Data Breach Management, Notification, and Incident Response: Practical Implications for Businesses and Organizations in Nigeria under the Nigeria Data Protection Act 2023.

**Uche Val Obi, SAN with Samuel Uzoigwe and Doyin Fadare*[1]

Introduction

The Nigeria Data Protection Act 2023 ("the NDPA") imposes several duties and obligations on businesses and organizations (whether a data controller or data processor). One of these is the obligation to report a personal data breach when such breach meets a certain reporting threshold. The NDPA defines Personal data breach as *"a breach of security of a data controller or data processor leading to or likely to lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."*[2] A personal data breach is not synonymous with a security incident . A security incident in data protection parlance is an event such as a malware attack, inadvertence of an employee, etc., that potentially puts personal data at risk for unauthorized exposure.[3] A security incident may be neutralized before any damage is caused, or personal data is compromised. Therefore, not all security incidents will lead to a personal data breach, and for a security incident to amount to a personal data breach, either one or all of the events in the above definition must have occurred. By virtue of the NDPA, not all personal data breach will create a reporting obligation for data controllers and processors. A data breach reporting obligation depends on a variety of factors and the business or organization involved.

In view of the intricacies surrounding personal data breach notification obligations, a data controller or data processor's ability to adequately fulfil this obligation is premised on the existence of adequate procedures and controls to ensure the health of personal data in its custody, monitor its use and location, and cultivate adequate compliance with the NDPA.

Types of Personal Data Breach

The NDPA does not categorize personal data breach into types, but drawing examples from other jurisdictions, personal data breach under the NDPA can be categorized using these three security principles - confidentiality, integrity and availability of personal data - as well as any combination of these.[4] This categorization helps in better understanding personal data breach.

---

[1] Uche Val Obi, SAN and Samuel Uzoigwe are Managing Partner and Executive Associate respectively at Alliance Law Firm, Lagos while Doyin Fadare was an Executive Associate at the same firm.

[2] Section 65, NDPA.

[3] Mahmood Sher-Jan, IAPP, https://iapp.org/news/a/is-it-an-incident-or-a-breach-how-to-tell-and-why-it-matters/ accessed August 15, 2023.

[4] Guidelines 9/2022 on personal data breach notification under GDPR, page 8, available at https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf accessed August 15, 2023.

Confidentiality Breach

This is where there is an unauthorized or accidental disclosure of, or access to personal data breach.[5] An example of this type of personal data breach is where an employee inadvertently sends personal information of data subjects to unauthorized email recipients. Similarly, where malicious actors through phishing or any other social engineering technique, gain access to the financial, residential or health records of a data subject, this qualifies as a confidentiality breach.

Integrity Breach

This kind of personal data breach involves the accidental or unauthorized alteration of personal data. An example is where a database containing a patients critical health information is altered. This may lead to catastrophic consequences for such patient if the altered information is relied on to render medical services to the patient. Another illustration is where the email address or mobile phone number of a data subject with a financial institution is altered, causing the data subject to lose the ability to properly secure their account using two-factor authentication purposes.

Availability Breach

This involves the accidental or unlawful destruction, or loss of access to personal data. Where personal data stored in the cloud is deleted accidentally or by unauthorized parties, it amounts to a personal data breach. An example is a significant disruption to the normal service of an organization, for instance, a power failure or denial of service attack, or infection from a ransomware rendering personal data temporarily or permanently unavailable.[6]

A personal data breach can occur in either of the above forms, or a combination of any or all of the above forms.

Identifying Personal Data Breach

Identifying whether a personal breach has occurred is key to a data controller or processor's data breach management process, and breach notification obligations, as it determines when a data controller or processor becomes "aware" of a personal data breach. Knowledge of a data breach may be instant to a data controller or processor, or it may take some time and investigation to confirm if there has been a personal data breach. It could also concern personal data stored in physical or virtual storage facilities or any other form of storage.

An apt example[7] is a case where a USB key with unencrypted personal data is lost. It is often not possible to ascertain whether unauthorized persons gained access to that data as the USB key might fall into a drainage system or a place unreachable to actors with malicious intent. In such a case, a Controller may not necessarily be certain whether unauthorized access to the personal data has taken place, but an availability breach has occurred and is deemed to be aware the moment it has

[5] Section 65 NDPA
[6] Ibid.
[7] Ibid.

notice of the loss of the USB key. Under the NDPA, the loss of a USB key containing personal data qualifies as a personal data breach.

