Key contacts

Emmanuel Gbahabo
Partner, Dispute Resolution and Head, Investigations, White Collar, & Compliance
emmanuel.gbahabo@templars-law.com

Oghomwen Akpaibor
Managing Counsel,
Corporate & Commercial
oghomwen.akpaibor@templars-law.com

Olivia Agunyego
Associate,
Corporate & Commercial
olivia.agunyego@templars-law.com

TEMPLARS ThoughtLab

Managing Internal Investigations in Nigeria's New Data Privacy Landscape: A Crucial Consideration

Corporate compliance programs are designed to prevent and detect misconduct. Effective detection tools include reporting and investigation. A well-conducted investigation can be invaluable in strengthening a company's defense in the event of law enforcement or regulatory scrutiny, helping it avoid liability, or mitigating damages. In these circumstances, companies tend to rely on investigations to uncover and address misconduct internally, before regulators or law enforcement become involved. Reporting and investigation are the company's first opportunity to identify, verify, and address misconduct before it blows out to be a big issue for the company. If a law enforcement or regulatory investigation occurs, companies are often asked when they became aware of the misconduct in issue, whether they thoroughly investigated the allegations, and if they took appropriate corrective actions. Internal investigations are therefore fundamental to corporate compliance and crucial for deterring employee misconduct, promoting good organizational reputation, and mitigating legal risks.

The growing significance of internal investigations in Nigeria is attributed to heightened regulatory scrutiny and the increasing emphasis on ethical business practices around the globe. Effectively conducting internal investigations requires accessing various data sets including client and employee personal records, electronic communications, call/visitor logs, and CCTV footage, all of which raise diverse privacy concerns.

The enactment of stringent data protection laws, such as the Nigeria Data Protection Act ("NDPA"), underscores the critical need for organizations to navigate the complexities of conducting internal investigations while safeguarding personal data. This paper examines the challenges inherent in balancing the internal investigative imperatives of corporate entities with data privacy obligations. It also seeks to offer best practices for effectively managing internal investigations by corporate entities.

Contextualizing Data Protection in Investigations

Internal investigations are designed to uncover misconduct or suspicious activity within an organization. However, the very nature of internal investigations necessitates the compilation and processing of internal data or processes, which can pose significant data protection risks if the data is mishandled.

The data-driven nature of investigations raises several data privacy concerns. These concerns are typically present from the commencement of an internal investigation. They play a significant role not only in the initial stages but also in the activities that trigger the investigation itself. With internal corporate investigations consistently being reshaped by the growing global focus on data protection, organizations must carefully plan for the privacy and security of personal data throughout the investigation lifecycle. Striking a balance between data privacy and investigations is key, therefore factors like data subject rights and privacy risks and vulnerabilities, reputational damage, and fines must be carefully considered before commencing internal investigations.

Privacy Challenges in Internal Investigations

There is no question that employees generally expect a certain degree of privacy in the workplace and respecting these expectations is crucial for cultivating trust and a positive work environment. Fundamental to respecting employee rights is for employers to be transparent about the types of information that may be accessed, the purpose of the investigation, and how the data will be handled. In navigating the murky waters of internal investigations, organizations often fall short of respecting the boundaries of personal data processing while addressing legitimate concerns related to workplace conduct. The prominent privacy related red flags in internal investigations include:

a. **Lack of adherence to Data Processing Principles**: The NDPA mandates adherence to specific principles for processing and controlling organizational data. Infringement of these principles during an internal investigation process can expose an organization to compliance issues and penalties. For instance, the Federal High Court in a recently decided case[1] recognised the unalterable right to consent and purpose limitation by data processors and controllers when dealing with sensitive data of data subjects, and ordered a bank to pay ₦8,000,000 (Eight Million Naira) in damages for unilaterally opening a domiciliary account without a customer's consent, which was deemed a gross violation of her privacy rights. Similarly, the United States Court of Appeal in a decided case[2], held that a former employee's personal data was accessed and leaked on the dark web due to inadequate security measures. Although no malicious use of the data was reported, the court found that the employee had standing to bring a claim for negligence and breach of contract based on the leaked data.[3]

