



ISSN: 3108-9003 (Print)

Tanzania Privacy Profesionals Association Journal

Volume 1, Issue 1 | May 2026



DATA PROTECTION IN POLITICAL PROCESSES

• AI voter Profiling • Cybersecurity in Political
Campaigns • Privacy-Enhancing Technologies.

EDITORIAL TEAM

Dr. Elifuraha Laltaika

Editor-in Chief

*Senior Law Lecturer & Environmental and Social Standards (ESS) Expert,
Faculty of Law,
Tumaini University Makumira, Arusha, Tanzania*

Dr. Patricia Boshe

Technical Editor

*Head - Data and Cyber Law Breakthrough Attorneys
Head - Research and Publications, Africa Digital Rights Hub (ADRH)*

Professor Sizwe Snail ka Mtuze

Editor

Attorney of South African High Court. Nelson Mandela University, South Africa

Rachel Magege

Editor

Director, Tanzania Privacy Professionals Association

Josephina Nshunju

Editor

Data Protection Representative, Volvo Group

Ridwan Oloyede

Editor

Tech Hive Advisory, Nigeria

Quency Otieno

Editor

Managing Partner, Olotieno Advocates, Kenya

EDITORIAL NOTE

On behalf of the editorial board, I am delighted to present to our esteemed readership, this inaugural Issue of the Tanzania Privacy Professionals Association (TPPA) Journal. While pertinent matters pertaining to privacy and data protection have occupied center stage in Africa and globally during the last decade, the intricacies of many of its crucial aspects remain unknown to the general public. To fill this knowledge gap, the TPPA has unveiled and rolled out this interdisciplinary journal to provide space for scholars and practitioners to share key research findings. In this context, I am immensely thankful and wish to heartily congratulate all contributors in this Inaugural Issue for the highly enlightening articles. Each article in this issue is not only well thought-out and organized but addresses topical issues pertinent to the domain of data privacy in the region.

Main themes of this Inaugural Issue could not be timelier. As we continue to navigate challenges of data protection in the context of general elections in Africa, the contributions offer deep insights and rigorous analysis that brighten our understanding of the two phenomena. The first article by Nuru Keenja and Cosmas Masimo titled "Accountability in the Age of Digital Disinformation: Assessing Tanzania's Data Protection Obligations during Electoral Processes" addresses a critical need for Tanzania to more robustly implement its data protection obligations during elections, considering the negative effects of the pervasive digital disinformation.

Amiri Sharifu's article "Politicizations Risk in Cross-border Transfer of Personal Electoral Data in Tanzania" unpacks rarely acknowledged risks embedded in the Tanzania's regulatory framework related to cross-border transfer of personal data connected to general elections. A broader perspective of almost the same issue is covered in Tolulope Idowu's groundbreaking article entitled "Oversight and Enforcement Challenges of Data Protection Authorities in African Electoral Context."

Idowu's key findings align well with some of the findings embodied in Uyavhuya Matibe's article. Titled "A Comparative Analysis of Legal Frameworks for Electoral Data Protection and Political Privacy in Africa", Matibe's article highlights selected jurisdictions' strengths and drawbacks relating to data protection and political privacy. With Kenya as a case study, the last article by Timothy Samson Omondi Ayuo titled "Kenya's Data Protection Laws Empower Voters to Access Cross-Border Personal Electoral Data" interrogates the extent to which Kenya laws empower eligible members of the Kenyan Diaspora to exercise their constitutional right of electing leaders during the country's general elections.

As Editor-in-Chief, my goal remains to foster a space where legal scholars, lecturers, researchers, and students in Africa can participate in enlightening our esteemed readership with key aspects of privacy and data protection in the continent. Considering that reliability of scientific works largely hinges on the value-addition of the blind peer-review exercise, I am immensely thankful to our dedicated peer-reviewers whose critical but constructive feedback gave birth to the quality of scholarship this Inaugural Issue showcases.

I invite you to enjoy reading the articles and where appropriate, challenge the findings. This way you will contribute to the important conversation on privacy and data protection in Africa. Your feedback and future contribution are key to the rolling out of subsequent issues and will ensure continued improvement of this journal.

Dr. Elifuraha Laltaika
Editor-in-Chief

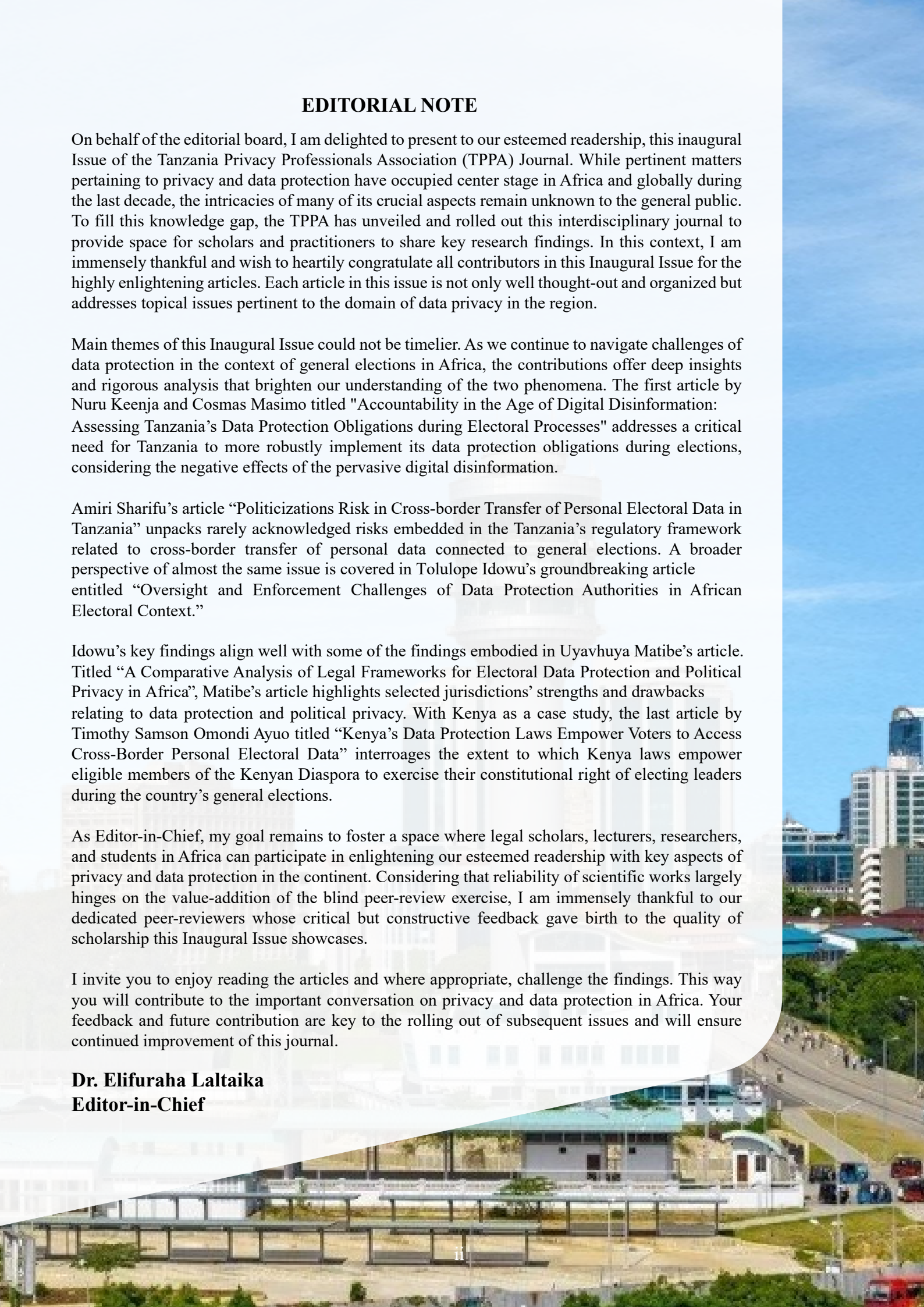


TABLE OF CONTENTS

Papers & Authors

Page

Comparative Analysis of Legal Frameworks for Electoral Data Protection and Political Privacy in Africa

Uyavhuya Matibe and Martha Elago Iyambo

1

Oversight and Enforcement Challenges of Data Protection Authorities in African Electoral Contexts

Tolulope Idowu

19

Accountability in the Age of Digital Disinformation: Assessing Tanzania's Data Protection Obligations during Electoral Processes

Nuru Keenja and Cosmas Babilas Masimo

35

Politicisation Risks in Cross-Border Transfers of Personal Electoral Data in Tanzania

Amiri Sharifu

57

Voters' Right to Access Cross-Border Personal Electoral Data in Kenya

Timothy Samson Ayuo

75

Comparative Analysis of Legal Frameworks for Electoral Data Protection and Political Privacy in Africa

Uyavhuya Matibe and Martha Elago Iyambo**

Abstract

This policy brief examines the adequacy of legal frameworks governing electoral data protection and political privacy in Africa amid the increasing digitisation of electoral processes. Through a comparative analysis of Kenya, Tanzania, Nigeria, South Africa and Ghana, the study evaluates how national data protection laws address the collection, processing and use of personal data in electoral contexts. The brief further considers continental and regional instruments, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and The Economic Community of West African States (ECOWAS). The analysis identifies significant regulatory gaps relating to political profiling, voter targeting, cybersecurity, enforcement capacity and election-specific data governance. It argues that while many African states have established comprehensive data protection regimes, these frameworks remain insufficient to address the unique risks posed by digital electoral technologies and data-driven political campaigning. The brief concludes by proposing targeted legal and policy reforms aimed at strengthening electoral integrity, protecting voter privacy and promoting harmonised data governance across the continent.

* Uyavhuya Matibe is the Head of Data Protection and Privacy at MK Legal Consultancy (Pty) Ltd. She holds an LLB and BA degree from Rhodes University and she is an Admitted Attorney and Notary Public. She currently leads her team's efforts in helping organisations navigate complex data protection regulations and privacy frameworks. She is passionate about translating legal compliance into practical, business-enabling strategies that promote trust, innovation, and sustainable growth. She can be contacted at via email at: uyavhuya@mklegal.co.za

* Martha Iyambo is a Research Consultant at MK Legal Consultancy (Pty) Ltd. She holds a BSc, BSc (Hons), and MSc from Rhodes University. As the lead researcher, her work focuses primarily on AI research and policy development within the African context. She has co-authored several papers examining the intersection of artificial intelligence, innovation, and digital governance in Africa. Martha's research examines how emerging technologies are reshaping legal frameworks, promoting responsible innovation and equitable IP systems across the continent. She serves as the implementing partner lead for the Africa Privacy Roundup Project, a Pan-African initiative dedicated to data protection, AI governance, and cybersecurity. Through this role, she advances Africa's voice in global digital policy and IP discourse; she is also a 2026 Techforward Policy Fellow. She can be contacted at via email at: martha@mklegal.co.za

Executive Summary

Over the recent years, electoral processes have succumbed to digital and technological transformation, due to the widespread use of digital data by government officials in public political campaigns. Across the African continent, governments, electoral management bodies, political parties and private actors collect and process vast amounts of sensitive personal data, including biometric information, voter registration data and behavioral profiles. This inevitable penetration of digital technology has forced society to adapt its very fabric to the methods associated with the digital revolution.¹

The rights to privacy and access to information are closely linked to democratic governance. Article 9 of the African Charter on Human and Peoples' Rights as well as political elections underpin an invaluable component of democracy.² In the electoral context, these rights enable citizens to make informed political decisions while ensuring that personal data is not unlawfully disclosed. These interests include electing political office holders; participating in decision-making processes on the implementation of laws and policies; and holding public officials accountable for their acts or omissions in the execution of their duties.³ Access to information fosters transparency and trust in electoral systems, which is essential to democratic legitimacy.

The right to access to information held by relevant electoral stakeholders may only be limited by narrowly defined exemptions, which must be provided by law and comply strictly with regional and international standards of good practice. Information may only be legitimately withheld if its release would result in the unreasonable disclosure of the personal information of a third party. This tension between transparency in electoral processes and the protection of voters' personal data highlights the need for specialised legal frameworks to govern electoral data processing.⁴

¹ Muswede T "Impact of Digital Media on Political Campaigns" (2022) *African Journal of Political Science* 10(1) 47.

² African Charter on Human and Peoples' Rights. (1981). *Adopted by the Organization of African Unity, Nairobi*. Retrieved from <https://au.int/en/treaties/african-charter-human-and-peoples-rights>.

³ African Commission on Human and Peoples' Rights. (2017). *Guidelines on Access to Information and Elections in Africa*, 3.

