© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723010

The Political Economy of Data Protection Governance in Africa: Institutional Revenue Generation, Regulatory Monetisation, and Comparative Compliance Design

ADEYEMI OWOADE

Abstract- ***Over the past five years, sub-Saharan Africa has produced one of the fastest-growing bodies of data protection legislation in the world, yet the institutional design underlying this expansion has received comparatively little scholarly attention. This article examines a structural feature that distinguishes several of the continent's leading data protection regimes from the European model that inspired them: the deliberate integration of fee-based revenue mechanisms into routine compliance workflows. Drawing on the statutory and regulatory architecture of Nigeria, Kenya, Tanzania, and Uganda, the article maps a common pattern of tiered enterprise registration fees, recurring renewal cycles, mandatory statutory audits, and privatised compliance intermediation, and situates this pattern within the broader political economy of regulatory finance in resource-constrained states. It then contrasts these monetised architectures with the European Union's accountability-based framework under the General Data Protection Regulation and the United Kingdom's lower-friction cost-recovery model, arguing that the European experience demonstrates that meaningful data protection compliance does not require upfront enterprise monetisation. The article concludes that, left unreformed, monetised registration and audit regimes risk converting data protection enforcement into a transactional exercise in fee collection, with disproportionate consequences for micro, small, and medium enterprises, and proposes a four-pillar reform agenda centred on budgetary independence for supervisory authorities, risk-based audit supervision, fee simplification, and outcome-oriented regulatory performance metrics.***

Keywords: Data Protection; Africa; Nigeria Data Protection Act; regulatory monetisation; GDPR; compliance costs; MSMEs; political economy of regulation; data protection authorities

I. INTRODUCTION

The rapid expansion of Africa's digital economy has been accompanied by an equally rapid wave of data protection legislation. By early 2026, forty-five of Africa's fifty-four states had enacted comprehensive data protection statutes, and thirty-nine had established functioning national data protection authorities (DPAs) tasked with safeguarding privacy rights, regulating cross-border data flows, and securing digital infrastructure[1] Yet an examination of how these statutes are operationalised in practice reveals a structural divergence from the international legislative paradigm that most of them profess to follow, namely the European Union's General Data Protection Regulation ('GDPR').[2]

In several prominent African jurisdictions, most notably Nigeria, Kenya, Tanzania, and Uganda, data protection compliance frameworks have increasingly integrated revenue-generating mechanisms directly into the machinery of regulatory oversight. Rather than relying solely on central government appropriations or ex-post punitive fines to fund supervisory capacity, these states have built statutory registration fees, recurring renewal cycles, mandatory audit filings, and, in at least one case, a licensed market of private compliance intermediaries into the ordinary business of becoming and remaining a compliant data controller or processor. This monetisation raises questions that sit at the intersection of administrative law, regulatory theory, and public finance: does the fee serve, as classical public-finance theory would suggest, as a

[1] Nixon Kanali, '45 African Countries Have Enacted Data Protection Legislation, Yellow Card Report' (TechTrends Kenya, 23 April 2026), reporting findings of Yellow Card, '2026 Report on Data Protection and Artificial Intelligence Governance in Africa' (Yellow Card, 22 April 2026) <https://techtrendske.co.ke/2026/04/23/45-african-countries-have-enacted-data-protection-legislation-yellow-card-report/> accessed 31 August 2026.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723010

proportionate charge for a service rendered by the state?[3] Or does it function, as this article argues, as a form of indirect taxation on formal business activity, with second-order effects on enterprise compliance behaviour and, ultimately, on the substantive protection of data subjects?

This article proceeds in five parts. Part II maps the statutory architecture of monetised data governance in Nigeria, Kenya, Tanzania, and Uganda, focusing on registration tiers, renewal cycles, audit obligations, and the treatment of enterprises that act simultaneously as controllers and processors. Part III offers a mechanistic analysis of how these architectures shape enterprise compliance behaviour, with particular attention to the disproportionate burden imposed on micro, small, and medium enterprises ('MSMEs') and the emergence, in Nigeria, of a privatised compliance-audit market. Part IV contrasts these monetised models with the European Union's accountability-based framework and the United Kingdom's hybrid cost-recovery model, asking whether upfront enterprise monetisation is in fact a precondition for effective data protection enforcement. Part V proposes a four-pillar reform agenda, and Part VI concludes.

