

How long should your organisation keep *personal data* in Nigeria?



Many organisations focus on collecting and securing personal data but overlook a critical compliance risk:
retaining personal data longer than legally permitted.



It is not enough to keep personal data secure. Holding on to it beyond the lawful period exposes organisations to regulatory, legal and reputational risks, especially given that no system can guarantee perfect security. Nigeria's data protection laws do not expect organisations to be eternal guardians of personal data.



While the Nigeria Data Protection Act 2023 (NDPA) doesn't prescribe a blanket retention period, Section 24(1) (d) provides that personal data must only be retained as long as necessary to achieve the lawful basis for which it was collected or further processed.



Once the lawful basis is fulfilled, the data must be either securely deleted or irreversibly de-identified—see Section 34(2)(b) of the NDPA and Article 4(vi) of Schedule 1 to the NDPA-General Application and Implementation Directive 2025 (GAID).





So, what qualifies as a “lawful basis” for retaining data? This includes:

1. Valid, unwithdrawn consent from the data subject; or necessity for fulfilling an ongoing contract with the data subject, complying with legal obligations (e.g., PAYE filings, pension remittances), or safeguarding the vital interests of the data subject or another individual.
2. Performance of a task carried out in the public interest, as authorized under applicable law.
3. Pursuit of legitimate interests by the data controller, processor, or a third party to whom the data is disclosed, provided such interests do not unjustly infringe upon the rights and freedoms of the data subject.



Under the NDPA, data controllers must inform data subjects of the specific lawful basis for processing and disclose the retention period before collecting personal data – Section 27(b) & (e).

Data controllers and data processors are also required to implement a clear, legally compliant data retention policy.



Retaining personal data indefinitely not only increases your exposure to data breaches and privacy violations, but it also invites regulatory scrutiny and sanctions. If your organization lacks a compliant data retention framework or hasn't reviewed its data retention practices in light of the NDPA and GAID, now is the time to act.



Don't wait for a data audit to highlight your weaknesses. Review your organisation's data retention policy today and ensure it reflects both regulatory requirements and operational needs.



Our Data Protection Team



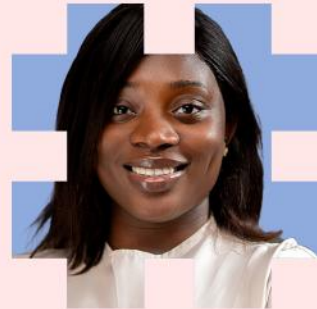
Bunmi Akinsanya

Senior Associate



Ifeoluwa Adelugba

Associate



Toluwalashe Osho

Associate





...built on *trust* 