⁴ Centre for Human Rights, University of Pretoria. *Proactive disclosure of information and elections in South Africa* (2020). Retrieved from

While many African countries have adopted general data protection laws over the past decade, specific regulations addressing the nuances of electoral and political data remain limited and inconsistent. This fragmentation increases risks of voter manipulation, discriminatory profiling, breaches of privacy and challenges to democratic legitimacy.⁵

1. Background

Elections serve as the cornerstone of democratic governance. In recent years, electoral processes across Africa have undergone significant digitisation, from biometric voter registration and electronic voting systems to targeted social media campaigns powered by data analytics.⁶ Biometric technology (BT) refers to the type of technology designed to identify unique individual using fingerprints, speech, gait, odour and DNA, among others.⁷ This increased deployment of technological electoral processes across Africa have been used for the purpose of sustainable democracy. For example, Zambia has adopted electronic voting, while Kenya, Ghana, Gambia and Nigeria among others have adopted one or multiple forms of BT as a means to curtail challenges in their electoral systems.⁸

This digital shift has not only enhanced electoral efficiency and inclusivity but has also introduced new privacy challenges. Electoral bodies now maintain large databases containing personally identifiable information (PII) such as names, addresses, identification numbers, fingerprints and facial recognition data. Furthermore, political parties and commercial data analytics firms increasingly rely on behavioral data and profiling to micro-target voters.⁹

However, this increased reliance on data has led to serious privacy concerns. Cases of data breaches, unauthorised data sharing and manipulation of voter profiles for political gain

https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Proactive_Disclosure_of_Information_and_Elections_in_South_Africa.pdf

⁵ Afolabi O.S “Biometric Technologies, Electoral Fraud and the Management of Elections in Nigeria and Zimbabwe” (2020) *Strategic Review for Southern Africa* 42(2) 1.

⁶ Idowu H.A “Biometric Technologies and the Prospect of Sustainable Democracy in Africa” (2021). *Journal of Africa Elections* 20(1), 24.

⁷ PSP Wang *et al* “Biometric Technologies and Applications” in *Proceedings of the 25th IASTED, International Multi-Conference, Artificial Intelligence and Applications* (Austria, 2007) 226-232.

⁸ H.A Idowu *Ibid.*, 24.

⁹ Watson A *et al* “*Learning from What has Worked in Africa*” (2024) 4.

have emerged as risks.¹⁰ In some instances, the misuse of data has been alleged to have influenced election outcomes. For example, during the 2013 and 2017 General Elections in Kenya, there was evidence of ‘Political Micro-Targeting’. Politicians retained the services of data analytics from firms such as Cambridge Analytica, which made use of citizens’ personal data to tailor political advertisements to individual voters, thus raising concerns about its impact on democracy and privacy.¹¹ This case demonstrates how voter data analytics can operate within legal grey areas despite the presence of a national data protection regime. While such practices may increase campaign efficiency, they also raise serious concerns to electoral democracy.

Nigeria’s recent elections further demonstrate how digital misinformation can distort democratic processes. During the 2019 presidential election in Nigeria, President Muhammadu Buhari vehemently denied widespread rumors that he had died and been replaced by a clone. These false claims spread rapidly across Facebook and private WhatsApp groups, illustrating the power of digitally amplified disinformation.¹²

The 2023 Nigeria election cycle also saw an even greater surge in coordinated misinformation. Investigations by the BBC revealed that political actors paid social media influencers significant sums to disseminate false narratives about opponents. Disinformation also targeted the Presidential Election Tribunal, casting doubt on the legitimacy of the legal process.¹³ As a result, this rapid growth of digital platforms complicates regulatory oversight, especially when foreign technology companies process African electoral data without sufficient transparency or accountability.¹⁴

This regulatory gap is exacerbated by the growing role of multinational technology

¹⁰ Tombari R.T “Technology, Cyber Security and the 2023 Elections in Nigeria: Prospects, Challenges and Opportunities” (2023) *Journal of African Elections* vol 22 72.

¹¹ Mude H “Political Micro-Targeting in Kenya: An Analysis of the Legality of Data- Driven Campaign Strategies under the Data Protection Act” (2021) *Journal of Intellectual Property and Information Technology Law* 1(1) 9. Retrieved from <https://doi.org/10.52907/jipit.v1i1.61>

¹² BBC 2019, ‘Nigerian elections 2019: the spread of false information’, BBC News, 14 February. Available at: <https://www.bbc.com/news/world-africa-47226397>

¹³ Omilusi, M “Fake news, election-related disinformation laws, and citizens’ rights in African political ecology” (2025) *Journal of African Elections*, 24(1), 2. <https://doi.org/10.20940/jae/2025/v24i1a1>

¹⁴ *Ibid.*, 72.

companies, predominantly based in the Global North ¹⁵, which control much of the digital infrastructure in African electoral processes. These actors often exert significant influence over data flows and digital systems, enabling large-scale collection and processing of personal data with limited regulatory oversight.¹⁶ As a result, existing legal frameworks struggle to ensure transparency, accountability and effective enforcement in the use of electoral data.

These structural vulnerabilities are not merely theoretical but are reflected in practice, as illustrated by electoral processes in Kenya during the 2013 and 2017 elections. Instances of electoral data misuse during these periods exposed significant regulatory gaps, demonstrating that existing data protection were inadequate to address risks relating to data security and exclusion.¹⁷ While these dynamics are sometimes conceptualised in the literature as forms of digital colonialism, their practical implication is a weakening of data sovereignty and regulatory control within African jurisdictions.¹⁸ The increasing use of artificial intelligence and data-driven systems further compounds these challenges, particularly where such technologies are developed outside local contexts and operate without sufficient legal safeguards.

These developments reveal a structural regulatory gap within African electoral governance frameworks. While several African states have adopted general data protection legislation, few legal systems explicitly regulate the use of personal data for political campaigning, voter profiling or algorithmic targeting. This creates a regulatory asymmetry where political actors may exploit digital technologies faster than legislators can respond, thereby undermining electoral fairness and voter autonomy.¹⁹ The aforementioned examples illustrate how data-driven campaign strategies can operate in legal grey zones despite the existence of a comprehensive data protection regime.

¹⁵ Effoduh, J. O. Digital Colonialism and the Role of Local Intermediaries: Examining Big Tech's Impact on Data Sovereignty and Human Rights in Africa (2025) *Business and Human Rights Journal*, 10(2-3), 301–317. <https://doi.org/10.1017/bhj.2025.10021>

¹⁶ *Ibid.*, 312.

¹⁷ *Ibid.*, 310.

¹⁸ *Ibid.*, 313.

¹⁹ Maseko M.M “Effects of Digital Technologies on Africa’s Electoral Democracy” (2024) *Digital Policy Studies* (DPS) 3(1) 45.

2. Comparing Electoral Data Protection in Africa: Methodological Approach

This article adopts a comparative analysis methodology to examine existing legal frameworks governing electoral data protection in Africa and how electoral data protection is regulated across the selected African jurisdictions. It compares regional and national laws, highlighting key gaps and proposing actionable recommendations to harmonise data protections and strengthen enforcement.

The research focuses on five representative African jurisdictions, namely; Kenya, Tanzania, Nigeria, South Africa and Ghana. These countries are selected for their diverse legal traditions, levels of digital electoral integration and regional representation. The analysis focuses on key legislative instruments including Kenya's Data Protection Act 2019, Tanzania's Personal Data Protection Act 2022, Nigeria's Data Protection Act 2023, South Africa's Protection of Personal Information Act 2013 and Ghana's Data Protection Act 2012. These frameworks are examined against continental and regional instruments such as the African Union Convention on Cybersecurity and Personal Data Protection 2014 (Malabo Convention) and the African Union Data Policy Framework 2022 to assess regulatory convergence, enforcement capacity and gaps in election-specific data governance.

3. Continental Legal Frameworks

3.1. African Union Convention on Cyber Security and Personal Data Protection

The Malabo Convention, adopted in 2014 and entering into force in 2023, represents the most comprehensive continental legal instrument on data protection. It outlines fundamental principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation and the right to privacy.²⁰

The Malabo Convention obliges member states to establish independent data protection authorities (DPAs) and enact legislation aligned with these principles. However, adoption

²⁰Abdulrauf L. A et al "The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?" (2016) 1.

and ratification have been slow, and as of mid-2025, only 15 out of 55 countries have fully ratified and domesticated the Malabo Convention.²¹

Crucially, while the Malabo Convention sets out a broad data protection framework, it does not contain specific provisions addressing the complexities of electoral data. Unfortunately, the Malabo Convention, like many other African international instruments, does not contain an explanatory memorandum which may aid in the understanding of its provisions.²² For example, it lacks clear rules on political profiling, consent requirements tailored to electoral contexts, or restrictions on data use by political parties and campaign firms.²³

This omission is significant given the increasing digitisation of electoral processes across the Continent. Without explicit provisions addressing this, the Malabo Convention provides only a general privacy framework rather than a specialised governance regime for democratic processes. As a result, member states retain broad discretion in regulating electoral data, leading to fragmented legal protections and uneven safeguards for voters across the continent.

3.2. African Union Data Policy Framework, 2022

Published in 2022, The African Union Data Policy Framework provides a continental blueprint for harmonised data governance across AU Member States. It seeks to unlock the developmental and economic value of data while safeguarding fundamental rights, including privacy and data protection. The Framework promotes principles such as trust, accountability, transparency, cooperation and security. It also encourages Member States to align national laws and institutional mechanisms with continental standards to enable secure and interoperable data ecosystems.²⁴

²¹ *Evaluating Data Privacy Across Africa: Toward a Unified GDPR-Inspired Framework* (International Association of Privacy Professionals, 2021) <https://iapp.org/news/a/evaluating-data-privacy-across-africa-toward-a-unified-gdpr-inspired-framework> accessed 25 July 2025.

²² *Ibid.*, 20

²³ *Ibid.*, 20

²⁴ Department of infrastructure and Energy “The African Union Data Policy Framework” (2022), 3 Retrieved from www.au.int



For electoral data protection and political privacy, the Framework is particularly significant because it promotes ethical data governance, digital rights protection and cross-border regulatory co-operation.²⁵ However, implementation remains uneven. In their 2022 article, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), highlighted that several AU Member States continue to experience democratic deficits, including election-period internet shutdowns and the use of cybercrime or surveillance laws to suppress dissent and political opposition.²⁶ In such contexts, the progressive commitments contained in the Framework may face resistance at national level. This complex political economy presents a structural challenge to realising the Framework's ambitions, particularly where electoral data governance intersects with state control over digital spaces.²⁷

3.3. African Union Digital Transformation Strategy for Africa (2020–2030)

The African Union Digital Transformation Strategy for Africa 2020–2030 sets out a long-term vision for building an inclusive and secure digital economy across the Continent. It aims to establish a Digital Single Market, strengthen digital infrastructure and enhance innovation, digital skills and governance frameworks.²⁸

Crucially, the Strategy recognises data protection, cybersecurity and regulatory harmonisation as foundational to digital trust.²⁹ While the strategy does not make specific mention to electoral data and political privacy, it reinforces the need for secure digital public systems, accountable data processing and coordinated legal frameworks that will ultimately prevent the misuse of personal data in democratic processes. Therefore, national efforts by African States need to be harmonized with this strategy and the rise of digital electoral technology with broader national data protection legislations.

²⁵ CIPESA “Key Takeaways From the 2022 African Union Data Policy Framework” (2022) Retrieved from <https://cipesa.org/2022/11/key-takeaways-from-the-2022-african-union-data-policy-framework/>

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ MEL Framework for the Digital Transformation Strategy for Africa 2020- 2030 (2024) 6 Retrieved from https://www.mainlevel.de/uploads/files/EN_DTS-MEL-Framework-MASTER.pdf

²⁹ *Ibid.*, 11.

4. Regional Economic Communities

AMU: Data protection laws in North African Arab Maghreb Union (AMU) states are among the more developed on the Continent; countries such as Algeria, Morocco, Tunisia and Mauritania have comprehensive data protection legislation.³⁰ Many North African states such as Algeria are progressively digitising aspects of voter registration and electoral management. Algeria has not yet fully implemented electronic voting across all electoral stages and maintains a hybrid approach with traditional methods. Despite success, legal challenges include establishing comprehensive legislation that guarantees electoral secrecy, transparency and legal robustness for electronic voting.³¹ These advances have not been accompanied by a deeply integrated regional electoral model under the AMU.

