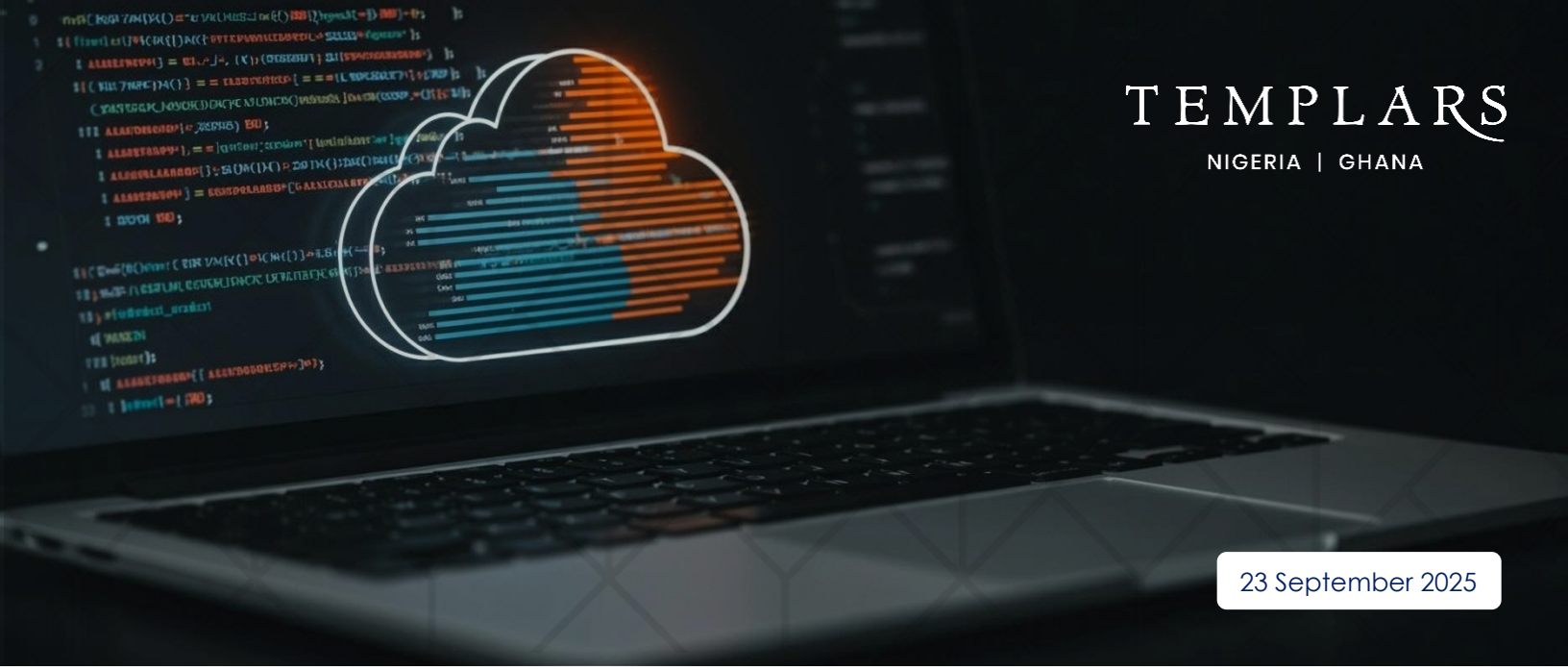


TEMPLARS
NIGERIA | GHANA

23 September 2025

Key contacts

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

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

Uwemedimo Atakpo
Associate,
Corporate & Commercial
uwemedimo.atakpo@templars-law.com

TEMPLARS ThoughtLab

Corporate Data Breaches: *Critical Risks, Legal Gaps and Best Practices*

The rise of cyber threats and growing dependence on technology has made data security a critical concern in today's digital world. Despite being one of Africa's largest economies[1] and a growing digital hub, Nigeria's significant strides in data protection, marked by the 2023 Nigeria Data Protection Act ("**NDPA")** and its 2025 General Application and Implementation Directive ("**GAID**"), remain limited, focusing primarily on safeguarding personal data of individuals while sensitive corporate data remain vulnerable.

