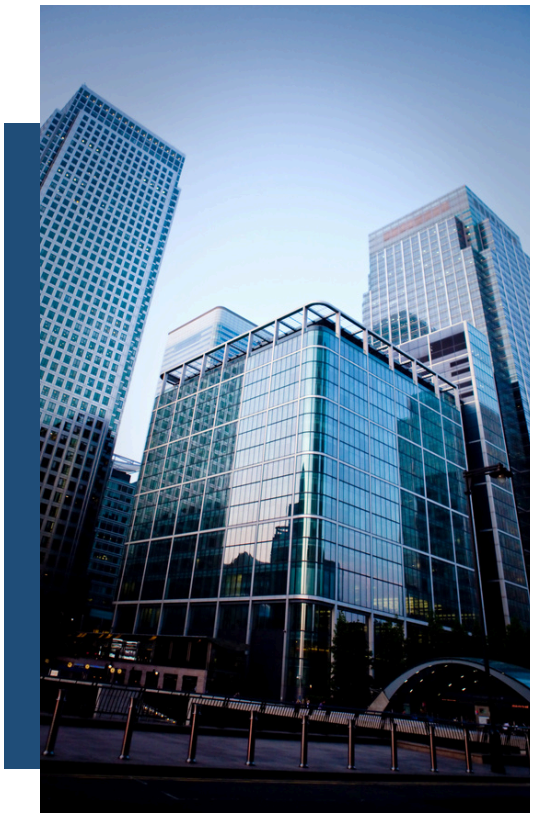
GOLDSMITHS

AFTER THE EXTENSION: A DATA PROTECTION PLAYBOOK FOR BANKS & FINTECHS

The extended deadline for the 2025 Compliance Audit Return has passed. For banks and FinTechs, the question is no longer simply whether a return was filed, but whether the data protection programme behind that filing can withstand regulatory scrutiny.



Data protection compliance in Nigeria has moved beyond simply having a privacy policy or obtaining consent from customers. The Nigeria Data Protection Act 2023 (NDPA) established the Nigeria Data Protection Commission (NDPC) and created a comprehensive statutory framework for the protection of personal data. The General Application and Implementation Directive 2025 ("GAID" or "Directive"), which took effect on 19 September 2025, turned this Act into the documented, auditable programme that now governs every Data Controller and Processor of Major Importance in the country. For banks and FinTechs, data protection compliance is therefore not simply another legal or IT issue. It is a governance, operational and reputational issue that should be receiving attention across all leadership cadres.

THE COMPLIANCE DEADLINE

The NDPC originally set 31 March 2026 as the deadline for filing the 2025 Compliance Audit Return (CAR), the annual filing through which Ultra-High and Extra-High Level registrants demonstrate to the Commission that their data protection framework is actually operating rather than merely documented. Following representations from stakeholders, the Commission extended that deadline to 30 May 2026. That extended deadline has now also passed. The GAID requires the audit process to address matters including lawful bases for processing, legitimate-interest assessments, data-subject rights, data-security measures, cross-border transfers and breach notification.

For organisations that filed their CAR on time, the filing should not be treated as the end of the compliance exercise. Rather, the audit trail submitted in May is now the baseline the NDPC will measure future conduct against. For organisations that missed the deadline, the issue should not simply be left unresolved. The GAID provides for an administrative penalty for late filing, in addition to the applicable CAR filing fee.

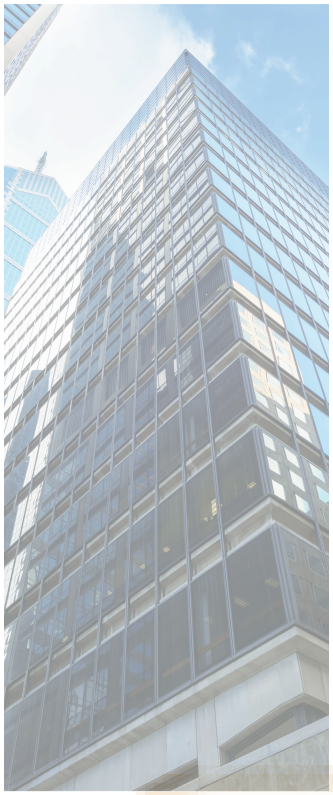
The practical approach is therefore to assess the reason for the delay, determine the applicable consequences and take steps to regularise the organisation's compliance position.