Identification of personal data breaches is dependent on a case-by-case basis and requires an expert understanding of the event juxtaposed with the applicable regulations. Whatever the case, it is important that an initial inquiry into a data breach should commence as quickly as possible to determine whether a breach has occurred with a reasonable amount of assurance; after which a further in-depth investigation can take place.[8]

Navigating Personal Data Breach Incidents

According to an IBM report, the global average cost of a data breach in 2023 was USD 4.45 million, which marks a 15% increase over 3 years.[9] The financial, regulatory and reputational consequences of a personal data breach could significantly hamper the operations and value of a business or organization. These consequences demand that businesses and organizations be adequately prepared at all times to navigate personal data breach incidents so as to be able to mitigate adverse consequences.

Navigating personal data breach incidents in Nigeria starts with the establishment of technical and organizational controls prior to the processing of personal data – not after a data breach - and at regular intervals during processing, following proper privacy risk assessment.[10] These necessary controls are preventive, detective and remedial in nature. As the names imply, the controls help to prevent, detect, and remediate personal data breaches if any to aid organizations in returning to normal working conditions as efficiently as possible ensuring business continuity. The first step to data breach management is from the point of determining the purpose for processing personal data, and this also entails understanding the kinds of personal data being processed by an organization and their locations throughout personal data lifecycle.

The items in the checklist below are the essential building blocks of an effective and efficient personal data management, breach navigation, and incident response plan which will help organizations efficiently prevent, quickly detect, and mitigate personal data breaches. The list below is not exhaustive and is only a general guide, meant to be expanded and tailored to an organization's unique operational privacy needs:

1. Establish and implement a written data breach management, response and recovery policy. Policies must be in touch with existing realities, laws, and be regularly updated.
2. Create and maintain a data map to indicate the types of personal data and their locations throughout data lifecycle. A data map will contain a Record of Processing Activities.
3. Identify the types of personal data processed and its locations and recipients.
4. De-identify personal data as much as possible during processing and delete personal data when it is no longer necessary unless for purposes allowed by law.

[8] Ibid.
[9] https://www.ibm.com/reports/data-breach
[10] Section 24 (1)(f) and 24(2) NDPA.

5. Establish internal and established detection controls in place to detect intrusions or personal data breaches, which may include automated tools.
6. Conduct frequent privacy and security awareness training for employees as part of an ongoing training and awareness program. One inadvertent error on the part of an employee could lead to a hack or data breach in the entire organizations.
7. Back up all personal data.
8. Validate/confirm the data breach.
9. Activation of an incident response team once a security incident has occurred, to implement the incident response plan led by an assigned incident manager.
10. Decide how to investigate the data breach to ensure that the investigative evidence is appropriately handled and preserved.
11. Determine the scope and composition of the breach.
12. Set up a contact point for queries and notify data subjects.
13. Determine whether a data controller, processor, data subject or Data Protection Authority should be notified, and notify when necessary.
14. Collect and review any breach response documentation and analyze reports.
15. Regularly conduct system security audits, checks and sweeps to identify new or existing vulnerabilities (if any) or Personally Identifiable Information (PII) and other sensitive data leakage. This could be done internally or through competent external parties. It is advisable to engage external auditors for system audits.
16. Ensure coordination among business functions to ensure that conflicting messages are not released into public domain in the event of a breach, to avoid public relations disaster.

Due to the increased responsibility of data controllers under the NDPA, a data controller must ensure it conducts due diligence on the systems deployed by vendors, and have a strong data processing agreement in place – inclusive of the right to audit - to govern the data processor's processing activities and limit liability. Vendors risk profiles must also be strictly assessed prior to engagement to ensure they do not have an unpalatable history of security and privacy breach.

The use of cloud storage is increasingly popular among organizations, and there could be a situation where a cloud storage vendor is colossal in value and stature, leaving a data controller in a position where they are unable to negotiate the terms of a processing agreement or conduct on-site audits. In such a case, an organization has to assess the vendors terms of processing and ensure it aligns with organizational goals and privacy obligations through the use of privacy experts and also consider alternatives. This process requires a thorough understanding of the policies, processes and risk profiles of prospective vendors irrespective of their size.

Data controllers should ensure that they conduct strict privacy due diligence during mergers, acquisitions or divestitures as security vulnerabilities could be inherited from other organizations during mergers and acquisitions. The Marriott Hotel personal data breach is a classic example of privacy risks that could arise from mergers, and a lack of proper breach detection tools or capacity.

The company suffered a breach in 2014 which went undetected till 2018 and led to a hefty fine.[11] The company's stock took a hit following the discovery of the breach and the circumstances surrounding the breach.[12] Customers' trust in the ability and dedication of a business entity to protect their personal data, is key to business success and reputation, as such, businesses and organizations should always be able to assure users and regulators of their adherence to appropriate data privacy and protection standards and practices even in the event of a personal data breach.