II. ARCHITECTURE OF MONETISED DATA GOVERNANCE IN SELECTED AFRICAN JURISDICTIONS

The monetisation of privacy compliance across sub-Saharan Africa manifests through a recurring set of administrative instruments: tiered enterprise registration fees, recurring operational renewals, mandatory statutory audit filings, and, in the Nigerian case, a specialised licensing scheme for private compliance service providers. The administrative logic relies on two parallel channels of revenue extraction. Regulated entities pay statutory registration and renewal fees directly to the national data protection authority, while, in Nigeria, they simultaneously remit commercial audit fees to privatised compliance intermediaries who are themselves licensed by, and pay licensing fees to, the state regulator. These dual revenue flows are directed into consolidated national revenue funds or dedicated agency accounts, embedding institutional incentives around fee collection alongside the ordinary business of regulatory oversight.

A. Nigeria: The Tiered DCPMI Framework and the DPCO Intermediary Model

Nigeria's data protection framework was substantially modernised by the enactment of the Nigeria Data Protection Act 2023 ('NDPA') and the subsequent issuance, on 20 March 2025, of the General Application and Implementation Directive ('GAID') by the Nigeria Data Protection Commission ('NDPC').[4] The GAID, which entered into force on 19 September 2025 following a six-month transitional window, replaced the former Nigeria Data Protection Regulation 2019 ('NDPR') and its Implementation Framework, and gives operational content to the statutory category of 'Data Controller or Processor of Major Importance' ('DCPMI') introduced by section 65 of the NDPA.[5]

Under the NDPA and its implementing guidance, any entity that processes the personal data of more than two hundred data subjects within a rolling six-month period, or that operates within a designated critical sector such as financial services, telecommunications, energy, or healthcare, is required to register as a DCPMI, regardless of whether it maintains a physical presence in Nigeria.[6]

---

[3] The classical distinction between a regulatory fee, calibrated to the cost of the service rendered, and a disguised tax, calibrated to revenue-raising objectives, is long-established in public finance and administrative law scholarship. See generally George J Stigler, 'The Theory of Economic Regulation' (1971) 2 Bell Journal of Economics and Management Science 3, on the tendency of regulatory institutions to be captured by, or to develop institutional interests that align with, the parties or activities they were established to supervise.

[4] Nigeria Data Protection Commission, General Application and Implementation Directive 2025 ('GAID'), issued 20 March 2025. See 'Navigating The Nigeria Data Protection Act General Application And Implementation Directive (NDPA-GAID): A Guide For Businesses' (Mondaq, 20 October 2025) <https://www.mondaq.com/nigeria/privacy-protection/1693812/navigating-the-nigeria-data-protection-act-general-application-and-implementation-directive-ndpa-gaid-a-guide-for-businesses> accessed 31 August 2026.

[5] ibid. See also NDPA (n 5), s 65; GAID (n 6), art 3(3), art 8.

[6] 'NDPC Issues Guidance Notice on the Registration of Data Controllers and Processors of Major

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723010

The NDPC further subdivides DCPMIs into three operational tiers (Ultra-High Level, Extra-High Level, and Ordinary-High Level) calibrated by reference to the volume of data subjects processed and, for certain sectors, the inherent sensitivity of the data involved, with the precise numerical thresholds and associated registration fees set out in the schedules to the GAID.[7] Under the registration fee schedule originally issued alongside the DCPMI framework, Ordinary-High Level entities pay an annual registration fee of ₦10,000 (approximately US$6.84), Extra-High Level entities pay ₦100,000 (approximately US$68), and Ultra-High Level entities, a category encompassing large commercial banks, telecommunications operators, multinational corporations, and payment gateways, pay ₦250,000 (approximately US$171).[8] However, where the company has been incorporated with the Corporate Affairs Commission (CAC) before 2023 and failed to register with NDPC within 6 months of its incorporation, it will pay a default fee, which is 50 per cent of the registration fee.

The GAID substantially raised the cost of the second, and arguably more consequential, statutory obligation: the annual Compliance Audit Return ('CAR'). Ultra-High Level and Extra-High Level DCPMIs, having registered once, must thereafter file a CAR with the NDPC on or before 31 March of each year, executed exclusively through a licensed Data Protection Compliance Organisation ('DPCO').[9] Whereas the CAR filing fee under the former NDPR regime topped out at ₦20,000, the GAID's revised schedule now runs from a floor of roughly ₦100,000 up to ₦1,000,000 for the highest-volume Ultra-High-Level entities, a fee that is payable directly to the NDPC in addition to whatever commercial fee the DPCO itself charges for conducting the underlying audit.[10] DPCOs, third-party law firms, consultancies, and IT audit practices licensed by the NDPC under section 33 of the NDPA, charge regulated entities separate commercial service fees for conducting the audit itself, with practitioner commentary reporting engagement fees ranging from roughly ₦350,000 for smaller organisations to several million naira for larger, higher-risk engagements, on top of the statutory filing fee owed to the NDPC.[11] Failure to file the CAR, in addition to the late-filing surcharge, exposes a DCPMI to a fine of up to ₦10,000,000 or

---

Importance' (Andersen Nigeria) <https://ng.andersen.com/ndpc-issues-guidance-notice-on-the-registration-of-data-controllers-and-processors-of-major-importance/> accessed 31 August 2026; GAID (n 6), art 8 (extending the extraterritorial reach of the DCPMI classification to entities targeting Nigerian data subjects without a physical presence).