EAC: The East African Community (EAC) comprises eight Partner States in East Africa, each of which conducts national elections under multi-party electoral systems managed by independent electoral commissions. Across the EAC region, governments have increasingly adopted digital technologies such as biometric voter registration, electronic databases and digital dissemination tools to improve voter registration integrity and speed of electoral administration.³²

At national level, EAC states vary in their data protection rules. Kenya, Rwanda, Tanzania and Uganda, have comprehensive Data Protection Acts while other countries like South Sudan are at various stages of implementation and enforcement. The EAC Legal Framework for Cyberlaws 2008 did however provide guidelines for member states to consolidate national laws on cybercrime and data protection but neglected to address important concepts like purpose limitation, data minimisation and accountability.³³

³⁰ Boshe P *et al.* “Data Protection Laws in Northern Africa: Regulatory Approaches, Key Principles, Selected Documents” (2022) 22 Retrieved from https://www.kas.de/documents/265308/22468903/230406_DataProtectionLawsNorthernAfrica_KAS_Web.pdf/

³¹ Nawel L *et al* “Eletronic Elections in Algeria: Between Reality and Expectations Comparative Study with the Omani Experience” (2025) *Russian Law Journal*, Volume 13(1) 16.

³² Omilusi M *et al* “Journal of African Elections” (2025) Vol 24:1 66. Retrieved from <https://www.eisa.org/storage/2025/08/2025-journal-of-african-elections-v24n1-eisa.pdf>

³³ Babalola O “Data Protection Legal Regime and Data Governance in Africa: An Overview” (2022) 4. Retrieved from <https://aercafrica.org/old-website/wp-content/uploads/2022/02/DG003.pdf>

Therefore, electoral data remains governed by disparate national and regional laws, creating uneven safeguards for voters' personal data and exposing electoral technology to differing levels of legal oversight and privacy risk.³⁴

ECCAS: Similarly, the Economic Community of Central African States (ECCAS) brings together eleven Central African countries with diverse political systems, including presidential and semi-presidential democracies. Historically, ECCASS has focused more on security and economic cooperation [i.e. Council for Peace and Security in Central Africa (COPAX)] due to the war in the Democratic Republic of Congo (DRC), where Angola and Rwanda fought on opposite sides. Ultimately leaving little to no room for harmonised regional data protection legislation.³⁵

The historical prioritisation of security and conflict management has also meant that digital governance and electoral data protection have remained largely underdeveloped at regional level. As a result, member states rely primarily on fragmented national frameworks that create uneven protections for voter data and limit the potential for coordinated regional standards on political data processing during elections.

ECOWAS: The Economic Community of West African States adopted the Supplementary Act on Personal Data Protection in 2010, and was the first subregional body to adopt a concrete framework on data protection law, which requires member states to protect personal data and establish supervisory authorities. Though binding, its implementation varies and it does not provide election-specific guidance. Furthermore, ECOWAS being a supplementary Act, may be legally binding in creating substantive rights in countries where treaties have direct effect and do not require local enactment.³⁶

SADC: The Southern African Development Community developed a Model Law on Data Protection in 2013 to harmonise privacy laws among member states. This Model Law is

³⁴ *Ibid.*, 6.

³⁵ African Union "Economic Community of Central African States (ECCAS)" Retrieved from <https://ceecac-eccas.org/>

³⁶ MEL Framework, *Ibid* 6.

voluntary and uptake is uneven. Like ECOWAS, it provides general principles but lacks specific rules for electoral data processing.³⁷

5. National Legal Frameworks: A Comparative Overview

Many African nations have made strides in adopting comprehensive data protection laws influenced by international standards such as the European Union’s General Data Protection Regulations (GDPR). However, the specificity and enforcement of these laws in electoral contexts vary considerably.

5.1. Kenya

Kenya’s Data Protection Act of 2019 is often cited as a regional benchmark. The Act establishes the Office of the Data Protection Commissioner and incorporates principles such as lawful processing, data minimisation, consent and data subject rights. It applies broadly to public and private entities, including electoral management bodies and political parties.³⁸ While Kenya’s Data Protection Act is progressive, it falls short in providing detailed guidance on core principles such as data anonymisation and pseudonymization.³⁹ These are key principles in the electoral process as they reinforce the right to privacy.

Despite its strengths, the Act does not explicitly regulate political micro-targeting or mandate transparency regarding the use of voter data in campaigns. The Independent Electoral and Boundaries Commission (IEBC) issues administrative guidelines on data security, but these lack statutory backing. Controversies over third-party data analytics companies’ involvement in political campaigns underscore enforcement challenges.⁴⁰ This illustrates a broader regulatory gap between the protection of personal data in general contexts and the specific risks posed by electoral data processing. It highlights the need for

³⁷Data Protection: Southern African Development Community (SADC) Model Law (2013) https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf accessed 23 July 2025.

³⁸ Shao D “Comparative Analysis of Data Protection Regulations in East African Countries” (2024) 4.

³⁹ Shao D “Comparative Analysis of Data Protection Regulations in East African Countries” (2024) 4.

⁴⁰ Office of the Data Protection Commissioner, Guidance Notes for Electoral Purposes (February 2024) <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Notes-for-Electoral-Purposes.pdf> accessed 24 July 2025.

clearer legal standards governing the use of electoral digital data and campaign analytics in Kenya's electoral framework.

5.2. Tanzania

Tanzania's Personal Data Protection Act, passed in 2022, introduced GDPR-style protections, including data subject rights, direct marketing restrictions and obligations for data controllers to register. The law establishes a Data Protection Commission.⁴¹ Just like its East African Counterpart, Kenya, Tanzania's Personal Data Protection Act also lacks specific details on the principle of anonymisation.

Despite some important recent legal reforms, Tanzania's electoral legal frameworks still fail to address technological processes such as biometric voter registration and the protection of personal data. In 2024–2025, the Parliament of Tanzania passed several significant statutes governing elections, namely; The Presidential, Parliamentary and Councillors' Elections Act (No. 1 of 2024)⁴², which consolidated the main procedures for presidential, parliamentary and local; The Independent National Electoral Commission Act (No. 2 of 2024)⁴³, which formally established and defined the mandate of the new electoral management body responsible for voter registration and election administration; and updated Election Expenses Act regulations (GN No. 421 of 2025)⁴⁴, which strengthen reporting and disclosure requirements for campaign financing.

While these are important developments in Tanzania's electoral law, none of them includes detailed provisions on digital governance, cybersecurity or data protection specifically in the context of election technologies. For example, the Independent National Electoral Commission Act does not make specific provisions on how the personally identifiable information (the names, number of the voter's card, disability if any, the sex of the voter and address)⁴⁵ on the Permanent National Voters' Register should be collected, stored,

⁴¹ Shao D "Comparative analysis of data Protection Regulations in East African Countries" (2024) 11.

⁴² Presidential, Parliamentary and Councillors' Elections Act (No. 1 of 2024).

⁴³ Independent National Electoral Commission Act (No. 2 of 2024).

⁴⁴ Election Expenses Act regulations (GN No. 421 of 2025).

⁴⁵ Section 12 (4) of the Presidential, Parliamentary and Councillors' Elections Act 1 of 2024

secured, audited or accessed and do not provide election-specific data protection oversight mechanisms for technologies used in voter registration and verification.

As a result, these electoral statutes define institutional roles and basic procedures but leave important gaps around emerging digital processes and digital accountability, meaning that electoral systems still operate without comprehensive statutory frameworks to govern data security, transparency or privacy of voters' personal information.

5.3. Nigeria

Nigeria's Data Protection Regulation (2019) and Data Protection Act (2023) create a comprehensive framework that recognises sensitive data types, including biometric and genetic data. The law requires explicit consent and empowers the Nigeria Data Protection Commission to enforce compliance, evidenced by sanctions against major tech companies such as Meta.⁴⁶

In Nigeria, parts of the election process have been digitised. The cybersecurity of Electoral Management Bodies (EMBs) and broader electoral processes still remain a key concern.⁴⁷ Nonetheless, Nigeria's laws do not contain specific provisions on electoral data or political micro-targeting. The Independent National Electoral Commission (INEC) has adopted technical guidelines for data security, but these are not legally binding. However, efforts have been made to facilitate networking and joint-learning opportunities to improve collaboration. For example, since 2013, Paradigm Initiative, a Nigeria-based digital rights and inclusion organisation focus on privacy, inclusion and access in the digital space has been hosting the Digital Rights and Inclusion Forum (DRIF).⁴⁸

5.4. South Africa

South Africa's Protection of Personal Information Act (POPIA), effective since 2020, imposes strong accountability requirements and grants significant enforcement powers to

⁴⁶ Watson A "Learning from What Has Worked in Africa" (2024) 27.

⁴⁷ Watson A "Learning from What Has Worked in Africa" (2024) 27.

⁴⁸ Watson A "Learning from What Has Worked in Africa" (2024) 27.

the Information Regulator. POPIA applies to political actors and has been invoked in cases concerning unsolicited political communications.

POPIA has largely kept up with the GDPR's lawful processing provisions, what it is lacking in, however, is the enforcement of cybersecurity laws and infrastructure, which are an important aspect in the election process. According to the Global Cybersecurity Index, only Mauritius, Kenya, Egypt and Rwanda demonstrate this high commitment.⁴⁹ This indicates that even with comprehensive data protection legislation, the broader cybersecurity ecosystem remains critical to safeguarding electoral processes and voter information for South Africa.

Furthermore, South Africa also faces challenges regulating cross-border social media campaigning and foreign data processors. The enforcement gap between local legislation and global digital platforms limits the effectiveness of protections during elections. While POPIA provides a strong legal foundation, its effectiveness in the electoral context ultimately depends on improved regulatory coordination, cybersecurity capacity and clearer accountability mechanisms for digital platforms involved in political campaigning.

5.5. Ghana

Ghana enacted its Data Protection Act in 2012, marking it one of the earlier data protection legislations in Africa. The Act established core data protection principles, outlines the rights of data subjects and created the Data Protection Commission (DPC) as the supervisory authority responsible for oversight and enforcement.⁵⁰ The legislation applies to both public and private bodies that process personal data and provides for registration of data controllers, security safeguards and sanctions for non-compliance.⁵¹

⁴⁹ *The Politics of AI and Data: Media and Elections in South Africa* (2021)

https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData8_ElecMedia_Elec.pdf accessed 25 July 2025.

⁵⁰ Bryant J "Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights" (2021) p. 391 Retrieved from https://law.stanford.edu/wp-content/uploads/2021/05/final_publish_this_-_bryant.pdf

⁵¹ Data Protection Act, 2012 (Act 843).

Despite this comprehensive framework, scholars note that enforcement capacity has been widely reported as constrained by limited institutional resources, funding challenges and low public awareness of data protection rights.⁵² The DPC has faced operational and compliance monitoring limitations, affecting the practical impact of the law more than a decade after its enactment. These implementation gaps raise concerns about the effective protection of sensitive categories of data, including electoral and voter information, particularly where cybersecurity safeguards and regulatory oversight require strengthening.⁵³ This lack of data protection enforcement prioritisation is ultimately linked to Ghana's lack of political will and institutional coordination.⁵⁴

6. Key Challenges and Gaps in Electoral Data Protection

6.1. Absence of Election-Specific Provisions

Most African data protection laws regulate personal data generally and fail to address the unique context of electoral data. There are few explicit rules governing political profiling, targeted advertising, or restrictions on the use of voter databases by private entities. For example, in 2019, “The South Africa information regulator, Advocate Pansy Tlakula, at the International Conference of Information Commissioners 2019 Conference, reiterated the need for developing a guideline in respect of access to information and the protection of personal data in the election process.”⁵⁵ This is largely due to the fact that electoral bodies must consider personal information of the voters and their constitutional right to privacy.

⁵² Bryant J “Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights” (2021) p. 394-395 Retrieved from https://law.stanford.edu/wp-content/uploads/2021/05/final_publish_this_-_bryant.pdf

⁵³ *Ibid.* 395.

⁵⁴ Dowuona S “Data Protection in Ghana: Legislation vs. Reality” (2022) Retrieved from <https://techfocus24.com/data-protection-in-ghana-legislation-vs-reality/>

⁵⁵ Burger-Smidt A ‘What Does the Protection of Personal Information Act, 2013 Mean for South African Elections?’ (Werksmans Attorneys, 2021) <https://www.werksmans.com/legal-updates-and-opinions/what-does-the-protection-of-personal-information-act-2013-mean-for-south-african-elections/> accessed 20 July 2025.

