

SYNTEGRAL LEGAL PRACTICE

DATA PROTECTION - DATA MINIMISATION AND RETENTION: KEEPING ONLY WHAT YOU TRULY NEED.

Authors



Oladiran Falore
Senior Partner, SyntegralLP



Precious Orowa
Senior Associate

Contact:
info@syntegrallp.com

Abstract

This article examines the legal and practical importance of data minimisation and retention under Nigeria's modern data protection framework, with particular reference to the Nigeria Data Protection Act 2023 (the "Act" and the General Application and Implementation Directive (GAID) 2025. It argues that data minimisation is not merely a drafting principle in a privacy notice or a box-ticking compliance exercise, but a core governance discipline that directly affects legality, proportionality, cybersecurity exposure, records management, and regulatory defensibility. The article also places the Nigerian position in dialogue with broader international standards, especially UK data protection guidance, to show that a "collect less, keep less" approach is both locally grounded and globally intelligible. It concludes that organisations that reduce unnecessary collection and define retention with precision are often in a stronger position not only to comply with the law, but also to reduce breach impact, improve data quality, and build trust.

Keywords: *data protection; data minimisation; retention; storage limitation; Nigeria Data Protection Act (NDPA) 2023; Nigeria Data Protection Commission; privacy governance; cybersecurity; accountability; compliance.*

1. Introduction: a small form, a big problem

Picture a Tuesday afternoon in Lagos. A compliance team is midway through a review when they hit a major red flag. They pull up a basic onboarding form for something as simple as internet or waste disposal service, only to find the provider is asking for everything, from IDs and Mother's maiden name to the customer's BVN and next-of-kin. It's total data overkill for a simple subscription. When asked why all that information is needed, the answer is familiar: "Let us just have it there. It may be useful later." That single sentence captures one of the most persistent weaknesses in privacy governance across organisations. It is not always bad faith. Quite often, it is habit. But in legal terms, habit is not a lawful basis.

Modern data protection law has moved sharply away from the culture of speculative collection. In Nigeria, that shift is now unmistakable. The Act requires personal data to be collected for specified, explicit and legitimate purposes, to be adequate, relevant and limited to the minimum necessary, and to be retained no longer than necessary for the lawful basis for which it was collected or further processed. The GAID 2025 then adds practical interpretation, explaining that "minimum necessary" means the least possible data essential to fulfil the stated purpose.

The message is clear enough in plain English: if an organisation cannot explain why it needs a category of data, it should be very slow to collect it. If it can no longer justify keeping it, it should be very ready to delete or irreversibly de-identify it. This is where minimisation and retention cease to be abstract principles and become everyday legal discipline.

2. The legal framework

The legal framework governing data minimisation and data retention in Nigeria is derived from a combination of statutes, subsidiary regulations, and regulatory guidance. These instruments collectively establish the principles that guide how personal data may be collected, processed, stored, and retained by both public and private entities. Among these, the most significant legislative development is the enactment of the Act.

NIGERIA DATA PROTECTION ACT 2023: This legislation was signed into law on 12 June 2023, constitutes Nigeria's primary legal framework for the protection of personal data. The legislation has a broad territorial scope. It applies not only to data controllers and processors operating within Nigeria but also to entities located outside the country where they process the personal data of individuals who are located in Nigeria. This extraterritorial application reflects a growing international trend in data governance, aligning Nigeria's approach with global data protection frameworks.

Central to the Act is Section 24, which requires that personal data be collected only for specific, explicit and lawful purposes, limited to what is adequate, relevant and strictly necessary for those purposes, and retained only for as long as is required to achieve the objective for which it was obtained. These requirements reflect the core principles of data minimisation and storage limitation, and they operate not as aspirational standards but as legally enforceable duties.

The significance of section 24 lies in the fact that it connects three matters that organisations often try to treat separately: purpose, quantity, and duration. In reality, they are legally linked. The narrower and clearer the purpose, the easier it is to justify the data set. The weaker the purpose, the harder it becomes to defend both collection and retention. A controller cannot simply say, "we may need it one day." The law expects the purpose to be specified, explicit and legitimate now, not imagined later.

The GAID is especially helpful because it gives practical meaning to the statutory words. It states that "adequate" means appropriate quantity and quality; "relevant" means materially useful and indispensable; and "minimum necessary" means the least possible data essential to the fulfilment of the specified purpose. On retention, it says that where data is kept solely for record purposes, the organisation should determine the minimum data relevant and necessary for that purpose, and any residue no longer needed should be properly destroyed or irreversibly de-identified. It also says the retention policy must be communicated to data subjects.