[7] The precise data-subject thresholds separating the three tiers have been described inconsistently across NDPC guidance issued at different points between 2023 and 2025; compare 'NDPC Registration: Who Must Register and How (2026 Guide)' <https://ndprtoolkit.com.ng/blog/ndpc-registration-guide-2026/> accessed 31 August 2026 with the Mondaq guide (n 6).

[8] 'Data protection laws in Nigeria' (DLA Piper Data Protection Laws of the World) <https://www.dlapiperdataprotection.com/index.html?t=law&c=NG> accessed 31 August 2026; Andersen Nigeria (n 8).

[9] 'Nigeria: NDPC Issues GAID – Key Compliance Insights' (Privacy Matters, DLA Piper, 3 June 2025) <https://privacymatters.dlapiper.com/2025/06/nigeria-ndpc-issues-gaid-key-compliance-insights/> accessed 31 August 2026; 'What You Should Know About The New Data Protection Compliance Audit Regime In Nigeria' (Mondaq, 21 January 2026) <https://www.mondaq.com/nigeria/data-protection/1734060/what-you-should-know-about-the-new-data-protection-compliance-audit-regime-in-nigeria> accessed 31 August 2026.

[10] ibid (Privacy Matters); 'Data Protection Compliance In Nigeria: Audit Return Obligations For 2026' (Mondaq, 28 January 2026) <https://www.mondaq.com/nigeria/data-protection/1736914/data-protection-compliance-in-nigeria-audit-return-obligations-for-2026> accessed 31 August 2026 (late filing after the statutory deadline attracts a further administrative fee of up to 50% of the applicable filing fee).

[11] 'DPCO Nigeria: What They Do and How to Choose the Right One' (Janus Compliance, 20 March 2026) <https://www.januscompliance.co.uk/blog/dpco-nigeria-what-they-do-and-how-to-choose-one> accessed 31 August 2026; NDPA (n 5), s 33; 'DPCO Registration & Requirements' (Nigeria Data Protection Commission) <https://ndpc.gov.ng/dpco-registration-requirements/> accessed 31 August 2026.

2% of the defaulting entity's annual gross revenue in the preceding financial year, whichever is greater.[12]

B. Kenya: Dual-Role Licensing and Sectoral Mandates

Kenya's Data Protection Act 2019[13] is operationalised through the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021, made under section 17 of the Act and administered by the Office of the Data Protection Commissioner ('ODPC').[14] Kenya's model combines structural headcount and turnover thresholds with compulsory sectoral triggers. An organisation operating within one of eighteen designated sectors, including financial services, telecommunications, healthcare, direct marketing, and transport, is subject to mandatory registration irrespective of its size or turnover; an organisation outside those sectors becomes subject to mandatory registration only where it employs more than ten staff or achieves an annual turnover exceeding KES 5,000,000, and remains exempt from the registration fee, though not from the substantive obligations of the Act, if it falls below both thresholds.[15]

The ODPC operates a tiered fee structure, with registration certificates valid for a two-year cycle. Large entities, those with more than ninety-nine employees and turnover above KES 50 million, pay a registration fee of KES 40,000 and a biennial renewal fee of KES 25,000. Micro, small, and non-profit entities, and public bodies, pay a substantially lower registration fee of KES 4,000 and a renewal fee of KES 2,000,[16] with intermediate fee bands applying to medium-sized entities. Where an enterprise acts simultaneously as a data controller, determining the purposes of processing, and as a data processor, processing personal data on behalf of a third party, the Regulations require separate registration, and separate fee payment, in each distinct legal capacity.[17] Operating without a valid registration is a criminal offence, punishable by a fine of up to KES 3,000,000, imprisonment of up to ten years, or both, in addition to administrative penalties of up to KES 5,000,000 or 1% of the entity's annual gross turnover.[18] Enforcement has intensified markedly: in 2025, the ODPC roughly doubled the number of enforcement determinations it issued in 2024 and imposed fines exceeding a combined KES 26 million.[19]

C. Tanzania: Five-Year Licensing Tiers and Financial Statement Verification

Tanzania's Personal Data Protection Act No 11 of 2022[20] is operationalised by the Personal Data Protection Commission ('PDPC'), which formally commenced full enforcement on 3 April 2024, and by the Data Protection (Collection and Processing of Personal Data) Regulations 2023[21], under which all legal entities, public bodies, and non-governmental

[12] Mondaq, 'Audit Return Obligations For 2026' (n 12).