6.2. Weak Enforcement Capacity and Independence of Enforcement Authorities

Many national Data Protection Authorities lack adequate resources, technical skills and institutional independence. Enforcement during politically sensitive electoral periods is often limited or influenced by political considerations. In the 2016 International IDEA Policy Dialogue, Raheemat Momodu reiterated that it is important to recognise that electoral structures in Africa are often met with limited resources.⁵⁶

6.3. Low Public Awareness and Data Literacy

Voters frequently lack an understanding of their data rights, often due to limited access to information and consequently low levels of digital literacy regarding electoral processes. This reduces pressure on political actors to comply and hampers data protection enforcement.⁵⁷

6.4. Cybersecurity and Infrastructure Vulnerabilities

Biometric voter registration systems and electronic voting technologies are susceptible to cyberattacks and data breaches, potentially undermining voter privacy and election integrity. Furthermore, limited broadband network extensions remain a pressing issue in several African countries. While Rwanda and South Africa's broadband network coverage exceeds 98%, significant portions of citizens still remain unconnected to the internet, just highlighting this lack of adequate infrastructure.⁵⁸

7. Policy Recommendations

7.1. Develop and Enforce Election-Specific Data Protection Regulations

National governments and data protection authorities should adopt binding rules tailored to electoral contexts. These should regulate political profiling, require informed consent

⁵⁶ International IDEA, *Emerging Trends and Challenges of Electoral Democracy in Africa* (Policy Dialogue, 2016) 47 <https://www.idea.int/sites/default/files/publications/emerging-trends-and-challenges-of-electoral-democracy-in-africa.pdf> accessed 27 July 2025.

⁵⁷ *The Politics of AI and Data: Media and Elections in South Africa* (2021) https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData8_ElecMedia_Elec.pdf accessed 25 July 2025.

⁵⁸ *Ibid.*

for data processing, restrict unauthorised sharing of voter data and mandate transparency in campaign data practices. In South Africa, the Information Regulator has begun engagements with the Independent Electoral Commission (IEC) to consider how the balance of data privacy and data access may be implemented in practice.⁵⁹

7.2. Mandate Data Protection Impact Assessments (DPIAs) for Electoral Systems

Electoral commissions should conduct DPIAs for all biometric voter registration systems, electronic voting platforms and political campaign data analytics to identify and mitigate privacy risks. In ‘Technology and election conundrum: A case study of Nigeria’, Sociology and Anthropology, Olurode argued that ‘without doubt, the culture of digital democracy is spreading in Africa, and it is triggering profound changes in its democratisation processes.’⁶⁰ Therefore, it is vital that these data protection practices be integrated into the voting systems.

7.3. Strengthen Institutional Independence and Capacity of Data Protection Authorities (DPAs)

DPAs should have financial autonomy, technical expertise, legal powers to investigate, sanction and supervise electoral data processing entities effectively. The Policy Network states that DPAs can play in challenging this technological context, by offering flexibility and expertise and issuing regulations that are responsive to sectoral peculiarities.⁶¹

7.4. Enhance Regional and Continental Harmonisation

The AU should consider adopting supplementary protocols to the Malabo Convention focused on electoral data protection. Regional economic communities like ECOWAS and SADC should harmonise rules and create cross-border enforcement mechanisms.

⁵⁹ *The Politics of AI and Data: Media and Elections in South Africa* (2021) https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData8_ElecMedia_Elec.pdf accessed 25 July 2025.

⁶⁰ Olurode L ‘Technology and Election Conundrum: A Case Study of Nigeria’ (2017) 5 *Sociology and Anthropology* 799.

⁶¹ *The Politics of AI and Data: Media and Elections in South Africa* (2021) https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData8_ElecMedia_Elec.pdf accessed 25 July 2025.

7.5. Increase Public Awareness and Civic Education

Governments and civil society should promote data literacy campaigns, informing voters about their privacy rights and how electoral data is used. Transparency requirements for political parties' data practices can foster accountability.⁶²

7.6. Regulate Digital Platforms and Political Advertising

Social media companies and data brokers operating in Africa should be required to maintain local compliance offices, disclose political advertising content and targeting criteria and adhere to data protection laws.

8. Conclusion

While significant progress in the data protection environment in Africa has been made, electoral data remains an under-regulated and high-risk area. This policy brief contributes to emerging scholarship on electoral data governance in Africa by demonstrating that existing data protection frameworks remain insufficient for regulating digital electoral practices. The increasing digitisation of elections demands stronger, harmonised legal frameworks that explicitly address the unique challenges of political data privacy. Without clear rules and enforcement, risks of voter manipulation, breaches of privacy and threats to democratic legitimacy will persist.

National laws like Kenya's Data Protection Act, South Africa's POPIA and Nigeria's Data Protection Act provide strong foundations. However, their application to electoral contexts is often limited or inconsistent. Continental and regional harmonisation, combined with targeted national reforms and capacity building, is crucial to safeguarding electoral integrity and protecting citizens' fundamental rights in Africa's evolving digital democracy. The analysis highlights the need for specialised electoral data governance mechanisms at both national and continental levels.

⁶² *The Politics of AI and Data: Media and Elections in South Africa* (2021)

https://policyaction.org.za/sites/default/files/PAN_TopicalGuide_AIData8_ElecMedia_Elec.pdf accessed 25 July 2025.

Oversight and Enforcement Challenges Facing Data Protection Authorities in African Electoral Contexts

Tolulope Idowu*

Abstract

This article examines the oversight and enforcement challenges faced by Data Protection Authorities (DPAs) in African electoral contexts amid the increasing digitisation of electoral processes. It argues that while many African states have established data protection frameworks and supervisory institutions, significant gaps remain in enforcement, institutional independence, technical capacity, and inter-agency coordination, particularly between DPAs and Electoral Management Bodies. The study highlights how the growing reliance on digital tools, including biometric systems and foreign election-technology vendors, has intensified data protection risks while exposing regulatory weaknesses such as jurisdictional limitations, legal lacunae, and inadequate oversight mechanisms. Drawing on regional frameworks such as the Malabo Convention, ECOWAS Supplementary Act, and SADC Model Law, the article situates these challenges within broader continental governance efforts. It concludes by proposing targeted reforms, including strengthening DPA independence, enhancing technical expertise, formalising collaboration with electoral bodies, increased civic engagement and public awareness, and regulating cross-border data processing, to ensure effective protection of personal data and the integrity of democratic processes in Africa's evolving digital landscape.

* Tolulope Idowu is a Legal Practitioner from Nigeria and Lead Associate at A.A. Ademidun Solicitors. He holds a Bachelor of Laws (LL.B.) from Obafemi Awolowo University and has over 10 years of experience as a legal practitioner. He is actively engaged in digital governance, data protection and policies. He can be reached via email at itolulopeidowu@gmail.com

1. Introduction: Data Processing in Electoral Processes

The conduct of elections often relies heavily on the processing of personal and sensitive data such as names, Voter Identification Numbers, social media handles, demography, political views/alignment, biometric data etc. relating to data subjects during electoral processes.

In line with the Data protection laws of various African countries, the supervision of lawful processing of personal data is a core duty of Data Protections Authorities (DPAs) who are saddled with the responsibility of enforcement and coordination of processing activities within their jurisdiction, more particularly in electoral processes. These institutions however often lack the requisite resources, independence, legal and technical tools to effectively execute this duty.

This brief explores how DPAs across African countries can function more effectively in the performance of their duties to enhance electoral integrity in their jurisdictions and concludes with actionable policy recommendations for strengthening institutional frameworks, clarifying mandates, and promoting a culture of data rights protection during elections.

2. Identifying the Gaps

As in world over, actors in African elections are increasingly relying on digital tools to manage electoral processes including voter registration, political messaging, biometric technologies, and election tech infrastructure.⁶³ This has in no doubt exponentially increased the scale and sensitivity of processing activities during elections, leaving data subjects to increased privacy risk and harm.

While significant number of African countries have established Data Protection laws and DPAs,⁶⁴ there remains the problem of weak enforcement and oversight functions by the

⁶³ Abdul Azeez Yusuf, 'Legal Perspectives on the Use of Emerging Technologies in Elections in Africa' (2024) 4(2) Journal of Law and Emerging Technologies 11 <https://jolets.org/ojs/index.php/jolets/article/view/187> accessed 26 March 2026.

⁶⁴ Mubarak Raji and others, 'An Assessment of the Enforcement Mechanisms in African Data Protection Laws' (2025) 2(1) *African Journal on Privacy & Data Protection*.

various supervisory authorities. Challenges such as a lack of independence from executive control, budget constraints, inadequate collaboration between DPAs and Electoral Bodies (EBs), a weak oversight machinery, inadequate skills and technical expertise, limited oversight of foreign election vendors etc., have significantly contributed to this problem.⁶⁵

This gap undermines voter trust, exposes electoral stakeholders to data misuse, and threatens the integrity of democratic processes across the continent. Without strengthening supervisory oversight and enforcement mechanisms, electoral data privacy vulnerabilities will persist, limiting the effectiveness of data protection frameworks in safeguarding citizens' fundamental rights during African electoral processes.

3. Policy Context

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) sets a normative framework for harmonizing standards across the African continent. With about 43⁶⁶ out of 55 countries having enacted data protection laws and 35 of them operationalizing DPAs to oversee compliance⁶⁷, it is arguably true that the establishment of data protection frameworks in African context is on a forward move.

These data protection laws typically include provisions regulating the lawful basis for processing, data minimization, purpose limitation, technical and organizational safeguards for protecting personal data, and the rights of data subjects, as well as defining the supervisory roles of DPAs. However, these frameworks are often not fully aligned with

⁶⁵ Winifrida M Ernest, 'Personal Data Protection in Tanzania: Legal Challenges and Enforcement Prospects in the Digital Era' (2025) 8(2) East African Journal of Law and Ethics 174

<https://journals.eanso.org/index.php/eajle/article/view/4032>; Isaac Juma and Bukola Faturoti, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) International Review of Law, Computers & Technology <https://doi.org/10.1080/13600869.2025.2506918>; D Eke and others, Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs (Centre for the Study of the Economies of Africa 2022) <https://cseaafrica.org/images/posts/8194277452151253.pdf>

⁶⁶ Tech Hive Advisory Africa, 'Bimonthly Update on Privacy in Africa (May–June 2025)' (LinkedIn, 2025) <https://www.linkedin.com/pulse/bimonthly-update-privacy-in-africa-may-june-2025-kuicf/> accessed 23 July 2025; Central African Republic, Loi n° 24.001 portant protection des données à caractère personnel (2024) <https://www.techhiveadvisory.africa/insights/review-of-the-central-african-republic-data-protection-law> accessed 23 July 2025.

⁶⁷ Thelma Okorie, '2025 Report on Data Protection in Africa' (Aptan Tech, March 2025) https://aptantech.com/wp-content/uploads/2025/03/Final-Data-Protection-Reports_March-2025.pdf accessed 22 July 2025; DataUlinzi, 'Regulatory Milestone in Madagascar' (LinkedIn, August 2025) https://www.linkedin.com/posts/dataulinzi_regulatory-milestone-in-madagascar-on-august-activity-7358882781738741761-JQyT/ accessed 23 July 2025.

electoral laws. It is suggested that greater emphasis should be placed on harmonization and coordination between the two regimes. This can be achieved through regulatory instruments such as DPA-issued guidelines specific to electoral processes, as seen in countries like Kenya⁶⁸ and Senegal⁶⁹, or through formal cooperation mechanisms that ensure electoral bodies operate in full compliance with established data protection principles. Coordination efforts such as the Network of African Data Protection Authorities (NADPA) conference, hosted in Abuja in May 2025, showcase collaborative efforts amidst African DPAs to further strengthen governance, enforcement and oversight capabilities across the continent.⁷⁰

Beyond the continental Malabo Convention, sub-regional frameworks play an increasingly practical role in shaping data protection standards. The ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010) is the continent's only binding sub-regional data protection instrument and directly obliges its fifteen Member States to enact data protection laws and establish DPAs.⁷¹ Its ongoing revision, further signals the relevance of sub-regional norm-setting to data governance in West Africa. In Southern Africa, the SADC Model Law on Data Protection provides a persuasive template for harmonising standards among Member States, even if it lacks binding force.⁷² These sub-regional frameworks are often more practically applied than the Malabo Convention, given that the latter has attracted limited ratifications, and their alignment with electoral data governance deserves greater attention in national legislative reform efforts.

⁶⁸ Office of the Data Protection Commissioner (ODPC), 'Guidance Note on the Processing of Personal Data for Electoral Purposes' (ODPC, March 2022) <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Notes-for-Electoral-Purposes.pdf> accessed 23 July 2025.

⁶⁹ Commission de Protection des Données Personnelles (Senegal), 'Mini-guide pour le respect des données à caractère personnel dans le cadre du parrainage électoral' (2018), reported in CIO Mag <https://cio-mag.com/presidentielles-au-senegal-la-cdp-publie-son-mini-guide-pour-le-respect-des-donnees-a-caractere-personnel/>.

⁷⁰ Nigeria Data Protection Commission (NDPC), 'NADPA–RAPDP Conference 2025: Nigeria Hosts African Data Protection Authorities' (NDPC, 29 April 2025) <https://ndpc.gov.ng/2025/04/29/nadpa-rapdp-conference-2025-nigeria-hosts-african-data-protection-authorities/> accessed 23 July 2025.

⁷¹ UNCTAD, *eTrade Readiness Assessment of ECOWAS Member States* (2022) 35; ESTDEV, *Inception Study on Data Governance in Africa* (2024).