As technology advances and cyber threats become more sophisticated, corporate entities are facing increasing threats that demand a more robust and proactive legal framework, much like South Africa's Protection of Personal Information Act ("**POPIA**"), which explicitly extends its scope of protection to corporate entities.

In this article, we highlight the escalating vulnerabilities impacting corporate data processing, analyze the gaps in Nigeria's current data protection laws, and advocate for best practices and new legal frameworks to mitigate data breach risks.

Why is Securing Corporate Data Crucial?

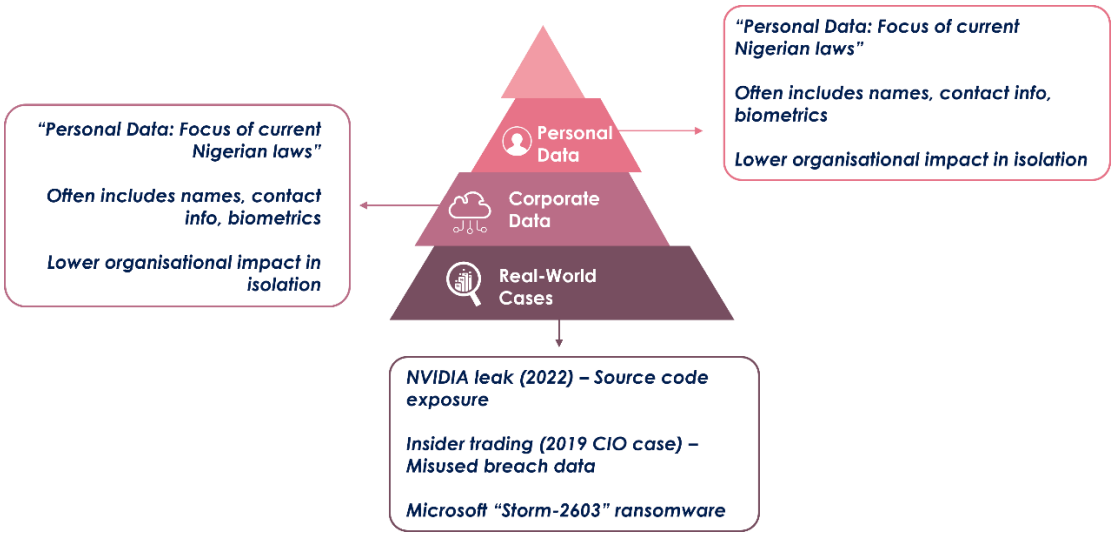
In an era defined by data, a company's digital asset is often its most valuable and vulnerable resource. More recently, corporate data[2], has gained significant relevance as a digital asset, given its central role in modern business operations, making its robust protection indispensable.

[1] According to Statistica an advanced analytics software package, Nigeria is fourth largest economy in Africa https://www.statista.com/statistics/1120999/gdp-of-african-countries-by-country/

[2] Corporate data is any unique information that identifies a specific company, distinguishing its operations and processes from other businesses. It encompasses sensitive corporate information such as financial history, credit worthiness, confidential operational data, intellectual property, trade secrets, proprietary algorithms, R&D data, customer databases, strategic plans, product designs, supply chain logistics, sensitive internal communications etc.

Quite unlike personal data, corporate data vulnerabilities are often more complex with far reaching impacts on the organizations to which they relate. This is majorly due to the high value and diversity of the data involved. In some instances, a single corporate data breach can pose a significant threat to a business's sustainability, even crippling its financial viability. For instance, a pharmaceutical company could have its clinical trial results, drug formulation or sensitive patient data compromised. Similarly, a tech company might suffer a leak of its source code for a new software release, or an entertainment company could see its unreleased films, music, or game assets appear online. These scenarios and similar events present existential threats to modern businesses with the potential to inflict irreversible damage to their reputation and competitive advantage. In essence, a breach of sensitive corporate data can be as devastating if not more so, than a personal data breach, due to the highly sensitive and often proprietary nature of the information.

