to the personal data breach, its effects, and the remedial action taken by the controller after the occurrence of the breach. The record will enable the NDPC to confirm whether the controller complied with its obligations under the Act.²

² Section 40 (8) of the NDPA.



Failure to comply with the NDPA, where an organisation suffers a data breach, can expose the organisation to regulatory sanctions such as monetary fines and criminal prosecution of its senior officers.³ There is also a risk of reputational damage to the organisation.

Recommended actions that organisations that have suffered data breaches can take include:

1. Locate and secure the source of the breach to prevent further unauthorised access or disclosure of personal data.
2. Determine the extent of the breach and confirm the obligations of the organisation under the Act.
3. Engage a licensed Data Protection Compliance Organisation (DPCO) to advise your organisation and assist it in complying with its obligations under the NDPA.
4. Engage data security experts/professionals to evaluate your organisation's architecture and advise on improving data security.

Penalties for non-compliance with obligations in the event of a data breach

Non-compliance by data controllers and processors with the obligations stipulated in the NDPA in the event of a data breach is an infraction of the provisions of the NDPA, which attracts fines and possible criminal action against the defaulting data controller or processor. Under the NDPA, Data Controllers or Processors of Major Importance ("DCPMI") that are found to have breached the provisions of the Act may be subject to the payment of a fine of whichever is greater between the sum of N10,000,000 or 2% of its annual gross revenue from the preceding financial year. Similarly, other data controllers or processors may be liable to pay a fine of whichever is greater between the sum of N2,000,000 or 2% of their annual gross revenue from the preceding financial year.

Conclusion:

The NDPA imposes specific obligations on data controllers and processors where they suffer data breaches. This article has summarised these obligations to enable organisations, at a glance, to be guided on how to respond and ensure they are compliant with applicable laws where they suffer data breaches.

UUBO is a licensed DPCO, and our data protection practice group offers a wide portfolio of data protection services. With a team of seasoned professionals with decades of data protection experience, we offer bespoke services to our clients across a broad spectrum. If you require any assistance or clarification regarding your obligations when dealing with a data breach under the NDPA or information about our practice area offerings, please contact us at: dpteam@uubo.org.

³ Regulation 10 of the NDPR Implementation Framework