⁷² Southern African Development Community, *SADC Model Law on Data Protection* (2013); UNCTAD, *Data Protection Regulations and International Data Flows: Implications for Trade and Development* (2016) 45.

Although there have been commendable efforts to promote collaboration between DPAs and EBs across Africa, such as Memoranda of Understanding (MoUs) and joint capacity-building initiatives⁷³, these efforts remain fragmented and limited in impact. In many jurisdictions, cooperation is still largely ad hoc, reactive, and insufficiently formalized. This gap persists despite the fact that electoral bodies routinely collect, store, and process vast volumes of personal and sensitive data.⁷⁴

These gaps undermine coherent data governance to ensure the integrity of the democratic process and accountability during elections and limit the potential for coordinated oversight that could strengthen electoral integrity. African DPAs must skilfully navigate this landmine by strengthening their autonomy, technical expertise, collaborative enforcement strategies, advocacy and enlightenment exercise to engage the populace in order to address the risks of data misuse, abuse and violations during electoral processes. This policy context underscores the urgent need for targeted reforms and regional cooperation to enhance DPAs' role in electoral data governance as Africa's digital democracy deepens.

4. Key Findings/Analysis

4.1. Weak Collaboration Between DPAs and Electoral Bodies (EBs)

In many countries across the African continent, collaboration between DPAs and EBs remains weak, with no reported existence in certain cases. Countries such as Nigeria have made efforts in establishing collaborative effort between the DPA, Nigeria Data Protection Commission, and the EB, Independent National Electoral Commission,⁷⁵ Kenya's Office of the Data Protection Commissioner had also published Guidance Note for Electoral

⁷³ 'INEC, NDPC Meet Over Data Protection Measures in Election Process' (Daily Post NG, 23 July 2024) <https://dailypost.ng/2024/07/23/inec-ndpc-meet-over-data-protection-measures-in-election-process/> accessed 23 July 2025.

⁷⁴ Guy Berger and Liz Orembo, 'Data Deficits and Democratic Processes: The Under-Explored Role of Data in African Elections' (Data for Development/Research ICT Africa, April 2025). https://dataalliance.africa/wp-content/uploads/Data-Deficits-and-Democratic-processes_-The-Under-Explored-Role-of-Data-in-African-Elections_D4D_RIA_2025_2304-1.pdf accessed 23 July 2025.

⁷⁵ Oladapo Riliwan, 'Data Protection: INEC, NDPC to Secure Nigeria's 93M Voters Records' (Technology Times, 2024) <https://technologytimes.ng/data-protection-inec-ndpc-secure-93m-voters-data/> accessed 23 July 2025.

Purposes,⁷⁶ enforcing subject rights and audit obligations across electoral stakeholders. This however is not the case in many African countries where there are no formal agreements or institutional mechanisms linking data protection authorities with electoral commissions. This lack of structured collaboration hinders joint risk assessments, policy development, response and enforcement strategies.

4.2. Enforcement Challenges and Capacity Gaps

Limitations such as inadequate funding, insufficient staffing, limited skills and technical expertise⁷⁷ have inhibited DPAs' capacity to effectively oversee electoral processes. While there have been recent reports of high profile enforcement cases such as Kenya's intervention against WorldCoin⁷⁸ for unauthorized biometric data collection and Nigeria's recent fine on MultiChoice⁷⁹ and record \$220 Million fine on Meta⁸⁰ which illustrate African DPAs' growing enforcement potential, there however remain persistent barriers including limited technical capacity, political interference, and resource constraints.⁸¹ According to Privacy International, the growing reliance on personal data throughout the election cycle introduces novel risks that DPAs are often ill-equipped to address.⁸²

⁷⁶Privacy International, 'Our Final Report on Kenya's 2022 Election: A Collaboration with The Carter Center' (Privacy International, 2023) <https://privacyinternational.org/long-read/5053/our-final-report-kenyas-2022-election-collaboration-carter-center-election-expert> accessed 22 July 2025.

⁷⁷Tech Hive Advisory Africa, 'Roundup on Data Protection in Africa – 2023' (Tech Hive Advisory Africa, 2023) https://cdn.prod.website-files.com/641a2c1dcea0041f8d407596/660c183b35ce75f5eb7b5654_Roundup%20on%20Data%20Protection%20in%20Africa%20-%202023.pdf accessed 23 July 2025.

⁷⁸ Irene Makau, 'Kenya High Court's Worldcoin Determination: Upholding Consent, Accountability and Data Sovereignty in Biometric Data Processing' (CIPIT, Strathmore University Blog, 11 September 2025) <https://cipit.strathmore.edu/kenya-high-courts-worldcoin-determination-upholding-consent-accountability-and-data-sovereignty-in-biometric-data-processing/> accessed 23 July 2025.

⁷⁹ 'NDPC Fines MultiChoice ₦766m for Data Privacy Violations' (Punch Newspapers, 6 July 2025) <https://punchng.com/ndpc-fines-multichoice-%E2%82%A6766m-for-data-privacy-violations/> accessed 23 July 2025.

⁸⁰ Associated Press, 'Nigeria Fines Meta \$220M for Facebook, WhatsApp Data Privacy Violations' (AP News, 2024) <https://apnews.com/article/nigeria-meta-fine-facebook-whatsapp-9c79447e348dcaaa1b8c59898e60c7fa> accessed 23 July 2025.

⁸¹ Tech Hive Advisory Africa, 'Roundup on Data Protection in Africa 2024: Projections for 2025' (Tech Hive Advisory Africa, 11 February 2025) <https://www.techhiveadvisory.africa/insights/roundup-on-data-protection-in-africa-2024-projections-for-2025> accessed 23 July 2025.

⁸²Privacy International, 'Data and Elections' (Privacy International, May 2025) <https://privacyinternational.org/learn/data-and-elections> accessed 23 July 2025.

4.3. Independence of DPAs and Political Influence

DPAs' institutional independence varies widely across the continent, affecting their ability to impartially oversee data practices during elections. In some countries, political control or influence over DPAs hinders proper enforcement against ruling parties or influential actors. This undermines voter trust and the legitimacy of electoral processes. Countries like Morocco, Tunisia, and South Africa have DPAs established by clear legislative mandate, with varying levels of operational and financial independence. South Africa's Information Regulator, for instance, enjoys comparatively stronger protections on appointment, tenure, and budget, but these are not uniform in the wider Southern African region. In contrast, Zimbabwe's 2021 Act fails to specify meaningful independence provisions, while Mauritius' DPA depends on government-determined funding.⁸³ According to reports from ALT Advisory, only 11 DPAs in Africa have protection from arbitrary removal from office⁸⁴.

This systemic challenge points to a structural weakness in Africa's data governance architecture. Without robust, legally enshrined independence, DPAs remain susceptible to political influence, particularly during sensitive electoral cycles.

4.4. Data Access, Transparency, and Electoral Integrity

Increased reliance on technology in electoral processes such as adoption of biometric voter registration systems, electronic transmission of results, digital campaign activities have significantly increased the challenges related to data access, transparency and effective use of these technological systems.⁸⁵ Zimbabwe's 2023 election is marred with reports of the Ruling parties' unauthorised use of voters' data likely sourced from voter's roll for its

⁸³ LA Abdulrauf, 'Independence of Data Protection Authorities in Africa: Trends and Challenges' in Luca Belli and Primavera De Filippi (eds), 'Data Privacy Law in Africa: Emerging Perspectives' (University of Pretoria Law Press 2024) 356 https://www.pulp.up.ac.za/images/edocman/edited-collections/data_privacy/Chapter%2012.pdf accessed 23 July 2025.

⁸⁴ Data Africa, 'Standing Alone: The Independence of African Data Protection Authorities' (Data Africa, 28 June 2023) <https://dataprotection.africa/standing-alone-the-independence-of-african-data-protection-authorities/> accessed 23 July 2025.

⁸⁵ Nic Cheeseman, Gabrielle Lynch and Justin Willis, 'Digital Dilemmas: The Unintended Consequences of Election Technology' (2018) 25(8) *Democratization* 1397 <https://doi.org/10.1080/13510347.2018.1470165>



campaign activities⁸⁶, a pattern that warrants closer examination of the legal mechanisms that enabled it. Zimbabwe's Data Protection Act (Chapter 11:12) of 2021 vests data protection functions in the Postal and Telecommunications Regulatory Authority (POTRAZ)⁸⁷, an existing telecoms regulator that was not purpose-built for data protection enforcement. POTRAZ lacks full independence from the executive; its board is appointed by the President after ministerial consultation. The Act also establishes the Cybersecurity and Monitoring of Interceptions of Communications Centre as a unit within the Office of the President, centralizing surveillance and creating structural conflicts that undermine impartial data oversight, especially for ruling-party activities. Critically, the Act contains no explicit provision prohibiting the secondary use of voter roll data for political campaigning, and the absence of a designated DPA with electoral oversight competence meant that no formal enforcement action was taken in relation to the 2023 incidents. This structural vacuum, combining a non-independent DPA, the absence of electoral data-specific regulations, and weak enforcement capacity, illustrates how legal inadequacies, not merely bad actors, enable electoral data misuse. Nigeria's electoral processes have also faced technological and cybersecurity challenges, such as the hacking of the Independent National Electoral Commission's (INEC) website during the 2015 elections, reported glitches in the deployment of biometric voter accreditation machines by Independent National Electoral Commission (INEC) ahead of Nigeria's 2023 election etc. Increasing usage and engagement of generative AIs, have spurred concerns about how platform (social media) algorithms may amplify content that can potentially harm electoral processes with misinformation and manipulation.⁸⁸

A culture of official secrecy, inconsistent data standards, fragmented data systems, and limited collaboration inhibit the sharing of electoral data necessary for transparency and

⁸⁶ Richard Kawazi, 'Unsolicited Political Messaging Violating Rights to Digital Privacy in Zimbabwe' (ZNCJ Digital Rights, 21 June 2023) <https://zncj.org/unsolicited-political-messaging-violating-rights-to-digital-privacy-in-zimbabwe/> accessed 23 July 2025.

⁸⁷ Section 5 of Zimbabwe's Data Protection Act [Chapter 11:12] (No. 05/2021).

⁸⁸ Chinasa T Okolo, 'African Democracy in the Era of Generative Disinformation: Challenges and Countermeasures against AI-Generated Propaganda' (2024) SSRN Working Paper <https://ssrn.com/abstract=4885958> accessed 23 July 2025; Abdul Azeez Yusuf, 'Legal Perspectives on the Use of Emerging Technologies in Elections in Africa' (2024) 4(2) Journal of Law and Emerging Technologies 11 <https://jolets.org/ojs/index.php/jolets/article/view/187> accessed 26 March 2026.

accountability which in turn negatively impacts and obstructs fact checking, audit accuracy and informed voter participation.

Without systemic reforms to promote open data practices and institutional cooperation, these barriers will continue to erode public trust in electoral outcomes and weaken democratic participation.

4.5. Legal and Regulatory Lacuna

Whilst admittedly many African countries have established legal frameworks for data protection, the discomfiting trend is that many of these legal and regulatory frameworks contain extensive exemptions on national security, or even in certain instances allow for loophole that may be engaged by private sector actors to bypass data protection during electoral processes. Nigeria's NDPA 2023 for instance includes extensive exemptions, allowing data processing without full compliance during national security operations, crime investigation or prosecution, public interest journalism or publication, legal proceedings, and personal or household purposes. Similarly, Ghana's Data Protection Act, 2012 (Act 843) has robust data protection principles, but national security laws and executive powers can override them e.g. Emergency Communications System Instrument, 2020 (Executive Instrument 63), which was later ruled against by the Courts for infringing citizen's privacy, compelled telecom providers to surrender subscriber data for contact tracing⁸⁹. Electoral actors can potentially rely on these exemptions to access and use voter data without adhering to key data protection principles. In practice, these exemptions have been weaponised by political actors with particular effectiveness during election cycles. The invocation of "national security" or "public interest" grounds by incumbents provides a legally defensible basis for accessing voter databases, intercepting digital communications, and directing state agencies to process citizens' data in ways that would otherwise require DPA authorisation. Because the exemptions are broadly worded and subject to executive determination rather than independent judicial oversight, DPAs in jurisdictions such as Nigeria and Ghana are effectively pre-empted from investigating data

⁸⁹ 'Court Orders NCA to Stop Collecting Personal Details of Mobile Phone Subscribers' (Modern Ghana, 22 July 2021) <https://www.modernghana.com/news/1094624/court-orders-nca-to-stop-collecting-personal-detail.html> accessed 23 July 2025.

processing activities that government actors choose to characterise as security-related. The consequence is that the most politically sensitive data processing during elections, precisely the activity that warrants the most rigorous DPA scrutiny, is the activity most easily shielded from it. Addressing this gap requires either the legislative narrowing of these exemptions by introducing necessity and proportionality tests reviewable by an independent body, or the conferment on DPAs of an explicit power to audit national security-related data processing in electoral contexts, subject to appropriate confidentiality safeguards.