Corporate Data vs Personal Data



What makes Corporate Data Exposures More Amplified than Personal Data Breaches?

Unauthorized access to, or loss of, a company's confidential information such as operational data, trade secrets, proprietary algorithm, R&D data or strategic business information, even without directly involving personal details, can be catastrophic to any business. This is because the impacts are far more profound and complex than isolated personal data breaches. The risks that any unauthorized exposure of sensitive corporate data poses to a business are far too numerous to mention but we have listed a few:

Erosion of Trust and Reputation - Beyond the immediate operational and financial impact of a corporate data breach, breach of sensitive corporate information such as trade secrets or business ideas poses severe risks to the company's most vital assets i.e. its reputation and the trust of its customers and stakeholders. For organizations which owe high fiduciary duties to their customers and stakeholders, breach of confidential corporate data – such as confidential strategic business plans, investment strategies, defense strategies or client personal data can directly erode consumer trust. It could also significantly undermine the company's reputation and cause widespread public distrust which could lead to consumer apathy. A classic example was the NVIDIA source code leak in 2022, where a massive

amount of corporate data, including the company's source code for certain digital assets, had been compromised. The unauthorized exposure had posed a threat that could have revealed security vulnerabilities in NVIDIA's products or given competitors an unfair advantage, which could have ultimately degraded user experience and the company's reputation for technical leadership.[3]

- ***The Risk of Sophisticated Threats*** - Unlike personal data, corporate data breaches can be perpetrated for illicit activities such as insider trading, competitive advantage, or even market manipulation, all of which could cripple any business, especially those in the financial services sector. In 2019, the former Chief Information Officer of a large information solutions company, was convicted and sentenced to prison for insider trading in the United States because of the use of insider information for personal gain[4].

- ***Unified System Risks*** - Many modern businesses, including banks, operate through interconnected systems and employ cloud computing services for the storage of their sensitive corporate data. In these environments, a weakness in any part of the ecosystem could potentially expose a company's sensitive information to external threats and manipulation which could compromise its security and integrity. Recently, Microsoft in a blog post announced that a group it dubs "Storm-2603" was using vulnerabilities in its on-premises SharePoint servers to plant ransomware, paralyzing victims' networks until a digital currency payment is made[5].

- ***Subtle Vulnerability of Certain Intangible Assets*** - Traditional data protection often focuses on tangible data like customer records or financial information. Intangible assets like IP on the other hand have certain unique features which, if stolen, could trigger substantial financial losses and undermine the company's long-term investments in R&D.

For businesses that are heavily reliant on their IP e.g. fashion, biotech, pharma companies, etc. such breaches could pose serious threats to their reputation and finances.

What Protections Exist Under Nigeria's Legal Framework?

Beyond the limited protections which certain Nigerian statutes provide, there is no specialized overarching framework for the protection of corporate data in Nigeria. Sadly, this gap leaves businesses vulnerable to a multitude of risks that can impact their operations, reputation and finances. Presently, regulatory protections for corporate data are limited to the following:

- ***Nigerian intellectual property (IP) laws*** – IP laws such as the Copyright Act, the Patents and Designs Act, and the Trademarks Act protect specific categories of intellectual property by granting exclusive rights to their creators or inventors. For example, the Copyright Act protects software code as a literary work. The Patents and Designs Act protect new inventions and aesthetic designs while the Trademarks Act protects brand names and logos. However, these traditional laws are notably limited in their ability to protect corporate IP information. Firstly, copyright law protects the expression of an idea and not the idea itself, allowing competitors to build upon unexpressed company ideas. Furthermore most of these IP laws require registration requirement to guarantee protection and still do not provide the proactive security mandates expected from a dedicated corporate data protection framework.