[13] Data Protection Act 2019 (Kenya).

[14] Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 (Legal Notice No 207 of 2021, Kenya), which took effect on 14 July 2022. See 'Registration as a Data Controller and Data Processor in Kenya with the ODPC' (Njaga Advocates) <https://njagaadvocates.com/registration-as-a-data-controller-and-data-processor-in-kenya-with-the-odpc/> accessed 31 August 2026.

[15] 'Data Protection Compliance in Kenya for Foreign Companies' (Manwa Advocates, 6 July 2026) <https://manwaadvocates.com/data-protection-compliance-in-kenya-for-foreign-companies/> accessed 31 August 2026; Njaga Advocates (n 15).

[16] 'Data Controller Registration | 11 Must Know Requirements' (CM Advocates LLP) <https://cmadvocates.com/blog/registration-of-data-controllers-and-data-processors/> accessed 31 August 2026 (large-entity fees); 'Registration of Data Controllers and Processors with the ODPC' (KO Associates) <https://koassociates.co.ke/insight/3-registration-of-data-controllers-and-processors-with-the-odpc/> accessed 31 August 2026 (micro/small-entity fees).

[17] Njaga Advocates (n 15); Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 (n 15).

[18] 'Mandatory Registration of Data Controllers and Processors' (MWC Legal) <https://mwc.legal/mandatory-registration-of-data-controllers-and-processors/> accessed 31 August 2026.

[19] 'Data Protection Compliance in Kenya for Foreign Companies' (n 16).

[20] Personal Data Protection Act No 11 of 2022 (Tanzania), which entered into force on 1 May 2023 by Government Notice No 326 of 2023.

[21] Data Protection (Collection and Processing of Personal Data) Regulations 2023 (GN No 349 of

organisations acting as data controllers or processors must register before collecting or processing personal data.

The PDPC's registration fee scale, valid for a five-year cycle, is calibrated by employee headcount and turnover. Small-scale controllers or processors, with between one and forty-nine employees and turnover below TZS 100 million, pay a registration fee of TZS 100,000 and a renewal fee of TZS 50,000; medium-scale entities pay TZS 200,000; and large-scale entities, with at least one hundred employees and turnover exceeding TZS 500 million, pay TZS 1,000,000, the highest tier in the schedule.[22] Public and non-commercial bodies pay between TZS 100,000 and TZS 500,000 depending on institutional scale. To verify an applicant's correct tier, the PDPC requires submission of certified financial audit reports alongside legal incorporation documents, and, where an entity performs dual functions as both controller and processor, it must obtain two separate certificates, doubling its cost exposure to as much as TZS 2,000,000.[23] Failure to complete registration by the statutory deadline exposes an entity to fines ranging from TZS 100,000 to TZS 5,000,000 for standard registration defaults, and to administrative corporate fines of up to TZS 5 billion (approximately US$1.93 million) for broader statutory violations.[24]

D. Uganda: Uniform Annual Fees and Adjacent Telecommunications Levies

Uganda's Data Protection and Privacy Act 2019[25] mandates online registration, through the Personal Data Protection Office ('PDPO'), for every public and private entity that collects or processes the personal data of Ugandan citizens or residents, including entities established outside Uganda that process such data.[26] Unlike the tiered structures adopted in Nigeria, Kenya, and Tanzania, the PDPO applies a uniform statutory registration fee of UGX 100,000 (approximately US$28–30) to every qualifying entity, together with an annual renewal fee of the same amount required to maintain valid status on the national data protection register; a certified copy of an entry in the public register attracts a further fee of UGX 25,000.[27]

Uganda's digital ecosystem also illustrates how data-related compliance monetisation extends beyond the data protection statute itself into adjacent telecommunications regulation. Commercial entities using Application-to-Person enterprise SMS for customer communication must register alphanumeric Sender IDs with telecommunications operators under the oversight of the Uganda Communications Commission, and, unlike comparable regional regimes that impose a one-off registration fee, Uganda imposes a recurring monthly maintenance

2023, Tanzania); 'Legal Alert: Data Controllers & Processors Registration in Tanzania Begins as the Personal Data Protection Commission Becomes Fully Operational' (Victory Attorneys, 28 March 2024) <https://victoryattorneys.co.tz/2024/03/28/legal-alert-data-controllers-processors-registration-in-tanzania-begins-as-the-personal-data-protection-commission-becomes-fully-operational/> accessed 31 August 2026.