RETHINKING CONSENT

One of the most common data-protection mistakes financial institutions make, is treating consent as the default lawful basis for processing personal data. Consent is important, but it is not the only applicable or appropriate legal basis for every processing activity. The NDPA recognises several lawful bases for processing personal data. These include consent, performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest and legitimate interests. The GAID also provides guidance on legitimate-interest assessments and expects organisations relying on legitimate interests to properly assess and document that basis. Financial institutions are required to identify the lawful basis that genuinely supports each processing activity rather than merely asking for or relying on consent because it is familiar. This requires financial institutions to move beyond generic privacy notices and actually map their processing activities to the appropriate lawful bases.

THE ROLE OF THE DATA PROTECTION OFFICER

The Directive mandates the appointment of a Data Protection Officer (DPO). The DPO is expected to have appropriate independence, access to relevant processing activities and sufficient resources to perform the role effectively. Banks and Fintechs are advised against folding this role into an existing legal or compliance title without giving it the independence or the resourcing the Directive actually requires. A DPO who is responsible for identifying data protection failures must have sufficient independence to raise those concerns and sufficient access to understand how personal data is actually being processed within the organisation. The GAID also provides for an annual credential assessment process for DPOs, including continuing professional development and inclusion in the Commission's relevant database.



CROSS-BORDER DATA TRANSFERS

Modern banking and FinTech operations rarely operate entirely within one country. As a result, Nigerian customers' personal data may be transferred to, accessed from or processed in another jurisdiction. The NDPA and GAID regulate cross-border transfers of personal data and provide recognised mechanisms and lawful grounds for such transfers. The practical problem for many institutions is not necessarily that there is no legal basis for a particular transfer. The problem is that the organisation may be unable to clearly explain what that basis is and where the supporting documentation is. An institution using offshore cloud hosting for its core banking platform, or routing customer data through an international payment processor, should therefore not wait for a regulatory enquiry before being able to clearly explain what the legal basis for a particular data transfer is and where the supporting documentation is.

THE COST OF NON-COMPLIANCE

The Commission has statutory powers to investigate, issue compliance orders and impose penalties, and a Data Controller of Major Importance can face a penalty of up to Ten Million Naira or two percent of its preceding year's gross revenue, whichever is greater. For a bank or a fintech of any scale, the revenue-based calculation is the one that matters, and it is a considerably larger number than the flat penalty most compliance teams have in mind.

COMPLIANCE PRIORITIES FOR THE SECOND HALF OF 2026

The starting point is to confirm, precisely, which registration tier the institution falls into, since the obligations attaching to Ultra-High, Extra-High and Ordinary-High Level Data Controller or Processor of Major Importance differ. Where the 2025 CAR has not been filed, the right move is to determine the appropriate steps for regularisation and address any applicable late-filing consequences. Lawful-basis audit should be conducted with major processing activities reviewed and the lawful basis supporting each one identified. Particular attention should be paid to any process still resting on consent by default rather than by design. A DPO should be appointed where necessary and where there is a DPO, its function should be reviewed. It should be confirmed that the DPO has the appropriate independence, competence, resources and access to perform the role effectively. The organisation should also confirm that applicable credential-assessment and professional-development requirements are being addressed. Finally, cross-border transfer grounds should be documented vendor by vendor, so that the institution can answer, without delay, exactly which lawful basis supports each transfer of Nigerian customer data outside the country.

The era in which data protection could be reduced to a privacy policy and a consent checkbox is rapidly disappearing. The strongest compliance programmes are those that are documented, operational, tested and capable of being demonstrated to the regulator at any time. Financial institutions must note that the CAR may be an annual filing, but data-protection compliance is a year-round obligation.

Please note that the contents of this article are for general guidance on the Subject Matter. It is NOT legal advice.

For further information or to see our other service offerings, please visit www.goldsmithsllp.com or contact:

Shola Adekunle
Senior Associate
+234) 0201 291 7913
shola@goldsmithsllp.com

Uzoamaka Ugoh
Senior Associate
(+234) 0201 291 7913
uzoamaka@goldsmithsllp.com