[3] https://techcrunch.com/2022/03/01/nvidia-hackers-leak-ransomware/
[4] https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading
[5] https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

- ***Cybercrime (Prohibition, Prevention, etc.) (Amendment) Act 2024*** – The Act contains provisions prohibiting and sanctioning a wide range of cyber related offenses in Nigeria including unauthorized access to computer systems. It also provides a legal basis for prosecuting individuals who illegally access and steal a company's digital assets. However, the concern here is that it is a criminal law and not a data protection framework, meaning it focuses on punishment for the crime rather than prescribing preventative corporate data protection measures for businesses.

- ***The Constitution of the Federal Republic of Nigeria 1999 (as amended) and the NDPA*** - The Nigerian Constitution and NDPA are the most significant body of rules, which, along with the GAID, primarily focuses on the protection of personal data of natural persons. They provide foundational legal principles that can be used to argue for the protection of personal data in legal proceedings, and they mandate organizations to process personal data lawfully, fairly, and transparently and to implement appropriate security measures. Although they seek to protect customer and employee data, the protection does not explicitly cover proprietary corporate data like trade secrets or business strategies.

Freedom of Information Act - Public institutions are explicitly prohibited from disclosing information that contains trade secrets, and commercial or financial information obtained from a person or business where such trade secrets or information are proprietary, privileged or confidential, or where disclosure of such trade secrets or information may cause harm to the interests of the owner[6]. However, as with most laws, the protection is not absolute but often applicable on a "public interest test" basis. For example, a court may order the disclosure of trade secrets if public interest outweighs the private interest of the owner.

- ***Contract*** - Under Nigerian law, victims of misuse or unauthorized disclosure of corporate data may be entitled to damages/compensation where a contract containing confidentiality obligations between the parties exist. In addition to damages, an affected company may also seek injunctions through the courts to prohibit an unauthorized discloser from further using or disseminating the confidential information.

- ***The Investment and Securities Act, 2007 (ISA) –*** In a very limited sense, the ISA also contains certain provisions which protect corporate data of public companies. For instance, the Act places investigating officers under conditions of confidentiality in their periodic assessment and examination of the books and affairs of capital market operators[7].

What are the Beneficial Insights from POPIA and Best Practices for Protecting Sensitive Corporate Data?

To effectively resolve corporate data vulnerabilities, a comprehensive approach that blends processes, people, technology and statute must be adopted. Businesses which have strong data protection practices typically have a systematic and well-documented approach to data security.

[6] Section 15(1)(a) Freedom of Information Act 2011.
[7] Part VII of the ISA 2007

Such companies adopt strong proactive corporate data protection mechanisms including the implementation of strong data access controls such as the principle of least privilege, encryption of sensitive corporate data both at rest and in transit, vigorously investing in employee training and awareness, undertaking prompt security audits and patches, and investing in a robust backup strategy.

Interestingly, South Africa's POPIA, enacted in 2013, stands out globally. Unlike many data privacy laws, a key and laudable feature of POPIA is that its definition of "personal information" explicitly includes information relating to an identifiable, existing juristic person – such as a company or organization - in addition to natural persons.

Section 1 of POPIA defines "personal information" as "*information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person*". This distinctively offers a broader scope of protection for proprietary corporate information[8] which, if unduly exposed, could cause significant harm to the company. Most importantly, POPIA provides eight core data protection principles which proactively protect the personal data of data subjects (i.e. natural and juristic persons) equally. In this regard, the Act mandates the following when processing personal data of both natural and juristic persons:

Accountability: Companies must implement robust governance frameworks to protect the corporate data they hold.

Processing Limitation: Processing of corporate data must be lawful and processed in a reasonable manner that does not infringe on the privacy of the entity.

Purpose Specification: Corporate data cannot be collected or processed without a clear reason.
Further Processing Limitation: Corporate data cannot be further processed in a manner incompatible with the original purpose for which it was collected.