[22] 'A guide to initial compliance with Tanzania's Data Protection Act' (Afriwise) <https://www.afriwise.com/blog/regulatory-and-compliance-update-a-guide-to-initial-compliance-with-tanzanias-data-protection-act> accessed 31 August 2026.

[23] Ibid.

[24] 'Registration for Companies under Data Protection Law Extended' (LexAfrica, 20 March 2026) <https://lexafrica.com/2025/01/registration-for-companies-data-protection-law/> accessed 31 August 2026; 'Data protection laws in Tanzania' (DLA Piper Data Protection Laws of the World) <https://www.dlapiperdataprotection.com/?c=TZ&t=l> accessed 31 August 2026.

[25] Data Protection and Privacy Act 2019 (Uganda) ('DPPA').

[26] 'Uganda: Data Protection Regulator Clarifies Compliance Requirements for Offshore Entities' (Privacy Matters, DLA Piper, 6 August 2025) <https://privacymatters.dlapiper.com/2025/08/uganda-data-protection-regulator-clarifies-compliance-requirements-for-offshore-entities/> accessed 31 August 2026.

[27] 'How to register with Uganda's Personal Data Protection Office' (ITLawCo) <https://itlawco.com/how-to-register-with-ugandas-personal-data-protection-office/> accessed 31 August 2026; 'Beat the Data Protection Registration Deadline' (MMAKS Advocates) <https://www.mmaks.co.ug/sites/default/files/article-attachments/beat-data-protection-registration-deadline.pdf> accessed 31 August 2026.

fee of approximately UGX 250,000 (US$65–70) per registered Sender ID,[28] demonstrating how privacy-adjacent compliance obligations can overlap with sectoral communications monetisation to compound the cumulative cost of doing business. Enforcement of the underlying registration obligation is also increasingly criminal rather than purely administrative in character: in July 2025, a Ugandan court convicted, by plea bargain, the director of a microfinance lender for failing to register with the PDPO and for unlawfully disclosing a borrower's personal data, imposing a fine of UGX 300,000, while the DPPA separately provides for fines of up to 240 currency points (approximately UGX 4.8 million) or imprisonment of up to ten years for the unlawful obtaining or disclosure of personal data.[29]

III. MECHANISTIC ANALYSIS OF REGULATORY MONETISATION: 'STEALTH TAXATION' VERSUS RIGHTS SAFEGUARDING

The economic design of these regimes reflects a structural choice about how the state finances an administrative function, data protection supervision, that did not previously exist as a discrete regulatory field in most of these jurisdictions. Analysed together, the four architectures reveal a common cycle. Statutory instruments first establish broad registration and audit requirements across all data-handling entities. This enables the state regulator to extract direct statutory fees, and, in Nigeria, allows private consultants to capture secondary audit rents. Enterprises respond by allocating compliance budgets primarily toward administrative filing costs rather than toward substantive privacy engineering, and, over time, the regulator's own performance incentives can shift toward fee-collection totals and certificate issuance volumes rather than toward the investigation of data breaches or the remediation of consumer complaints.

A. Regulatory Rent-Seeking and the Nigerian 'Double-Rent' Intermediary Market

In conventional administrative law theory, a regulatory fee is intended to offset the direct cost incurred by a state agency in processing an application or delivering a specific regulatory service.[30] In Nigeria, however, the interaction between the NDPC's own statutory fee schedule and the privatised DPCO audit market produces what might be described as a double-rent structure. The NDPC extracts a statutory registration fee from data controllers of up to ₦250,000, and, since the GAID, a separate CAR filing fee that can reach ₦1,000,000 for the highest-volume entities,[31] while simultaneously licensing and collecting licensing fees from the DPCO consultancies through which that CAR must be filed.[32] The DPCOs, in turn, capture a further, privatised regulatory rent by charging the same regulated entity a separate commercial audit fee, often running into the hundreds of thousands or low millions of naira, to conduct the underlying compliance audit that the CAR merely records.[33] The result is an ecosystem in which private audit intermediaries depend for their revenue on a mandatory state filing requirement, while the state delegates the substance of preliminary audit oversight to those same private actors. A regulated entity therefore effectively pays twice for the same underlying compliance event: once to a private, state-licensed gatekeeper to obtain the audit itself, and again to the state Treasury to record that the audit has occurred.

