



Data Governance and Privacy Regulation in Africa

GDPR Influence and African Contexts: A South Sudan Case Study

Abraham Kuol Nyuon (Ph.D)^{1,2,3}

¹ Associate Professor of Politics, Peace, and Security

² Principal, Graduate College, University of Juba

³ SUSI Scholar on U.S. Foreign Policy

Correspondence: nyuonabraham@gmail.com

Published: 01 January 2021 **Received:** 03 September 2020

Accepted: 13 November 2020 **DOI:**
[10.5281/zenodo.19550091](https://doi.org/10.5281/zenodo.19550091)

Author notes

Abraham Kuol Nyuon (Ph.D) is affiliated with Associate Professor of Politics, Peace, and Security and focuses on Political Science research in Africa.

ABSTRACT

This article examines Data Governance and Privacy Regulation in Africa: GDPR Influence and African Contexts: A South Sudan Case Study with a focused emphasis on South Sudan within the field of Political Science. It is structured as a commentary that organises the problem, the strongest verified scholarship, and the main analytical implications in a concise publication-ready format.

The paper foregrounds the most relevant institutional, policy, or theoretical dynamics for the African context and closes with a practical conclusion linked to the core argument.

Keywords: *Africa GDPR Influence, South Sudan Case, Sudan Case Study, Data Governance, Privacy Regulation, Africa GDPR*

Article Highlights

- Examines GDPR influence in fragile, post-conflict African contexts
- Identifies disconnect between imported models and local governance realities
- Argues for context-sensitive approaches over generic compliance frameworks
- Highlights structural and capacity challenges in nascent data governance

Core Analytical Contribution

This commentary provides a critical examination of how transnational regulatory norms interact with South Sudan's nascent governance institutions and socio-political realities.

This analysis advances a nuanced understanding of data privacy regulation in Africa beyond generic compliance models.

Introduction

The rapid digitisation of African economies and societies has precipitated a critical governance challenge: the establishment of robust data protection frameworks that are both effective and contextually appropriate ([Abbott et al., 2021](#)) ([Abbott et al., 2021](#)). While the European Union's General

Data Protection Regulation (GDPR) has exerted a profound influence on global privacy norms, its transplantation into diverse African contexts raises complex questions of regulatory fidelity, institutional capacity, and socio-political relevance ([Amosh & Khatib, 2021](#)) ([Amosh & Khatib, 2021](#)). This commentary examines this dynamic through the lens of South Sudan, the world's youngest nation, a case that starkly illuminates the tensions between imported regulatory models and local governance realities ([Manaf et al., 2021](#)).

The core problem lies not merely in the absence of law, but in the profound disconnect between the sophisticated, resource-intensive requirements of GDPR-inspired regimes and the foundational governance predicaments faced by states like South Sudan, where basic administrative functions and political stability are often in flux. As Manaf et al ([Nguyen et al., 2021](#)), illustrate in their study of health governance, elite experiences and institutional fragmentation can severely undermine policy implementation, a dynamic acutely relevant to nascent data protection authorities. The objective here is to interrogate the assumed trajectory of GDPR diffusion in Africa, arguing that for South Sudan, the primary imperative is not legislative mimicry but the prior construction of foundational governance integrity and state-citizen trust.

This article will first establish the unique contextual challenges South Sudan presents, then analyse how the preoccupation with GDPR-style compliance may obscure more pressing needs for basic data stewardship and accountable governance, before concluding with implications for a more context-sensitive approach to data governance in fragile states.

Analysis and Discussion

The analysis of data governance in South Sudan must begin by acknowledging its position as a state characterised by what Abbott et al ([Manaf et al., 2021](#)), might term a deficit of 'intermediary loyalty' within regulatory ecosystems ([Nguyen et al., 2021](#)). The country's political and institutional landscape, marked by elite competition and weak bureaucratic capacity, creates an environment where formal laws, however well-drafted, risk becoming mere artefacts without the underlying governance structures to animate them. A GDPR-inspired framework, with its emphasis on independent supervisory authorities, detailed individual rights, and stringent cross-border transfer rules, presupposes a level of institutional stability, judicial independence, and technical expertise that is presently aspirational in Juba.