That is a strong regulatory position. It leaves little room for indefinite retention by inertia. It also means that organisations operating in Nigeria should not treat "data retention policy" as a mere internal administrative note. It is part of legal compliance architecture.

The legal framework governing data minimisation and data retention in Nigeria is derived from a combination of statutes, subsidiary regulations, and regulatory guidance. These instruments collectively establish the principles that guide how personal data may be collected, processed, stored, and retained by both public and private entities. Among these, the most significant legislative development is the enactment of the Act.

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY ACT 2004: The National Information Technology Development Agency (NITDA) Act 2024 established the National Information Technology Development Agency and vested it with responsibility for developing policies and regulatory frameworks for Nigeria's information technology sector. Historically, this mandate included the issuance of the Nigeria Data Protection Regulation 2019, which served as the country's primary data protection instrument prior to the enactment of the Nigerian Data Protection Act 2023. Although the direct regulatory responsibility for data protection has since shifted to the NDPC, the NITDA Act remains part of the broader statutory framework of Nigeria's digital governance architecture and continues to shape policy development within the technology sector.

CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT 2015, (AS AMENDED): The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 introduces a distinct regulatory obligation in relation to data retention. In particular, section 38 requires service providers to retain traffic data and subscriber information for a minimum of two years. This creates an apparent tension with the storage limitation principle under the Nigeria Data Protection Act 2023, which requires that personal data be retained only for as long as necessary for the purposes for which it was collected.

Organizations that fall within the scope of both frameworks, particularly telecommunications operators, internet service providers, and digital platform companies, must therefore adopt a careful structured compliance approach. In practice, this is usually addressed through a targeted retention policy under which only the specific categories of data required by section 38 are retained for the statutory period. This helps ensure that the legal obligation does not become a basis for indiscriminate or indefinite retention of personal data across the organisation.

CENTRAL BANK OF NIGERIA REGULATIONS: The Central Bank of Nigeria (CBN) requires banks and financial service providers to retain customer due diligence and transaction records for at least five years after the end of the business relationship or completion of the transaction. This obligation is further reinforced by section 8(1) (a) of the Money Laundering (Prevention and Prohibition) Act 2022, which imposes statutory record-keeping requirements on financial institutions. Under that provision, relevant customer and transaction records must be retained for a minimum of five years. Even so, organizations must design their retention schedules in a way that satisfies these minimum regulatory requirements without treating them as a justification for the indefinite storage of personal data.

3. Why minimisation matters more than many organisations realise

We often talk about data minimisation like it is just a box to tick for privacy compliance. In reality, that's only half the story. It is actually a design principle, a security principle, a records management principle, and a litigation-risk principle. The moment an organisation starts hoarding more data than it actually needs, the cracks start to show.

First, the legal justification falls apart. If a controller relies on contract, the question becomes whether the collected data is actually necessary to perform the contract. If it relies on legitimate interests, the necessity and balancing exercise becomes more difficult where the organisation has collected excessive material. If it relies on consent, the quality of that consent may be questioned where the request is bundled, broad or disproportionate. The problem is not only the existence of data. It is the absence of a disciplined explanation for why it is there.

Secondly, excessive collection weakens proportionality. The Act requires an assessment of necessity and proportionality where a data privacy impact assessment (DPIA) is required for high-risk processing. That means a controller should not leap straight to technical safeguards without first asking whether the volume and type of data being processed are justified at all. In practice, many DPIAs are strongest where the first control is reduction of the data set itself.

Thirdly, excessive collection is the parent of excessive retention. Once data enters multiple folders, inboxes, vendor tools, spreadsheets and backups, it becomes harder to trace, harder to review, and harder to delete. One can see this in organisations that still carry years of examination scripts, old CVs, unneeded medical records, stale onboarding files, redundant CCTV exports and legacy customer profiles simply because no deletion trigger was ever built. From a governance standpoint, that is not prudent record keeping. It is unmanaged accumulation. The Act gives data subjects the right to erasure where the data is no longer necessary or where there is no other lawful basis to retain it.

4. The retention question: not forever, not “just in case”

Data retention is frequently the "Achilles’ heel" of even the most sophisticated privacy programmes. While many organisations fall back on the rhetorical safety blanket of keeping data “for as long as necessary,” this phrase is practically hollow without a specific anchor. To be truly functional, necessity must be defined by something concrete, a statutory rule, a business requirement, a limitation period, or a pending litigation hold.
In the Nigerian context, the Act and the GAID 2025 demand a much more rigorous approach. The shift from “vague intent” to “strict compliance” is driven by three key provisions.