Information Quality: Corporate data collected for processing must be complete, accurate, not misleading, and updated where necessary.

Transparency: Proper documentation of all processing operations about juristic persons must be maintained and information about such processing provided where required.

Data Security: Most importantly, a "responsible party" (i.e. data controller) must implement appropriate, technical and organizational measures to prevent loss, unauthorized access or disclosure of corporate data. This also includes protecting against internal and external risks, regularly verifying the effectiveness of security safeguards, and updating them and notifying the regulator as well as the affected juristic data subject of any data breach.

Data Subject Participation: Companies also have the right to correct, access or object to the processing of their personal data.

Similarly, several notable steps have been taken in other jurisdictions to protect the sanctity of sensitive corporate information, some of which include:

[8] includes any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person, the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence, the views or opinions of another individual about the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

- ***The French Commercial Code*** – The Code which regulates commercial and business relationships in France contains several provisions that serve to ensure the confidentiality of sensitive corporate data. For instance, it provides that the directors of a company or any other person invited to attend board meetings are bound by secrecy in regard to any information of a confidential nature presented as such by the chairman of the Board.[9] Additionally, the Code provides for the maintenance of confidentiality of documents containing business secrets even in the course of competition related disputes. The Code allows the chairman of the Competition Council to refuse discovery or consultation of documents which affect business secrecy.[10]

- ***The German Commercial Code*** – Similar to the French Code, the German Code also contains several provisions ensuring the continued confidentiality of corporate data. It prohibits a commercial agent, even after the termination of his agency contract, from using or disclosing business or trade secrets that have been entrusted to him by virtue of his engagement with his principal, to third parties.[11] The Code also has extensive provisions on breach of confidentiality obligations.[12] It provides that a person who discloses a trade secret or business secret of a company or a subsidiary in the course of auditing the annual financial statement or the financial information of a company will be liable to a term of imprisonment not exceeding 1 (one) year or to a fine.

In effect, these laws provide a uniquely broad level of protection for sensitive corporate information. By legally defining corporate data as "personal information" when it relates to an identifiable juristic person, businesses subject to POPIA are compelled to treat their own sensitive corporate information with the same sensitivity and confidentiality as individual customer data. In other words, sensitive corporate data like operational data, strategic plans, financial records, and other confidential business information are statutorily protected and subject to robust protection requirements under these laws. Companies are mandated to be more diligent when sharing sensitive corporate data with third parties. Notably, these laws incorporate provisions that impose increased liability on entities that fail to implement holistic data protection measures in respect of the corporate data they process. For instance, penalties under POPIA, can be up to R10 million (circa USD$564,972/NGN 864,742,939) with potential imprisonment of convicted defaulters[13].

Conclusion

Why Nigeria must urgently legislate on Corporate Data Protection

Beyond the protection of personal data, a significant legal gap still exists in Nigeria's framework for securing sensitive corporate data. Despite some deterrence provisions in the NDPA and the Cybercrime Act, these laws still fall short of providing comprehensive protection for confidential, sensitive corporate information. What is more, other than suing for damages, or initiating criminal proceedings in the case of offences under the Cybercrime Act, there is currently no clear path to

[9] Article L225-37 of the Code
[10] Article L463-4 of the Code
[11] Section 90 of the Code
[12] Section 333 of the Code
[13] Section 109 of the Code

recourse for businesses affected by a corporate data breach. It is therefore time for Nigeria to build on the solid foundations of the NDPA and enact a specific corporate data regulation or commercial code to govern the use, disclosure, and third-party interaction with sensitive corporate data. Such a framework would undoubtedly protect corporate assets, establish clear organizational duties, and empower businesses to seek legal redress where necessary. More importantly, this proactive measure would signal to the world that Nigeria is committed to creating a secure and reliable business environment, thereby fortifying its economy for future growth.

If you require any further clarification, do not hesitate to contact us.