Data Breach Notification under the NDPA

Before a data controller or processor can comply with any data breach notification obligations, it must also possess the capacity to distinguish between a personal data breach that requires notification and otherwise. The trigger for this obligation varies for data controllers and data processors. For data processors, any personal data breach requires notification to its engaging data controllers or data processors that engaged the personal data[13], and for data controllers, this obligation is dependent on the likelihood of risks presented to data subjects by the personal data breach. For data controllers, there are two levels of risks - risk and high risk - which will trigger notification to the Nigeria Data Protection Commission ("the NDPC") and notification to the data subject respectively[14].

Determining Risk and High Risk to Data Subjects

In determining the existence of a likelihood of risk to the rights and freedoms of data subjects, a data controller will consider the nature of damage done or likely to occur to a data subject as a result of a personal data breach. Damage can occur in the form of physical or psychological harm, discrimination, financial loss, inability to exercise a fundamental human right, etc. The effectiveness of any technical and administrative measures implemented by businesses or organizations to mitigate the likely harm resulting from the personal data breach will also be considered in determining the risk posed to a data subject. These measures may include any encryption or de-identification of the personal data; or any subsequent measures taken by the data controller to mitigate such risk; and the nature, scope and sensitivity of the personal data involved.[15] If for instance, a data controller suffers a security incident but timely activates its data incident response controls, regains full control of its systems and prevents any personal data at risk from getting exposed to unauthorized actors, a data breach that triggers the data breach notification obligation has not occurred. Also, where unauthorized parties gain access to pseudonymized data of data subjects which alone cannot be used to identify a data subject, the level of risk posed to the data subjects who own the pseudonymized personal data is significantly reduce.

---

[11] Carly Page, Hotel Giant Marriott confirms yet another breach", TechCrunch https://techcrunch.com/2022/07/06/marriott-breach-again/ accessed August 15, 2023.

[12] Kate Fazinni, "The Marriott hack that stole data from 500 million people started four years ago — investors should ask how the company missed it", CNBC, https://www.cnbc.com/2018/11/30/marriott-hack-raises-questions-about-merger-diligence-tools-in-use.html, accessed August 15, 2023.

[13] Section 40 (1), NDPA.

[14] Section 40 (2), NDPA.

[15] Section 40(7), NDPA.

In assessing levels of risks, an insight could be taken from the European Data Protection Board's Guidelines[16] for instance, which states that the more sensitive the data, the higher the risk of harm will be to the people affected. A small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a correspondingly large number of individuals.[17]

In 2022, the betting platform Bet9ja suffered a cyberattack from criminal threat actors and the company's press release assured users and customers that their personal data and funds were secure and not compromised as a result of the attack.[18] Such an incident would not ordinarily trigger a data controller breach notification obligation under the NDPA since personal data and funds were not compromised and thus no risks were presented to data subjects.

The inability to access one's gambling account which is usually assigned a distinct identification number could be considered a personal data breach as it concerns the availability of personal data. In that case, the question to determine a breach notification obligation becomes "Will a temporary lack of access to sports betting accounts present risks to the rights and freedoms of customers?" Answers will always differ on a case-by-case basis, for instance where the lack of access was occasioned by a data controller carrying out a system upgrade. Where a customer is denied access to their sports betting account containing the customer's funds, due to a hack, or an alteration of the customers personal details by an employee, a risk can be occasioned to the customer, impacting the customers right to access and use of their funds.

Where no breach notification obligation arises after a personal data breach or security incident, properly crafted public statements may be necessary to assuage the fears of data subjects, and in turn, restore user confidence in the dedication and ability of the business or organization to secure and protect their personal data.

An example of probable high risk to a data subject that will trigger breach notification is when malicious third parties gain unauthorized access to the debit card details, PIN, and other bank account information of a data subject. The information can be used to steal the data subject's finances, or used to engage in the purchase of prohibited or highly regulated items on the dark web, which constitutes criminal activities that can cause risks to the personal liberty of the data subject whose personal information was used to make such purchase. Similarly, where the critical medical information of a patient is unavailable, it will present high risk to the rights of such patient for instance during a medical emergency.

Data Breach Notification Obligations and Reporting Timeframe:

---

[16] Guidelines 9/2022 on personal data breach notification under GDPR, available at https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf accessed August 15, 2023.

[17] Ibid.

[18] The Cable, https://www.thecable.ng/bet9ja-ceo-statement-we-have-control-all-accounts-data-and-funds-are-secure accessed August 15, 2023.

(1) **For Data Processors**: Where a personal data breach has occurred, the data processor shall, on becoming aware of the breach[19] — notify the data controller or data processor that engaged it, and among others shall respond to all information requests from the data controller or data processor that engaged it. There is no stipulated timeframe, but a good practice would be for a data controller to stipulate the reporting timeframe in the data processing agreement, as time is of the essence in handling personal data breaches.