- Section 24 (Act) prohibits retaining data beyond the lifespan of its lawful basis. Once the original purpose is exhausted, the justification for holding the data expires with it.

- Section 27 (Act) empowers data subjects by requiring transparency. Organisations must disclose specific retention periods or, at the very least, the objective criteria used to calculate them.

The GIAD directs that retention policies must align with broader Nigerian law and clearly communicate how these periods affect a user’s right to access their information.
That means a proper retention framework should identify at least four things: the category of data, the purpose and lawful basis, the trigger for the retention period, and the end-of-life action. That last point matters. A retention rule is incomplete if it says only how long data may be kept. It should also say what happens next: deletion, anonymisation, restricted archive, or preservation under legal hold.

For Nigerian organisations, this is where one must be realistic. Some records will need to be retained because other legal regimes require it: employment law, tax law, sector regulations, financial reporting obligations, anti-money laundering controls, contractual limitation periods, or active disputes. But it does not follow that every piece of personal data within a record must remain in full, live or in searchable form forever. The GAID's direction to keep only the minimum data relevant and necessary for record purposes is especially important here. It encourages disciplined trimming rather than blanket hoarding.

5. Why collecting less improves security

There is a simple truth every seasoned privacy lawyer or Data Protection Officer eventually accepts, the safest personal data is the one you never collected in the first place. Even the Act makes this connection clear by insisting that personal data must be handled in a way that ensures proper security and guards against unauthorised or unlawful use. The more data you hold and the more sensitive it is the heavier that responsibility becomes.

That's why data minimisation is not just a compliance rule; it's a security strategy. When a business collects fewer data points, fewer staff need access. When it keeps records for shorter periods, there are fewer old files lying around waiting to be compromised. When it deidentifies older data, the information becomes less valuable to attackers. And when it clears out stale data from old systems, backups and shared folders, the number of possible breach points drops. None of this requires fancy theory. It's simply reducing risk.

The UK Information Commissioner's Office (ICO) guidance on data minimisation and data protection by default is very helpful, especially for organisations with international operations. The ICO's position is straightforward: organisations should identify the minimum amount of personal data needed for their purpose and collect only that. Data protection by default also means limiting the use of personal information strictly to what is necessary for each specific purpose. This aligns closely with the Nigerian approach and shows that minimisation is not some local peculiarity, it is recognised global best practice.

There's also a practical enforcement angle. Whenever a breach or incident occurs, regulators and claimants tend to ask two quick questions: Why did you collect this data? and Why were you still keeping it? If an organisation cannot answer those questions convincingly, its position becomes much harder to defend. An oversized data estate doesn't just increase the impact of a breach it weakens your justification and your defence.

6. The DPO's role: asking awkward but necessary questions

Section 32 of the Act makes it clear that any data controller of major importance must appoint a Data Protection Officer (DPO) who has solid expertise in data protection law and practice, and who is capable of performing the statutory functions. These functions include advising the organisation on compliance and serving as the primary contact point for the Nigerian Data Protection Commission ("Commission"). In practical terms, one of the DPO's most valuable roles is to ask the uncomfortable questions that business teams sometimes prefer to overlook:

- Why do we need this data field?
- What is the lawful basis for collecting it?
- Can we deliver the service without it?
- Who truly needs access?
- How long should it remain identifiable?
- What is triggers deletion?
- Are we distinguishing between what is "useful" and what is "necessary"?

These are not bureaucratic hurdles. They are the basic questions that turn privacy from a written policy into operational control. Too often, teams inherit old forms or vendor templates and assume every requested field is justified simply because "the system asks for it." That is not enough. The controller remains fully responsible for ensuring that processing is lawful and proportionate, even when third-party processors are involved. The Act is explicit that processors engaged by controllers must comply with the relevant principles and obligations.

A seasoned DPO also understands that data minimisation is not a onetime decision taken during onboarding. It must be revisited during system redesign, procurement, vendor onboarding, incident response reviews, and records management cleanups. Data estates grow quietly in the background. Good governance requires regular pruning.

7. International relevance: a Nigerian principle with global alignment

For an international reader, the Nigerian position is s both uniquely grounded and globally recognisable. It is uniquely grounded because it now sits firmly within Nigeria's own statute and regulatory framework, rather than relying solely on subsidiary instruments or borrowed doctrines. It is familiar because the underlying principles closely resemble mainstream global privacy norms, including those reflected in UK GDPR guidance such as purpose limitation, data minimisation, storage limitation, security, and accountability.