B. Compliance Friction, Enterprise Behaviour, and the MSME Disadvantage

The structural monetisation of data protection compliance tends to convert what is, in substance, a rights-protective exercise into an administrative cost centre. Where compliance is measured chiefly by the possession of a paid registration certificate, a filed financial audit return, and a stamped annual renewal, regulated entities have every incentive to prioritise fiscal settlement over the deeper structural reforms

[28] 'Uganda SMS Compliance: UCC Sender ID and DPPA Requirements' (Telerivet) <https://www.telerivet.com/blog/uganda-sms-compliance-ucc-dppa> accessed 31 August 2026.

[29] 'Data Protection Obligations in Uganda (DPPA)' (Wakilii, 6 July 2026) <https://wakilii.org/knowledge/data-protection-uganda> accessed 31 August 2026, discussing Uganda v Ronald Mugulusi (Makindye Standards, Wildlife and Utilities Court, 10 July 2025); DPPA (n 20), s 35(2).

[30] Stigler (n 3).

[31] See section II(A) above.

[32] NDPC, 'DPCO Registration & Requirements' (n 14).

[33] Janus Compliance (n 13).

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723010

that actually reduce privacy risk, privacy-by-design architecture, data minimisation, and automated subject-access-request handling among them.

These monetised structures also bear disproportionately on MSMEs. Large corporations absorb tier-one registration fees and audit consultancy costs as a routine, and comparatively immaterial, operating expense; MSMEs, by contrast, face a materially higher relative cost burden.[34] A Kenyan fintech start-up with twelve employees and KES 5,500,000 in annual revenue, for instance, may be required to pay a KES 40,000 registration fee if it acts in dual roles as both controller and processor, on top of whatever legal and compliance costs it incurs in preparing its registration documentation and internal privacy documentation.[35] Commentary from Kenyan practitioners advising smaller businesses increasingly frames data protection registration as an unavoidable cost of doing business rather than a discretionary compliance choice, reflecting the ODPC's intensified enforcement posture.[36] In response to this friction, many MSMEs either restructure their operational headcount or revenue reporting to avoid regulatory visibility, or continue to operate in informal, non-compliant status altogether. These dynamic risks the perverse outcome of driving small enterprises into shadow operation, leaving the data subjects whose information they process with less actual privacy protection than they would enjoy under a non-fee, risk-tiered supervisory regime that reserved its scrutiny for higher-risk processing activity regardless of the size of the entity conducting it.

IV. COMPARATIVE ANALYSIS: NON-FEE AND LOW-FEE ACCOUNTABILITY FRAMEWORKS

To evaluate whether high levels of data protection compliance require mandatory registration and audit fees of the kind described in Part II, the monetised African models can usefully be contrasted with the structural design of the European Union's GDPR and the United Kingdom's hybrid cost-recovery framework. The European accountability architecture operates on a fundamentally different logic. By abolishing generalised notification fees, the GDPR eliminates upfront financial barriers to market entry; entities instead maintain internal compliance documentation, and supervisory authorities rely on direct government funding to perform targeted, ex-post investigations, backed by high-deterrence statutory fines calibrated to penalise substantive violations rather than the mere non-payment of an administrative fee.

A. The European Union: Abolition of Registration and the Accountability Principle

Prior to the GDPR, several European jurisdictions operating under the earlier Data Protection Directive 95/46/EC maintained national notification regimes requiring data controllers to pay administrative processing fees to their supervisory authorities.[37] The GDPR deliberately abolished these general notification requirements, the European Parliament and Council having concluded that universal registration schemes generated administrative burden without materially improving privacy outcomes. In their place, the GDPR established what is generally described as the accountability principle, codified in Article 5(2)[38]entities are not required to register with, or pay recurring compliance fees to, national data protection authorities, nor to submit annual third-party compliance audit filings to the state. Instead, they must internally document their processing activities through Records of Processing Activities

[34] 'How to Register with Uganda's Personal Data Protection Office (PDPO)' (Global Advisory Experts, 15 June 2026) <https://globaladvisoryexperts.com/how-to-register-with-pdpo-uganda/> accessed 01 September 2026, noting the recurring nature of the compliance burden for smaller entities; see also 'Registration as a Data Controller and Data Processor in Kenya with the ODPC' (n 15).

[35] See section II(B) above; CM Advocates LLP (n 16).

[36] 'Why Kenya's Small Businesses Can No Longer Ignore Data Protection' (MNW Law, 25 March 2026) <https://mnwlaw.co.ke/2026/03/25/why-kenyas-small-businesses-can-no-longer-ignore-data-protection/> accessed 01 September 2026.

[37] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, art 18 (notification requirement, subsequently abolished by the GDPR).