[1] Suit No. FHC/L/CS/2625/2023 – Folashade Molehin v UBA Plc (unreported) judgement delivered on 13th May 2024.
[2] Clemens v ExecuPharm Inc. 48 F.4th 146, 157-58 (3d Cir. 2022)
[3] In the Clemens case, the court of appeal stated that *"In an increasingly digitalised world, an employer's duty to protect its employee's sensitive information has significantly broadened. Now, employers maintain massive data sets on digital networks. To protect the data, they must implement appropriate security measures and ensure that those measures comply with ever-changing industry standards."*
Similarly, an incident involving the Irish Department of Justice & Equality illustrates the consequences of failing to restrict access to sensitive data. An employee's personal information was unintentionally exposed to a broad audience within the department due to poor access controls. The department was found in violation of data protection laws for disclosing the data improperly. [DPC 2017 Annual Report – Pre GDPR, Case study 11.]

Key data processing principles potentially contradicted in internal investigation include:

- Lawfulness, Fairness, and Transparency [4] : Internal investigations often lack transparency, as the need for confidentiality can prevent informing data subjects about how their data is being used.
- Purpose Limitation[5]: Data collected for internal investigations might be used beyond the initially specified purpose[6], potentially violating this principle.
- Data Minimization[7]: Investigations may require collecting large volumes of personal data, making it difficult to apply data minimization principles.
- Integrity and Confidentiality: Ensuring the security and confidentiality of personal data collected during investigations can be challenging due to the risk of unauthorized disclosure, increasing the risk of data breaches.

b. **Consent and Notification:** Obtaining the required informed consent from data subjects and providing adequate notification about processing can be challenging in investigation contexts**.** This is because investigations often require a degree of surprise to gather credible evidence and informing data subjects about the investigation could compromise the investigation by allowing potential wrongdoers to conceal or destroy evidence. The Supermarket Case[8] investigated by the Irish Data Protection Commission illustrates this challenge. In this case, an employee was dismissed for obstructing a CCTV camera placed in the staff canteen, which was not previously notified to staff. The CCTV'S placement and use were deemed excessive, highlighting the need to balance investigative secrecy with the requirement for transparency and consent.

c. **Data Protection Rights**: The NDPA grants data subjects various rights regarding their personal data, which, when exercised, may impact investigations to some degree. These rights including the right to be informed[9], access, rectification, erasure[10], restriction of processing[11], and objection[12], empower individuals to exert control over their personal data. While these rights are essential for protecting individual rights, they can present challenges for organizations conducting investigations, as they may hinder data collection, analysis, and retention efforts. Furthermore, the right to withdraw consent[13] and object to data processing, can disrupt ongoing investigations. The ability of individuals to request access to data collected during an investigation may also compromise the confidentiality of the inquiry. Additionally, data subjects' rights concerning automated decision making and profiling[14] allows them to challenge and request human intervention in decisions made solely by automated processes, thus complicating investigations that rely on automated data analysis. The

[4] Section 24 (a) of the NDPA
[5] Section 24 (b) of the NDPA
[6] For example, consider a scenario where an organization collects employee data primarily for payroll processing. During an internal investigation into suspected fraud, the organization might be tempted to use this payroll data to cross-reference financial discrepancies without informing the employees. This repurposing of data violates the principle of purpose limitation because the data was initially collected solely for payroll purposes and not for investigative reasons.
[7] Section 24 (c) of the NDPA
[8] DPC 2015 Annual Report – Pre GDPR, Case study 7. https://www.dataprotection.ie/en/pre-gdpr/case-studies#staff (Accessed 08 August 2024).
[9] Section 27; 34 of the NDPA
[10] Section 34 (1) d of the NDPA
[11] For instance, if an employee disputes the accuracy of certain data collected during an investigation, they can request that its processing be restricted until the accuracy is verified. This can slow down the investigation as it halts further analysis or use of the data in question.
[12] Section 36 of the NDPA
[13] Section 35 of the NDPA
[14] Section 37 of the NDPA

Supermarket case underscores the importance of respecting employee privacy rights while conducting investigations.

d. **Cross-border data transfers**: investigations that involve transferring data to a third party located outside Nigeria, raises additional data protection considerations due to the added pressure of ensuring compliance with varying data protection regulations in different countries which may complicate the investigation process.

e. **Data Breach/Security Issues**: the sensitive nature of data involved in investigations increases the risk of data breaches. Data breaches can have severe consequences, both for the organization and the individuals whose data is compromised.

f. **Collaboration with external parties**: investigations may require working with external parties, such as forensic specialists which may necessitate sharing of sensitive data and raise privacy risk.

g. **Statutory/Regulatory Sanctions:** Failure to comply with data protection laws can lead to severe consequences, including regulatory fines of up to Ten Million Naira or 2% of annual gross revenue if classified as Data Controllers of Major Importance ("DCMI") or Data Processors of Major Importance ("DPMI"), or up to Two Million Naira or 2% of annual gross revenue if otherwise classified. [15] There is also the risk of organisations being held liable for privacy breaches of third-party processors engaged during investigations where such third parties fail to strictly comply with applicable data protection standards.