(2) **For Data Controllers:** A data controller shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the Commission of the breach and, where feasible, describe the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned.[20]

(3) **Notification to Data Subjects:** 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 shall immediately communicate the personal data breach to the data subject in plain and clear language, including advice about measures the data subject could take to mitigate effectively the possible adverse effects of the data breach and if a direct communication to the data subject would involve disproportionate effort or expense, or is otherwise not feasible, the data controller may instead make a public communication in one or more widely used media sources such that the data subject is likely to be informed.[21] The NDPC may make a public communication about a personal data breach notified to it by the data controller if dissatisfied with the data controller's notice to data subjects.[22]

4) **Data Breach Records:** A data controller and data processor shall keep a record of all personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in a manner that enables the Commission to verify compliance with this section.[23] This obligation also comes in handy for organizations to draw lessons from incidents and improve existing data breach detection, notification and remediation controls and mechanisms. This will translate into evolved adherence by data controllers and data processors to the security principles of personal data processing which is to be observed in a supply chain/structure.

5) **Data Breach Notification Content**

There is no hard and fast rule under the NDPA regarding the content or style of reporting that a data breach notice will be communicated, but a data breach notification at a minimum must contain—[24]

(a) the name and contact details of a point of contact of the data controller, where more information can be obtained;
(b) a description of the likely consequences of the personal data breach; and
(c) a description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

---

[19] Section 40(1), NDPA
[20] Section 40(2), NDPA.
[21] Section 40(3), NDPA.
[22] Section 40(5), NDPA
[23] Section 40(8), NDPA.
[24] Sec. 40(4), NDPA.

It is key that the contact point should be easily accessible, and allow for a quick response from the data controller or its agents to inquiries by affected data subjects, especially as every "minute" is key for personal data breach remediation.

Why Does it Matter?

Data breach management starts from the point of determining the basis of the collection of personal data and is tied to the security principle of personal data processing. The less irrelevant data a data controller processes, the less risk will likely be constituted to data subjects in the event of a personal data breach, although this is not a hard and fast rule as quantity does not necessarily correlate with sensitivity of personal data. Data breach notification is closely tied to the transparency obligations of organizations that process personal data. From a business perspective, it is also key to maintaining credibility among users. Failure to imbibe the security, integrity and confidentiality principles, and comply with breach notification obligation can lead to the issuance of fines, sanctions,[25] or a search of premises[26] by the NDPC which will affect the financial capacity of the affected entity, and in turn, affect the reputation and business value of the entity.

The technical and organizational controls instituted by data controllers and processors are factored by regulatory commissions generally when faced with the question of issuing orders, fines and sanctions against a data controller or processor. Data controllers will have to be mindful of any regulations issued by the NDPC to adjust their privacy policies to reflect their contents.

Obligation Fatigue and Regulatory Blowbacks

Data privacy and protection obligations under the NDPA, as in other advanced jurisdictions are a handful. Due to the nature of data privacy, what amounts to the extant regulation is usually fluid, and the powers of the NDPC to make subsequent regulations and guidelines pertaining to numerous provisions of the NDPA make the NDPA a live document. There may be a tendency for data controllers and data processors to develop obligation fatigue due to the never-ending changes and guides. This is more so as the trans-border nature of many business activities demands that data controllers and processors keep up with the privacy laws of many jurisdictions, sectors or industries. On the flip side, failure to keep up with regulations will inevitably lead to substantial regulatory blowbacks, and it will only be a matter of "when" not "if."

Conclusion

The ongoing digital transformation of businesses to meet increasing customer demands come with increased threats, complex and malicious cybersecurity assaults, and human error factor.[27] Physical

---

[25] Sec. 47, NDPA.

[26] Section 58(2), NDPA.

[27] Shuman Ghosemajumder , "You Can't Secure 100% of Your Data 100% of the Time" Harvard Business Review, https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time accessed August 15, 2023.

facilities where files and paper documents are stored are also exposed to a variety of natural and societal risks.

The consequences for businesses and organizations that lack appropriate personal data management, data breach management, and incident response controls could be severe, and create huge financial and business operational challenges and losses. The key to surmounting this challenge is the development of a sophisticated data privacy governance framework that charts a data controller or data processor's data breach management process at every point in time, which will form part of a larger privacy framework updated regularly to ensure compliance with any guidelines and standards issued by the NDPC and any other regulatory authority. This is done with the aid of a knowledgeable Data Protection Officer (DPO) or a licensed Data Protection Compliance Services provider, that understands the complex nature of determining what constitutes a personal data breach, and what breach triggers data breach notifications to controllers, data subjects or the NDPC.