[38] GDPR (n 2), art 5(2).

under Article 30[39]execute Data Protection Impact Assessments for high-risk processing under Article 35[40], and, where required, designate a Data Protection Officer under Article 37.[41] Supervisory authorities across the Union (including the Commission Nationale de l'Informatique et des Libertés in France, the Federal Commissioner for Data Protection and Freedom of Information in Germany, and the Data Protection Commission in Ireland) are funded through direct fiscal allocation from national state budgets rather than through enterprise registration collections,[42] and compliance is enforced through ex-post supervisory investigation, risk-based sectoral audits, and the handling of individual data-subject complaints, backed by punitive fines under Article 83 of up to €20 million or 4% of an undertaking's total global annual turnover, whichever is higher.[43]

B. The United Kingdom: A Low-Friction Cost-Recovery Fee without an Intermediary Audit Market

The United Kingdom presents a hybrid framework that sits between the two poles. Under the Data Protection (Charges and Information) Regulations 2018, the Information Commissioner's Office ('ICO') requires most data controllers to pay an annual Data Protection Fee, structured across three tiers by headcount and turnover.[44] The original 2018 fee schedule set Tier 1 (micro-organisations) at £40 per annum, Tier 2 (small and medium organisations) at £60, and Tier 3 (large organisations, broadly those with turnover above £36 million or more than 250 staff) at £2,900.[45] Those figures were revised upward by 29.8%, with effect from 17 February 2025, by the Data Protection (Charges and Information) (Amendment) Regulations 2025, which substituted new charges of £52, £78, and £3,763 for the three tiers respectively, to reflect movement in the Retail Price Index since 2018; each figure is reduced by a further £5 where payment is made by direct debit.[46] While the UK model therefore does impose a mandatory enterprise fee, unlike the EU's fully fee-free approach, it differs from the monetised African regimes described in Part II in two material respects. First, the UK framework does not mandate that data controllers file annual compliance audit returns through licensed private third-party intermediaries; the fee paid to the ICO is a direct cost-recovery charge that funds public supervisory operations, without the intervening layer of privatised audit rent-capture that characterises the Nigerian DPCO model.[47] Second, the baseline Tier 1 fee, even after the 2025 uplift, remains nominal at £52 per annum, preventing the kind of administrative friction or barrier-to-entry distortion that the Nigerian, Kenyan, and Tanzanian fee schedules impose on MSMEs entering the formal digital economy.

C. Efficacy Assessment: Compliance without Upfront Enterprise Monetisation

A comparison across the three models suggests that upfront regulatory monetisation is not a precondition for achieving legal compliance or for securing strong data-subject protections. Under the monetised African model, the primary statutory mandate is upfront enterprise registration and periodic third-party statutory audit, with an ex-ante, annually recurring audit obligation prepared by a licensed private broker; the principal revenue destination is a mix of consolidated state revenue and the DPA's own operational budget, supplemented, in Nigeria, by a private brokerage industry; and the principal distortion risk is that compliance is reduced to a form of pay-to-play administrative status, with MSMEs

[39] ibid, art 30.
[40] ibid, art 35.
[41] ibid, art 37.
[42] GDPR (n 2), art 52(4), requiring each Member State to ensure its supervisory authority is provided with adequate financial resources from its general state budget.
[43] GDPR (n 2), art 83(5).
[44] Data Protection (Charges and Information) Regulations 2018, SI 2018/480, reg 3(1).
[45] ibid.
[46] Data Protection (Charges and Information) (Amendment) Regulations 2025, SI 2025/63; 'Rise in ICO Data Protection Fees from February 2025' (Acuity Law, 13 February 2025) <https://acuitylaw.com/rise-in-ico-fees-data-protection-fees-february/> accessed 01 September 2026; 'ICO registration and the 2026 data protection fee explained' (31 July 2026) <https://ico.opencourtdata.uk/do-i-need-to-register-with-the-ico> accessed 01 September 2026, confirming no further amendment as at mid-2026.
[47] 'Guide to the data protection fee' (ICO) <https://ico.org.uk/for-organisations/data-protection-fee/data-protection-fee/> accessed 01 September 2026.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723010

pushed toward informality.[48] Under the EU's accountability framework, by contrast, the primary statutory mandate is the internal demonstration of compliance rather than an external, fee-generating filing; the cost to the enterprise is confined to internal operational and compliance expenditure rather than a direct state fee; the audit mechanism is ex-post and risk-based, triggered by breaches, complaints, or sectoral risk indicators rather than by an annual filing calendar; and the principal distortion risk lies instead in the administrative burden of maintaining internal Records of Processing Activities and Data Protection Impact Assessment documentation to a standard that would withstand ex-post scrutiny.[49] The UK's hybrid model occupies an intermediate position: a modest, direct cost-recovery fee funds ICO operations without a mandatory audit-brokerage market, and enforcement remains ex-post and complaint- or breach-triggered, producing what practitioner and regulatory commentary consistently describes as minimal administrative friction relative to the fee's revenue-raising function.[50]