4.6. Regulating Foreign Election-Technology Vendors

A structurally under-examined challenge for African data protection authorities in electoral contexts lies in the growing reliance on foreign election-technology vendors, which function as data processors within domestic electoral infrastructures,⁹⁰ thereby raising complex issues of jurisdiction, accountability, and regulatory oversight. Electoral Management Bodies (EMB) frequently engage foreign vendors to supply biometric voter registration kits, results transmission systems, and electronic voting machines. In such arrangements, the EMB is typically designated the data controller under national law, while the foreign vendor operates as the data processor with *de facto* technical custody of the most sensitive electoral data. This controller/processor split creates acute jurisdictional difficulties. African DPAs nominally retain authority over the data controller (the EMB), but their powers to practically compel disclosure, conduct audits, or impose sanctions on a foreign processor domiciled outside their jurisdiction are often absent from national data protection statutes or practically unenforceable without mutual legal assistance treaties or bilateral data protection agreements with the counterpart countries hosting the vendors.

The resource asymmetry is stark: a foreign vendor deploying technology across multiple African elections simultaneously commands legal teams, proprietary data architectures, and cross-border operational capacity that vastly exceeds the investigative and enforcement resources of most African DPAs. The result is that the technical layer of the election, often

⁹⁰ Okechukwu Obinna Ibeanu, 'Digital Technologies and Election Management in Africa's Democratisation Process: More Technocratic than Democratic?' (2022) 47(2) *Africa Development / Afrique et Développement* 15 <https://doi.org/10.57054/ad.v47i2.2197>

the layer most vulnerable to data breach, unlawful secondary use, and manipulation effectively escapes meaningful DPA oversight.

Addressing this gap requires targeted regulatory interventions: national data protection laws should be revised to impose data processor obligations directly enforceable against foreign entities where they process data of citizens within the jurisdiction, mirroring the extra-territorial reach of the European Union General Data Protection Regulation (GDPR). EMBs should additionally be required by statute or electoral regulations to include DPA audit access rights as a mandatory clause in contracts with foreign technology vendors, alongside data localisation obligations, prescribed deletion timelines, and incident notification duties. These measures would transform the vendor contract from a governance gap into an enforcement tool, allowing the DPA to exercise oversight over the processor indirectly through the contractually obligated data controller.

5. Policy Recommendations

The following recommendations are suggested to strengthen activities of African DPAs, bridge institutional gaps and reduce enforcement limitations:

5.1. Enhanced Institutional Independence of DPAs

Policy stakeholders and lawmakers across the continent should make revised legislative frameworks that enhances stronger institutional independence for DPAs by ensuring that DPA heads and members are appointed with less political *cum* executive interference. Appointment should be merit based, through legislative/administrative procedures, without executive interference, with clearly defined non-arbitrary grounds for the constitution and removal of DPA leadership and ensured tenure security to reduce the risk of political bias and fear of reprisal removal.

DPA budgets should be allocated through protected statutory frameworks or autonomous financing mechanisms that include legal safeguards against executive interference. Stable, independent funding is essential to preserve institutional autonomy, support effective enforcement, and insulate regulatory/supervisory decisions from political pressure, especially during election cycles.

5.2. Harmonised Collaboration Between DPAs and EBs

Existing legislative and regulatory frameworks should be revised to institutionalize collaboration between EBs and DPAs. Electoral Bodies should be legally required to consult DPAs during the design and implementation of data systems, particularly those used for voter registration, result transmission, and digital campaign management. There should also be clear and enforceable protocols for secure data sharing and transparency among DPAs, EBs, political parties, and civil society organizations. These measures will help safeguard personal data while enhancing credible electoral oversight.

In addition, EBs must be required to comply with core data governance principles, including privacy by design and by default. This involves limiting data collection to what is strictly necessary, ensuring that privacy settings are enabled by default, embedding safeguards throughout the data lifecycle, and conducting Data Protection Impact Assessments (DPIAs) before deploying technologies that process personal data. EBs should also implement appropriate technical and organizational measures to reduce data-related risks.

To support consistent collaboration, Memoranda of Understanding (MoUs) should be established between DPAs and EBs. These agreements should outline practical cooperation mechanisms that apply before, during, and after elections. To move beyond aspirational language, a model MoU between a DPA and an Electoral Commission should contain the following concrete elements at a minimum: (i) a requirement that the EB designate a Data Protection Officer (DPO) or a senior officer with equivalent data governance responsibility for the duration of each electoral cycle; (ii) a joint DPIA process to be completed before the deployment of any new or materially changed electoral technology, with the DPA having sign-off authority; (iii) shared and mutually accessible audit logs of all processing activities carried out by the EB and its contracted vendors, maintained in a format specified by the DPA; (iv) a defined incident response protocol, specifying notification timelines (for example, within 72 hours of detection) and the investigative roles of each institution in the event of a data breach; (v) pre-election data mapping and inventory obligations requiring the EB to disclose to the DPA all categories of personal data processed, all processors engaged, and all international data transfers; and (vi) post-election data

retention and deletion schedules, with certification of destruction provided to the DPA. The Nigeria DPA–INEC engagement of 2024 and Kenya’s Office of the Data Protection Commissioner (ODPC) electoral guidance demonstrate that the institutional will for such cooperation exists; what is now needed is its formalisation into binding, justiciable instruments.

5.3. Stricter Oversight of Electoral Processes and Strengthened Enforcement

DPAs should be empowered with a clear and enforceable mandate to oversee data practices within electoral processes. While several DPAs across Africa already possess statutory authority to investigate, impose sanctions, and refer matters to the courts, these powers must be actively exercised and consistently enforced to deter violations and build accountability. DPAs should conduct investigations, access relevant data, and apply fines or corrective measures where breaches occur. They should also require political parties and electoral bodies to disclose how voter data is collected, stored, and used, ensuring transparency and compliance with lawful processing standards. Furthermore, DPAs must be empowered to penalize unauthorized harvesting, use, retention, or transfer of electoral data, particularly where consent was not freely obtained, and to sanction the misuse of disruptive technologies, such as generative AI, for misinformation, manipulation, or interference in electoral processes.

5.4. Invest in Human and Technical Capacity

There should be increased investment in both human resources and technical capacity of DPAs to effectively oversee activities of EBs and political actors in Electoral Processes.

DPAs must be equipped with specialized skills and modern tools to address data protection challenges unique to election contexts. Regular and targeted training programs should cover data protection principles, AI-driven disinformation, digital election infrastructure audits, risk mitigation strategies, and best practices in electoral data governance.

Encourage collaboration, exchange, and mentorship programs with well-established DPAs across Africa. Active engagement with regional networks such as the Network of African

Data Protection Authorities (NADPA) can enhance institutional resilience, promote peer learning, and support the harmonization of enforcement practices across jurisdictions.

5.5. Harmonize Legal Frameworks

Continued collaboration between regional DPAs should be encouraged and adopted to facilitate knowledge sharing sessions, develop model guidelines on data protection in electoral settings, establish minimum regional standards for data privacy in elections, including biometric data management, diaspora registration and voting, enforcement of social media accountability and joint investigative activities.

National data protection electoral laws should be jointly reviewed to align with African regional frameworks, thereby encouraging harmonised standards and coordinated cross border/continental overview of Data Protection Laws.

5.6. Regulate Foreign Election-Technology Vendors

National legislatures should amend data protection statutes to extend processor obligations expressly to foreign entities processing electoral data of citizens within their jurisdiction, modelled on the extra-territorial approach of the EU General Data Protection Regulation. EMBs should be required by law to include in all procurement contracts with foreign technology vendors: (i) mandatory DPA audit access rights; (ii) data localisation obligations for voter biometric and registration data; (iii) incident notification duties to the DPA within a prescribed period; and (iv) data deletion and certification obligations upon contract expiry. Regional bodies, particularly NADPA, ECOWAS, and the African Union, should develop model contractual clauses for the procurement of election technology by member states, ensuring that data sovereignty concerns are addressed uniformly across the continent. DPAs should further publish sector-specific guidance on the procurement of election technology, setting out the data protection requirements that EMBs must satisfy before engaging any foreign processor.

5.7. Increase Civic Engagement and Public Awareness

General electoral populace should be empowered through public engagements and civic campaign to understand digital privacy and exercise their rights under the various data protection laws.

DPAAs should partner with civil society watchdogs and media organisations in monitoring compliance, enhance public engagement and awareness to make it easier to file complaints about misuse and abuse of electoral data, for microtargeting and harmful campaign activities.

Prioritizing these recommendations will help reinforce the credibility and effectiveness of DPAs to safeguard personal data and electoral integrity. The ability of DPAs to function independently, transparently, and robustly will be crucial to maintaining democratic trust and upholding citizens' rights as Africa's digital democracy deepens.

6. Conclusion

As African countries increasingly digitize their electoral processes, the role of DPAs in safeguarding voters' personal data and ensuring privacy compliance has never been more critical. While significant progress has been made in establishing legal frameworks and institutional bodies across the continent, persistent challenges related to DPA independence, capacity, enforcement powers, and political influence continue to undermine their effectiveness in electoral contexts.

Strengthening institutional autonomy, enhancing technical expertise, harmonizing legal frameworks, and fostering regional cooperation are essential steps to empower DPAs to meet the complex demands of data governance during elections. Equally important is building public awareness and transparency to reinforce voter trust and uphold democratic integrity.

Without these reforms, gaps in electoral data protection risk exposing personal information to misuse, eroding citizen confidence, and weakening democratic processes. By implementing targeted policy measures that address these issues, African governments and

stakeholders can ensure that data privacy protections keep pace with technological advances, supporting free, fair, and credible elections throughout the continent.



Accountability in the Age of Digital Disinformation: Assessing Tanzania's Data Protection Obligations during Electoral Processes

Nuru Keenja * and Cosmas Babilas Masimo *

Abstract

This paper is intended to assess how Tanzania's legal framework responds to growing challenges brought by digital disinformation during political elections. The focus is on the Personal Data Protection Act⁹¹ and its interaction with other laws such as the Cybercrimes Act⁹², the Electronic and Postal Communications Act⁹³, and other electoral laws. Using doctrinal and qualitative methods, the paper argues that, although Tanzania has formal rules on personal data protection, these laws have many gaps and are inadequately enforced, especially during election periods. These weaknesses give political actors and institutions leeway to misuse personal data and spread disinformation. The paper offers recommendations for improving data protection, strengthening institutions, and ensuring accountability to protect democratic integrity amidst digital transformation. These findings have broader implications for digital governance and democratic integrity across Tanzania, East Africa and Africa at large.

* Nuru Keenja is an Assistant Lecturer in the School of Law at the University of Dodoma. She holds a Bachelor of Laws (LL.B.) from Ruaha Catholic University and a Master of Laws (LL.M.) from the University of Iringa. Nuru is actively involved in both teaching and scholarly research, with focused interests in ICT Law, Human Rights, and International Law. Her academic work contributes to advancing legal understanding and policy development in these critical areas. She can be contacted via email at: nurucharleskeenja@gmail.com / nuru.keenja@udom.ac.tz

* Cosmas Babilas Masimo is an Assistant Lecturer in the School of Law at the University of Dodoma, Tanzania. He is a duly enrolled as an Advocate of the High Court of Tanzania and subordinate courts thereto, as well as a Notary Public and Commissioner for Oaths. He holds a Bachelor of Laws (LL.B.) and a Master of Laws (LL.M.) from the University of Iringa. His research interests lie in intellectual property laws, ICT Laws, and the intersection of law, technology, and governance. Mr. Masimo is actively engaged in legal scholarship and professional practice.

He can be contacted via email at: cosmasmasimo12@gmail.com / cosmas.masimo@udom.ac.tz.

ORCID: <https://orcid.org/0000-0001-8433-3600>

⁹¹ Act No.11 of 2022.

⁹² Act 14 of 2015.

⁹³ [CAP. 306 R.E. 2022].