Beyond regulatory fines, organizations may also face reputational damage and substantial costs from breach response efforts, legal fees, and potential civil actions[16] due to data protection breaches.

Recently, an employee of a Nigerian transnational FMCG sued his employer for obtaining his bank account statement and releasing same to the police on alleged breach of the employer's code of conduct which led to his detention for a period of over five days by the police. The employee in his affidavit stated that the bank owed him a duty of confidentiality and had a responsibility as a data controller to limit the processing of his personal information for the purpose for which he gave instruction and nothing more. Premised on the above, the employee in addition to seeking a declaration that the action of his employer and his bankers was a breach of his right to the privacy of his personal information also sought ₦500,000,000 (Five Hundred Million Naira) in damages against both parties [17].

The case is ongoing at the Federal High Court,[18] however it has generated significant criticism in social circles for the brazen display of corporate malfeasance on account of an alleged breach of the Company's code which had not even been proven. It brings to fore once more the fact that organizations and even third parties cannot simply, on account of internal investigations, disregard data privacy protection of their employees and/or customers.

[15] Sections 48 & 49 of the NDPA.
[16] Section 51 of the NDPA.
[17] https://www.lawyard.org/news/court-set-to-hear-data-breach-action-against-promasidor-zenith-bank/ (Accessed 08 August 2024)
[18] FHC/L/CS/2465/23

Practical Considerations for Effective Investigations Management

To effectively manage personal data during investigations and mitigate liabilities associated with data breaches, organizations can adopt five key strategies:

a. ***Develop Robust Privacy and Data Protection Policies and Training Programs:*** Organizations should establish clear data protection policies that outline how personal data should be handled during investigations, ensuring alignment with data protection best practices. Regular training for employees on these policies is essential, with an emphasis on the importance of compliance with the NDPA and other relevant laws.

b. ***Implement Data Minimization and Proportionality***: Organizations must ensure that only necessary data is collected during investigations and that investigative activities remain proportionate to the issue being addressed. This approach minimizes privacy risks and aligns with data protection principles.

c. ***Maintain Transparent Communication and Data Retention Practices***: Often, organizations lay the foundation for alleged data rights actions because they fail to transparently communicate the purpose of the data collected or the processes implemented to the employees. Keeping employees informed about how their data is handled and their rights under the NDPA can help mitigate the impact of any breach. Additionally, it is crucial to retain personal data only for the duration necessary to complete the investigation.

d. ***Enhance Data Security and Access Controls:*** implementing strict access controls, encryption, and other security measures can help protect sensitive data from unauthorized access. Regular audits and Data Privacy Impact Assessments ("DPIAs") [19] should also be conducted to identify and address potential vulnerabilities.

e. ***Establish Comprehensive Incident Response and Documentation Procedures***: Developing a robust incident response plan to quickly address and mitigate the effects of any data breach is crucial. Furthermore, it is pertinent for organizations to maintain detailed records of data processing activities and decisions made during investigations to demonstrate their commitment to data protection and accountability.

[19] The NDPA mandates organizations to conduct a Data Privacy Impact Assessment ("DPIA") before processing personal data where such processing poses significant risks to the rights and freedoms of individuals, which is often the case with internal investigations. Section 28 (1) of the NDPA.

Conclusion

Balancing the needs of internal investigations with data protection requirements is a complex but essential task for organizations and navigating the complexities of data protection in the context of such investigations can be challenging. The critical strategies for success include developing robust data protection policies, conducting regular training and DPIAs, ensuring transparent communication, and implementing robust data security measures. Organizations can effectively manage investigations by adopting these best practices while safeguarding data privacy and minimizing liabilities. This approach fosters trust within the organization and reduces the risk of data breaches and regulatory sanctions.