That matters in practice. Nigerian businesses increasingly serve international customers, use offshore vendors, and undergo due diligence by overseas partners. A disciplined approach to minimisation and retention therefore has a dual benefit. It improves local compliance while also making the organisation more intelligible to foreign auditors, investors, and counterparties. Where a Nigerian entity can show that it collects only what is necessary, documents its lawful basis, communicates retention clearly, and deletes or de-identifies data appropriately, it is speaking a compliance language that resonates globally.

8. Consequences of getting it wrong

The legal risks are no longer theoretical. Under the Act, an aggrieved data subject may lodge a complaint with the Commission. The Commission may investigate, issue compliance orders, require the violation to be remedied, award compensation to affected individuals, and impose sanctions. A data subject who suffers injury, loss or harm may also recover damages in civil proceedings.

Against that backdrop, unnecessary collection and indefinite retention are particularly hard to justify. They can affect the regulator's view of proportionality, negligence, accountability, and the seriousness of the breach. They can also make remedial work more expensive. The larger and more diffuse the dataset, the harder the clean-up, the slower the access-response process, and the greater the cost of notification, review and containment.

9. Practical Tips

Below are actionable steps for both organizations and individuals, aligned with the Act and GAID 2025.

For Businesses and Organisations

- **Conduct a Data Audit:** Map out all the personal data you collect, why you collect it, and where it is stored. This helps you identify redundant or unjustified data.

- **Define Clear and Lawful Purposes:** Every data field must be tied to a legitimate business or legal purpose. If you cannot justify it, you should not collect it.

- **Minimise Data Collection:** Avoid "justincase" data gathering. Collect only what is essential for the service or transaction.

- **Restrict Access and Secure Storage:** Limit internal access strictly to those who need the data to perform their roles. Use secure, encrypted systems, not informal storage like personal drives or WhatsApp.

- **Encrypt and Anonymise Sensitive Data:** Protect highrisk identifiers such as NIN, BVN, and financial details. Where longterm storage is needed, anonymise or pseudonymise the dataset.

- **Train Staff and Conduct Regular Reviews:** Make minimisation part of your organisational culture. Carry out periodic compliance reviews and audits as required by the Commission.

For Individuals and Consumers

- **Share Personal Data Selectively:** Provide only the information necessary for the service. Challenge excessive or intrusive data requests.

- **Control Online and App Permissions:** Limit what apps and platforms can access. Reduce social media visibility and disable unnecessary permissions.

- **Strengthen Account Security:** Use strong passwords, avoid reusing them, and enable twofactor authentication wherever possible.

- **Exercise Your Data Rights:** Request access, correction, or deletion of your personal data when appropriate. Nigerian law gives you these rights, use them.

- **Delete Unused Accounts and Monitor for Breaches:** Close dormant accounts and keep an eye out for suspicious activity. Report concerns promptly.

10. Conclusion

Put simply, in Nigerian everyday language not every data field is your friend. If you do not genuinely need a piece of information, do not ask for it. And if the reason for holding that information has expired, do not keep it out of habit or convenience. At its core, data minimisation and retention discipline is really about restraint and it is that restraint that ultimately strengthens both compliance and security.

The Act and the GAID 2025 are unambiguous. Organisations are required to collect only what is necessary, retain personal data only for as long as it remains justified, and secure it appropriately throughout its lifecycle. For organisations that embrace this seriously, the benefits are significant: stronger defensibility, improved data quality, reduced breach exposure, clearer accountability, and deeper trust from customers, partners, and regulators.

Choosing to collect less is not a sign of fear or excessive caution. It is a clear indication that the organisation understands what lawful and responsible stewardship of personal data truly demands. And with the Commission increasing its audit activity and enforcement visibility, organisations should anticipate closer scrutiny of retention schedules, datamapping records, access controls, and the justification for every category of personal data collected.

REFERENCES

- Nigeria Data Protection Act 2023
- General Application and Implementation Directive (GAID) 2025
- National Information Technology Development Agency Act 2004
- CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT 2015, (AS AMENDED):
- Money Laundering (Prevention and Prohibition) Act 2022
- UK Information Commissioner's Office Data Minimisation Guidance

Disclaimer:

The information provided in this publication does not, and is not intended to constitute legal advice. It is intended for general informational purposes only. Please contact us for further information.

Contact us:

Lagos Office: No 13, Mustapha Street, Off Olanrewaju Street, Billingsway, Oregun, Ikeja, Lagos.
Abuja Office: No. 16, Nkwere Street, Area 11, Garki, Abuja, FCT.
Email: info@syntegrallp.com Telephones: 08025754547, 08023007172, 07015694060

© Copyright 2026 - Syntegral Legal Practice