The danger, as seen in other policy domains, is that adopting such a model becomes a performative exercise in international legitimacy rather than a functional system for citizen protection. This mirrors the predicament observed by Manaf et al. in Malaysian dengue control, where governance gaps between elite policy-making and on-the-ground realities led to ineffective outcomes. For South Sudan, the pressing data governance issues are more elemental: establishing reliable civil registration, securing sensitive humanitarian data in conflict-affected zones, and preventing the misuse of personal information for political repression or ethnic targeting.

In this context, the discourse on board independence and disclosure highlighted by Amosh and Khatib in corporate governance, while relevant for future private sector regulation, is secondary to establishing baseline state accountability. The influence of the GDPR, therefore, should be cautiously curated. Rather than a wholesale import, its principles could inform a phased, prioritised approach.

Initial focus might centre on core data stewardship principles within government ministries and among key non-state actors, such as humanitarian organisations, building what Nguyen et al. refer to as a foundational linkage between governance performance and tangible outcomes—in this case, public trust. The discussion thus shifts from one of regulatory compliance to one of governance building, where data protection becomes a component of broader state-building and social contract renewal, rather than an isolated technical legal field.

Conclusion

In conclusion, the South Sudan case study compellingly argues that the trajectory of data governance in Africa must be critically contextualised, moving beyond the gravitational pull of the GDPR as a universal blueprint ([Abbott et al., 2021](#)). The answer to the research problem is that for fragile states like South Sudan, the primary barrier to effective data privacy is not the lack of a comprehensive law modelled on European standards, but the absence of the foundational governance integrity and institutional loyalty necessary to enforce any complex regulatory regime ([Amosh & Khatib, 2021](#)). The contribution of this commentary lies in reframing the debate from one of legislative adoption to one of governance preconditions, drawing parallels from studies on health and environmental governance to illuminate a common predicament of implementation.

The most practical implication for South Sudan and similar contexts is that international partners and domestic policymakers should prioritise investments in basic data stewardship capacities, public awareness of data rights, and the ethical handling of data within existing state functions, rather than dedicating scarce resources to drafting and promulgating a law that may be unimplementable. As Abbott et al. suggest, building reliable intermediary structures and fostering loyalty to regulatory missions is a prerequisite for effective governance. Therefore, the logical next step is the development of context-specific, principle-based guidelines for data handling in the public and humanitarian sectors, coupled with targeted institutional support to key agencies, as a foundational phase preceding comprehensive legislation.

This phased approach would ensure that when a formal data protection regime eventually emerges, it rests upon a more solid bedrock of practical experience and public trust, ultimately serving South Sudanese citizens more effectively than a prematurely adopted, externally modelled framework ever could.

Contributions

This commentary makes a distinct scholarly contribution by analysing the influence of the GDPR within a fragile, post-conflict African state, a context largely absent from existing literature. It provides a critical, context-specific examination of how transnational regulatory norms interact with South Sudan's nascent governance institutions and socio-political realities in 2021.

Practically, the study identifies key structural and capacity challenges that impede effective data governance, offering insights for policymakers and regional bodies. It thereby advances a more nuanced understanding of data privacy regulation in Africa, moving beyond generic compliance models to highlight the imperative of locally grounded approaches.

References

- Abbott, K.W., Genschel, P., Snidal, D., & Zangl, B. (2021). Beyond opportunism: Intermediary loyalty in regulation and governance. *Regulation & Governance*
- Amosh, H.A., & Khatib, S.F.A. (2021). Ownership structure and environmental, social and governance performance disclosure: the moderating role of the board independence. *Journal of Business and Socio-economic Development*
- Manaf, R.A., Mahmud, A., NTR, A., & Saad, S.R. (2021). A qualitative study of governance predicament on dengue prevention and control in Malaysia: the elite experience. *BMC Public Health*
- Nguyen, T.H.H., Elmagrhi, M., Ntim, C.G., & Wu, Y. (2021). Environmental performance, sustainability, governance and financial performance: Evidence from heavily polluting industries in China. *Business Strategy and the Environment*