Keywords: *Data protection, electoral disinformation, accountability, Tanzania, digital governance, democracy.*

1. Introduction

In the age of Information and Communication Technology, and with the increased use of the internet and mobile phones, how people communicate, access information, and engage in national affairs has changed greatly. In Tanzania, more citizens are now using digital platforms such as social media, websites, and mobile apps to receive political news, express opinions, and participate in public discussions. These changes have brought many benefits to democratic processes, including faster communication and wider public engagement. However, they have also introduced serious challenges, one of the most concerning being the spread of digital disinformation.⁹⁴

Digital disinformation refers to false or misleading information that is deliberately created and shared to confuse, deceive, or manipulate people.⁹⁵ This kind of information can be used to influence public opinion, attack political opponents, or create mistrust during important events like elections. Disinformation can be shared quickly and widely through social media, messaging apps, and websites. What makes the problem worse is the growing use of personal data such as names, ID numbers, or even biometric details which can be collected, stored, and used without people's knowledge or consent.⁹⁶

The Personal Data Protection Act 2022 (PDPA),⁹⁷ was introduced to safeguard personal privacy by regulating how personal data is collected, processed, and used, including during

⁹⁴ Larry Diamond, "Facing Up to the Democratic Recession," *Journal of Democracy* 26, no. 1 (2015): 144 available at https://www.researchgate.net/publication/271730529_Facing_Up_to_the_Democratic_Recession accessed on 16.03.2026

⁹⁵ Ariel Kruger, Morgan Saletta, Atif Ahmad and P. Howe. "Structured expert elicitation on disinformation, misinformation, and malign influence: Barriers, strategies, and opportunities." *Harvard Kennedy School Misinformation Review* (2024).

⁹⁶ Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," *The Guardian*, March 17, 2018 available at <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed on 16.03.2026

⁹⁷ The Personal Data Protection Act, No.11 of 2022.



elections, when large amounts of voter information are gathered. Although the law establishes key principles such as consent and purpose limitation, significant gaps remain, particularly on how election related data may be repurposed by political actors or third parties to influence public opinion. Importantly, not all political information qualifies as personal data, and digital disinformation does not always rely on personal data processing. This means, the connection between disinformation and the PDPA is not straightforward and mostly vague as it can be observed under the case of *Tito Magoti v. Attorney General*.⁹⁸ In this case, the applicant challenged the constitutionality of several provisions of the PDPA arguing that they were unclear and failed to provide clear procedures for enforcement, thus infringing fundamental rights such as the right to privacy and equality before the law. In this case the High Court examined whether the disputed provisions met the standard of legal certainty required under the Constitution. In its reasoning, the Court emphasized that laws affecting fundamental rights must be precise and accompanied by clear procedural safeguards. Therefore, it declared section 22(3) and parts of section 23(3) unconstitutional for lack of clarity and enforceable standards. This decision highlights the bigger issue that ambiguities within the Act may weaken its effectiveness, particularly in sensitive contexts such as electoral processes.

The Constitution of United Republic of Tanzania,⁹⁹ and other legal instruments such as the Cybercrimes Act¹⁰⁰, the Electronic and Postal Communications Act¹⁰¹, and election-related laws have provisions that provides for rights such as the right to data privacy, and other obligations related to online safety, and electoral conduct. However, these laws are not always harmonized, and some fail to address how personal data should be handled in electoral contexts or how digital disinformation should be countered. This lack of coordination weakens the ability of institutions to hold offenders accountable.

This paper looks into the legal and institutional gaps to ascertain and legal obligations on personal data protection during elections. The assessment intends to verify if the existing

⁹⁸ *Tito Magoti vs. The Attorney General (Miscellaneous Civil Cause No. 18 of 2023)*.

⁹⁹ The Constitution of United Republic of Tanzania of 1977 (as amended from time to time).

¹⁰⁰ Act 14 of 2015.

¹⁰¹ CAP. 306 R.E. 2022.

framework can support accountability in combating digital disinformation during political election processes. The central argument is that Tanzania's data protection framework provides formal mechanisms to promote accountability but suffers from actual application. In addition, there are legal gaps that undermine its effectiveness. The PDPA¹⁰² sets foundational standards but problems such as weak enforcement powers, institutional overlap, and lack of remedial mechanisms allow electoral disinformation to take place and spread unchecked.¹⁰³

The methodology used in this study combines doctrinal legal research and qualitative analysis. The doctrinal approach focuses on analyzing statutes, regulations, and policy documents to understand their structure and intent. The qualitative element reviews secondary sources and publicly available materials and information to assess how laws are applied in practice. This paper does not rely on fieldwork or interviews.

This paper argues that Tanzania has made valuable progress in establishing a legal framework for personal data protection. However, for the country to safeguard its democratic integrity in the digital age, especially during election periods, laws must be clarified, public awareness increased, and institutional capacity improved. Only then can citizens' data be protected and electoral disinformation effectively curbed.

2. Conceptual and Normative Framework

Understanding how digital disinformation affects elections and how data protection can improve accountability begins with clarifying key terms and ideas. This section explains what digital disinformation is, what accountability means in the digital environment, and how data protection laws can help reduce electoral abuse arising from digital disinformation.

¹⁰² Act No.11 of 2022.

¹⁰³ Augustino Mwogosi and Richard Simba, "Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review," Digital Policy, Regulation and Governance (2025), <https://doi.org/10.1108/dprg-11-2024-0289> accessed on 16.03.2026.

2.1. Digital Disinformation and Electoral Manipulation

Digital disinformation refers to false or misleading information that is intentionally created and spread to deceive others.¹⁰⁴ It differs from misinformation, which may also be false, but is shared without the aim of causing harm or confusion.¹⁰⁵ In electoral settings, disinformation is often used to influence voters, discredit candidates, or create social and political unrest. It is commonly spread through digital platforms such as social media, messaging apps, or websites.

One of the most concerning features of digital disinformation is its connection to personal data. Political actors or other groups may collect data about voters such as their names, location, political opinions, or browsing habits and then use that information to send them targeted false messages.¹⁰⁶ In Tanzania there is a legal requirement under the National Elections Act to establish and maintain a voters' register that includes personal details such as names, sex, and residential address of registered voters.¹⁰⁷ This register, including a provisional version for public inspection and its amendment, is made accessible as part of the election process. For one, this increases availability of personal data and heighten risks when such data are used for targeted messaging or manipulation without adequate safeguards. This makes it easier to manipulate public opinion in a subtle and powerful way.¹⁰⁸

2.2. Accountability in the Digital Age

Accountability refers to the responsibility of individuals, groups, or institutions to explain and justify their actions and to face consequences when they fail to meet expected

¹⁰⁴ Tom Buchanan, "Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinformation." *PLoS ONE*, 15 (2020), p. 1. Available at <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0239666> accessed on 16.03.2026.

¹⁰⁵ American Psychological Association, "Misinformation and Disinformation," *APA*, accessed July 11, 2025, <https://www.apa.org/topics/journalism-facts/misinformation-disinformation>.

¹⁰⁶ Carole Cadwalladr and Emma Graham-Harrison, (Supra)

¹⁰⁷ Cap 343.

¹⁰⁸ *Ibid.*

standards.¹⁰⁹ In digital governance, and in the context of political elections, accountability can be divided into four key types as follows; -

- a. Legal accountability, which refers to the requirement to follow laws and face legal penalties when those laws are broken.
- b. Political accountability which means that public leaders and institutions must answer to voters and elected bodies.
- c. Administrative accountability which deals with internal oversight within institutions, such as disciplinary systems in election commissions.
- d. Social accountability which involves external checks from civil society, journalists, and the public.

In the context of digital disinformation, accountability means asking important questions like who should be held responsible when lies are spread online? What happens when a political party uses personal data without relevant consent of the data subject? Can institutions be legally challenged for failing to stop disinformation? These questions are not easy to answer. In many cases, disinformation may be created by private companies, spread through foreign servers, or supported by political groups. Therefore, laws and systems must clearly state who is responsible and how they can be held accountable. Without this clarity, efforts to stop disinformation will likely fail.

2.3. Data Protection as an Accountability Tool

Data protection laws play an important role in strengthening accountability in elections. These laws regulate how personal data is collected, used, stored, and shared. When effectively enforced, they can help reduce misuse of personal data that often lead to electoral disinformation.¹¹⁰ In Tanzania, the PDPA¹¹¹ and its Regulations¹¹² set out clear

¹⁰⁹ Evert Lindquist and Isabelle Huse, “Accountability and Monitoring Government in the Digital Era: Promise, Realism and Research for Digital-Era Governance,” *Can Public Admin*, 60: 627-656. (2017) <https://doi.org/10.1111/capa.12243> accessed on 16.03.2026.

¹¹⁰ Augustino Mwogosi and Richard Simba, “Digital Policy and Governance Frameworks for EHR Systems in Tanzania: A Scoping Review,” *Digital Policy, Regulation and Governance* (2025), <https://doi.org/10.1108/dprg-11-2024-0289> accessed on 10.03.2026.

¹¹¹ Act No.11 of 2022.

¹¹² Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, G.N. No. 449C published on 4/7/2023.

rules on how personal data should be collected, stored, used, and shared. These rules are very important during elections because large amounts of personal data are handled. When personal data is not well protected, it can be misused for spreading false information or for unfair political targeting.

The following principles help prevent these problems and promote accountability in electoral processes; -

- 1) Lawfulness, this principle means that data must be collected and used according to the law. The purpose must be legal, and the person whose data is being used must understand what is being done with their information. They should also be able to withdraw their permission if they change their mind.¹¹³ In elections, this stops political actors from using personal data for illegal purposes like secret targeting or manipulation. This is in alignment with the best practice from Article 6 of the European Union General Data Protection Regulation (GDPR) which requires that data processing be grounded in a clear lawful basis, with explicit consent and transparency.¹¹⁴ Best practice requires data controllers to ensure that all personal data is collected and processed strictly in accordance with the law. This includes providing clear notices, obtaining valid consent, and documenting the legal basis for each processing activity. Data controllers should also maintain internal compliance systems, such as data-protection policies and regular audits, to prevent unlawful use. If a data controller fails to comply, data subjects should be able to exercise their right to withdraw consent, request explanations, or file complaints with the Personal Data Protection Commission (PDPC). The PDPC, in turn, should investigate, issue compliance orders, impose administrative penalties, or direct the suspension of unlawful processing activities.
- 2) Specific Purpose, this principle says that data should only be used for the purpose it was collected for.¹¹⁵ If voter data is collected for registration, it should not be

¹¹³ The Personal Data Protection (Personal Data Collection and Processing) Regulations, GN No. 449C of 2023, Regulation 25.

¹¹⁴ The General Data Protection Regulation (Regulation (EU) 2016/679).

¹¹⁵ *Ibid.*, Regulation 26.



used for political advertisements or other unrelated goals unless the voter agrees. This protect voters from their data being secretly reused or exploited during campaigns. To comply with this principle, data controllers must define and communicate the exact purpose for which data is collected and ensure that the data is not repurposed without fresh consent or legal basis. Best practice includes maintaining purpose, limitation registers and training staff to avoid unauthorized secondary uses. Where violations occur, such as using voter data for political advertising, data subjects may demand cessation of processing and lodge complaints. The PDPC should require the controller to stop the unlawful use, delete improperly used data, and take corrective measures to prevent recurrence.

- 3) Security measures, under this principle the law requires strong protection for personal data so that it does not get stolen, changed, or shared with the wrong people.¹¹⁶ This includes having strong passwords, restricted access, and quick action if there is a data breach. During elections, this protects voters from data leaks that could be used to spread disinformation or manipulate their opinions. Data controllers should adopt robust technical and organizational measures, including encryption, access controls, secure servers, and breach-response procedures. Regular vulnerability assessments and staff training are essential to prevent unauthorized access or leaks. If security failures occur, data subjects should be notified promptly and may demand remedial action or compensation where applicable. The PDPC should enforce mandatory breach reporting, conduct investigations, and impose sanctions for negligent or reckless handling of personal data.
- 4) Data minimization, only the data that is truly needed should be collected.¹¹⁷ This principle helps avoid collecting too much information that could later be abused. For example, collecting just a voter's name and ID may be enough, without needing their full address or other sensitive details. It also encourages using methods that reduce risk, such as hiding names when not needed. Best practice requires data controllers to collect only the minimum data necessary for the intended purpose.

¹¹⁶ *Ibid.*, Regulation 27.

¹¹⁷ *Ibid.*, Regulation 28.

This includes conducting data-minimization assessments and avoiding the collection of excessive or sensitive information unless strictly required. If a controller collects unnecessary data, data subjects may challenge the collection and request deletion of irrelevant information. The PDPC should review such practices and direct controllers to redesign their data-collection processes to comply with the principle of data minimization.

- 5) Accuracy, voter data must be correct and kept up to date.¹¹⁸ If someone's information is wrong, they have the right to ask for it to be corrected. This is very important in elections where wrong information could stop someone from voting or could be used to send them misleading messages. Data controllers must establish mechanisms for regular data updates, verification procedures, and correction workflows. In electoral contexts, this includes ensuring that voter rolls are accurate and promptly updated. Where inaccuracies arise, data subjects have the right to request correction or deletion. The PDPC should ensure that controllers implement effective correction systems, and issue enforcement notices where persistent inaccuracies undermine electoral integrity.
- 6) Storage Limitation, data should not be kept forever. It should only be stored for as long as it is needed, and then it must be safely discarded.¹¹⁹ In elections, this helps stop political actors from keeping and reusing data for future campaigns without permission. Controllers should implement retention schedules that specify how long each category of data is kept and ensure secure deletion once the purpose is fulfilled. Best practice includes automated deletion systems and periodic reviews of stored data. If data is retained longer than necessary, data subjects may request deletion. The PDPC should require controllers to justify retention periods and order the destruction of data kept unlawfully.
- 7) Rights of the Data Subject, people must have control over their own data. They should be able to ask who has their data, how it is being used, and to challenge any misuse.¹²⁰ This principle gives power to voters and helps make sure those who

¹¹⁸ *Ibid.*, Regulation 29.