The European experience suggests that high rates of data privacy compliance are achievable through mechanisms other than revenue extraction: the deterrent effect of proportionate, turnover-linked penalties under Article 83, which forces corporate governance structures to internalise privacy risk at board level; the structural integration of independent Data Protection Officers within enterprise management under Article 37; and an active ecosystem of civil-society oversight, individual complaint mechanisms, and, increasingly, collective redress litigation, which sustains continuous supervisory pressure on data controllers independently of any registration cycle. Monetised registration frameworks, by contrast, risk substituting substantive privacy enforcement with the accumulation of administrative compliance receipts; organisations may prioritise securing a registration certificate or an audit trustmark sufficient to avoid an immediate statutory fine[51], while the underlying internal processing practices that the certificate is supposed to attest to remain substantively unmonitored until a breach forces the issue into the open.

V. STRATEGIC POLICY REFORM AGENDA FOR AFRICAN DATA PRIVACY REGIMES

Aligning African data protection governance with international best practice, while preserving a degree of administrative self-sustainability appropriate to fiscally constrained supervisory authorities, does not require the wholesale abolition of every fee described in Part II. It does, however, warrant structural reform across four pillars.

First, national parliaments should decouple DPA operational budgets from registration and intermediary audit fee revenue. Providing supervisory authorities with direct budgetary allocations from consolidated state funds, even if only partial, would begin to remove the structural dependence of DPAs on registration volumes and licensing collections, enabling an institutional reorientation away from revenue targets and toward active enforcement, rights protection, and breach prevention.

Second, regulatory authorities should replace universal, annual, mandatory audits with targeted, risk-based supervision. Frameworks that require every DCPMI, regardless of demonstrated risk, to file an annual third-party compliance audit return (as Nigeria's DPCO model currently does for Ultra-High Level and Extra-High Level entities) should transition toward a model in which internal compliance documentation suffices for lower-risk entities, reserving mandatory external audit for high-risk processing operations, large-scale biometric deployments, or entities with a documented history of prior compliance violations.

Third, governments should simplify fee schedules to reduce financial friction for growing businesses. The administrative practice, common to Kenya and Tanzania, of requiring a single enterprise that performs both controller and processor functions to pay separate registration and renewal fees for each capacity should be reconsidered, and baseline exemption thresholds should be periodically reviewed and, where appropriate, raised, to protect early-stage micro-enterprises and non-profit organisations from registration costs disproportionate to their scale.

[48] See section III above.
[49] See section IV(A) above.
[50] ICO (n 40).
[51] Janus Compliance (n 13).

Fourth, data protection commissions should reorient their institutional key performance indicators away from revenue collection totals and certificate issuance volumes. Supervisory effectiveness is better measured by average breach-investigation response times, the issuance and enforcement of binding corrective orders, measurable improvements in public privacy literacy, and the timely resolution of individual data-subject complaints; metrics that track the substantive purpose of the legislation rather than the fiscal health of the regulator.

VI. CONCLUSION

The emergence of monetised data protection regimes across sub-Saharan Africa represents a distinctive institutional response to a genuine fiscal constraint: the need to fund a newly created category of regulatory supervision in states where general budgetary allocation to nascent agencies is often unreliable. Driven by that constraint, Nigeria, Kenya, Tanzania, and Uganda have each built tiered registration fees, recurring renewal schedules, and, in Nigeria's case, a privatised compliance-audit industry, into the statutory architecture of data protection enforcement.

These mechanisms provide short-term operational funding for regulatory authorities that might otherwise struggle to establish supervisory capacity at all. But left unreformed, they risk transforming data privacy enforcement into a transactional, revenue-focused exercise, in which regulated entities come to treat mandatory fees and third-party audit returns as routine operational expenses to be minimised, rather than as catalysts for the deeper structural privacy transformation the legislation was designed to compel. As the European Union's accountability-based framework, and to a lesser degree the United Kingdom's low-friction cost-recovery model, demonstrate, robust data privacy compliance does not depend on upfront enterprise registration fees or statutory audit-filing schemes; it is driven instead by systemic corporate accountability, risk-based supervisory oversight, and credible, proportionate enforcement.

For African jurisdictions seeking to build data protection frameworks capable of sustaining, rather than taxing, dynamic and globally competitive digital economies, reforming supervisory financing to emphasise substantive data-subject rights over administrative fee extraction is not merely a matter of regulatory aesthetics. It is a precondition for ensuring that the considerable legislative achievement represented by forty-five national data protection statutes translates into the substantive privacy protection those statutes were enacted to deliver.