¹¹⁹ *Ibid.*, Regulation 30.

¹²⁰ *Ibid.*, Regulation 31.

handle their data act responsibly. Data controllers must establish accessible procedures for data subjects to exercise their rights, including access, correction, objection, and deletion. This requires clear communication channels, timely responses, and transparent record-keeping. If controllers fail to respect these rights, data subjects may escalate the matter to the PDPC. The PDPC should enforce compliance, issue penalties, and ensure that controllers adopt rights facilitation mechanisms.

These principles are not just technical requirements. They are important tools for ensuring that individuals have control over their data and that those who misuse data can be held responsible. In the context of electoral processes, data protection becomes a powerful way to ensure fairness, build trust, and reduce the risk of manipulation through disinformation.

3. Legal and Institutional Landscape in Tanzania

This part discusses set of laws and institutions for governance and regulation of digital disinformation and the protection of personal data protection.

3.1. Legal Framework

There are several laws that are relevant to when dealing with digital disinformation and protection of (personal) data protection as follows;

3.1.1. The Constitution of the United Republic of Tanzania¹²¹

The Constitution explicitly recognizes the right of privacy under article 16(1) which provides that:-

“Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications.”

¹²¹ Cap 2 of 1977 as amended from time to time.

The above clause establishes a fundamental right to privacy and under this constitutional guarantee citizens can claim a general right not to have their private correspondence or personal space arbitrarily invaded. This constitutional provision reflect article 17(1)¹²² of the International Convention for Civil and Political Rights (ICCPR) which provides that;-

“No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

This reaffirms the constitutional standard and implies that Tanzania undertook the obligation to enact and enforce laws to prevent unlawful interference with individual privacy – including those related to correspondences and information exchange – their collection or disclosure. In an electoral setting, this would suggest that any derogation to the protection of this right should have a clear legal basis and justifiable necessity.

3.1.2. The Personal Data Protection Act¹²³

The PDPA¹²⁴ is the first comprehensive data protection law applicable on mainland Tanzania and Zanzibar, on union matters. It applies to any person or entity that is likely to be a data controller or processor who processes personal data in Tanzania. The PDPA explicitly includes public bodies within its scope and the definition of data controller¹²⁵ covers a public body that determines the purpose or means of processing. This means government agencies including the Independent National Electoral Commission (INEC) are equally bound by the Act when they handle personal data. This also means that the

¹²² International Covenant on Civil and Political Rights (adopted 19 December 1966, entered into force 23 March 1976).

¹²³ Act No.11 of 2022.

¹²⁴ *Ibid.*

¹²⁵ *Ibid*, section 3, state that “data controller” means a natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data; and where the purpose and means of processing are determined by law, “data controller” is the natural person, legal person or public body designated as such by that law and it includes his representative.

voter registration list, biometric records, or polling data maintained by election authorities must be done so in accordance with the PDPA.

The PDPA establishes an autonomous PDPC responsible for registration of data controllers and processors, for handling complaints, and for enforcement actions. The Commission can investigate violations, issue enforcement notices and financial penalties, seek court preservation orders, and demand compensation for data subjects.¹²⁶

The PDPA spells out data protection principles in Part IV by stating that personal data must be processed lawfully, fairly, and in a transparent manner collected only for explicit and legitimate purposes, and kept no longer than necessary. It also requires data to be accurate and secure, and grants data subject rights to access, correct or erasure. For example, Section 5(1) of the PDPA¹²⁷ requires persona data to be processed lawful, fair and in a transparent manner, Sections 22 to section 30 elaborate obligations on consent, purpose limitation, accuracy, and special categories of data which are sensitive like health, race and biometric details. These provisions reflect global standards, and if enforced could restrict ability to exploit personal data that may lead to disinformation during election processes.

The PDPA¹²⁸ also contains significant exemptions and ambiguities under Part IX especially Section 58, which provides that processing may be exempted if done by; the data subject personally; in accordance with any law or court order; for purposes of national security or public interest; to prevent or detect crime; to prevent tax evasion; to investigate misappropriation of public funds, or; for vetting appointments. This means that if an agency claims to be acting under another law, for instance election law or national security laws, the principles for the processing of personal data within the PDPA will cease to apply.¹²⁹ For example, an electoral official could argue that processing voters' data for election monitoring is authorized by the National Election Act, thus bypassing consent requirements.

¹²⁶ *Ibid*, section 7.

¹²⁷ *Ibid*.

¹²⁸ *Ibid*.

¹²⁹ *Ibid*.



Furthermore, a significant part of the problem arises from the National Elections Act,¹³⁰ which permits the large-scale collection, publication, and dissemination of voters' personal information like as names, addresses, polling stations, and identification details, as part of the voter register and verification process. Because this law predates the PDPA, it contains broad exemptions framed around safeguarding national security, public safety, and public interest, which effectively allow electoral authorities to process and disclose personal data without applying the strict safeguards required under the PDPA.

In practice, this creates a legal conflict: the Elections Act¹³¹ authorizes extensive data processing and public disclosure, while the PDPA requires purpose limitation, data minimization, and strict protection of personal data – including restrictions on public disclosure of such data. As long as the Elections Act remains unamended, regulators and courts retain wide discretion to interpret public interest in ways that may override normal data-protection rules, thereby exposing voters to risks such as profiling, targeted political messaging, and manipulation during elections. For this reason, the National Elections Act¹³², like many statutes that pre-dates the PDPA require urgent harmonization with the PDPA to ensure that electoral transparency does not defeat the very purpose of data protection.

The PDPA also grants individuals various rights under Part VI to include the right to access and correct personal data, the right to object to certain processing and the right to have data erased or blocked.¹³³ A voter could use these rights to challenge improper use of their data, including demand deletion if such data was used without consent or legal basis. The PDPA also allows individuals to seek compensation for damage caused by unlawful data processing¹³⁴ and to complain to the PDPC.¹³⁵

The PDPA criminalizes unauthorized data practices and makes it an offence for a data controller to unlawfully disclose, delete, or conceal personal data, with penalties reaching

¹³⁰ [Cap 343 of 2024].

¹³¹ *Ibid.*

¹³² *Ibid.*

¹³³ *Ibid.*, section 38.

¹³⁴ *Ibid.*, section 50.

¹³⁵ *Ibid.*, section 39.

20 million Tanzanian shillings or imprisonment of up to 10 years. This punitive approach also exposes a deeper regulatory challenge. The existence of criminal sanctions without clear harmonization with sector specific laws, such as the National Elections Act creates uncertainty for both regulators and data controllers. This misalignment means that electoral authorities may continue processing and publishing personal data under older legal regimes while simultaneously risking criminal liability under the PDPA. This tension underscores the urgent need for regulatory amendments and alignment to ensure that criminal provisions operate coherently and do not undermine the broader purpose of protecting voters' personal data.

3.1.3. Electronic and Postal Communications Act¹³⁶

The Electronic and Postal Communications Act regulates telecoms and online content. It has two salient features for privacy. First, it requires all SIM card owners to register their identity and biometric data (fingerprints) before using a mobile SIM. The country's mandatory SIM card registration framework requires all mobile phone users to provide personal information, which includes biometric fingerprints, to mobile operators, who must then submit this information to the Tanzania Communications Regulatory Authority (TCRA)¹³⁷ as part of a centralized regulatory database. Independent research further confirms that Tanzania's SIM registration system is integrated with the national biometric identity infrastructure, meaning that the personal data of virtually every mobile phone subscriber is stored within systems controlled by the government.¹³⁸ In principle, such centralized datasets could be cross-checked with voter registers or other state-held files, creating significant risks of profiling, political targeting, or other forms of electoral manipulation, if not properly regulated.¹³⁹

Secondly, the Act includes a privacy provision which prohibits network operators from disclosing customer data except as authorized by law.¹⁴⁰ The Act gave TCRA power to

¹³⁶ [CAP. 306 R.E. 2022].

¹³⁷ The *Electronic and Postal Communications (SIM Card Registration) Regulations*, G.N. 112 of 2020.

¹³⁸ Digital Agenda for Tanzania Initiative. (2023), "Digital Identity Ecosystem Mapping for Tanzania". Dar es Salaam, DATI, 2023.

¹³⁹ G.N. no.112 of 2020.

¹⁴⁰ [Cap 306 R.E. 2022], Section 93.

oversee SIM registration and allowed disclosure of SIM data to law enforcement with a warrant. In elections, SIM registration helps to verify voters' identity, but it also means all voters' phone numbers and fingerprints are known by the state.¹⁴¹ The Act focus on technical infrastructure rather than content regulation creates gaps in addressing sophisticated disinformation campaigns.

Within this Law, the government issued the Electronic and Postal Communications (Online Content) Regulation¹⁴² which requires online platforms, blogs, and streaming media to register and pay high fees to operate. During election periods the provisions of this regulation can be used to block unauthorized dissemination of any politically sensitive content, thus indirectly limiting the sharing of data or analysis about the election.

3.1.4. Cybercrimes Act¹⁴³

The Cybercrimes Act criminalizes various forms of online acts and omissions, including the publication of false information with intent to cause harm. It prohibits the publication of false, deceptive, misleading, or inaccurate information, with penalties including fines and imprisonment. While this provision could theoretically address electoral disinformation, its broad language and vague standards raise concerns about selective enforcement and potential misuse to silence legitimate political criticism.¹⁴⁴

3.1.5. Media Services Act¹⁴⁵

This Act imposes licensing and accreditation requirements on news media and online publishers. It established the Media Services Council to license outlets such as online and satellite broadcasters. The Act does not directly address data protection, but it has been criticized for chilling media freedom. By requiring journalists to register with the Council and follow a code of conduct, it may indirectly affect what information is reported. During

¹⁴¹ *Ibid*, section 58.

¹⁴² G.N No. 913 of 2020.

¹⁴³ Act 14 of 2015.

¹⁴⁴ *Ibid*, section 16.

¹⁴⁵ Chapter 229.

elections, media scrutiny is crucial, so constraints on media bodies matter indirectly for transparency.

3.1.6. The Statistic Act¹⁴⁶

The Statistics Act makes it illegal for anyone including journalists or party agents to publish or disseminate election results even partial results without official approval. This was widely seen as curbing transparency and even led to the detention of civil society actors. In effect, the law controls information flow from polling stations. In terms of data protection, it is less about personal data and more about information control, although it illustrates how non-data laws can restrict the handling of election-related information.

3.1.7. The National Election Act¹⁴⁷

The National Election Act governs voter registration through the Independent National Electoral Commission. The Commission operates a biometric voter registration system, and the collected data includes fingerprints and photos of all registered voters. Legally, this system is established by election law, which does not include detailed privacy provisions. However, any processing of this data should be subject to the Personal Data Protection Act.¹⁴⁸

3.2. Institutional Mechanisms

Tanzania's institutional framework for addressing electoral disinformation involves multiple institutions with deferent mandate. These institutions include the following;

3.2.1. Personal Data Protection Commission

The PDPC established under the PDPA¹⁴⁹ is the primary regulator of personal data protection. Its independence is assured by law, but in practice it is an administrative agency under the President's office. The PDPC has powers to enforce the law by issuing

¹⁴⁶ Chapter 351 R.E. 2019.

¹⁴⁷ Chapter 343 of 2024.

¹⁴⁸ Act No.11 of 2022.

¹⁴⁹ Act No.11 of 2022.

enforcement notices, specific orders, administrative and financial penalties. However, it lacks prosecutorial powers; it relies on the Director of Public Prosecutions to prosecute offences.¹⁵⁰

3.2.2. Tanzania Communications Regulatory Authority

The Tanzania Communications Regulatory Authority (TCRA) plays a crucial role in regulating electronic communications, including oversight of telecommunications operators and internet service providers. The Authority sits at a junction of security vs. rights: it can enforce communications policy swiftly.

3.2.3. The Independent National Electoral Commission

This Commission is responsible for voter registration, the conduct of elections, and announcing results. It collects and safeguards highly sensitive data such as voter biometrics, polling forms, etc. As a public body, the Commission is bound by the Data Protection Act, like any other data controller.

3.2.4. The Tanzania Police Force and the Judiciary of Tanzania

The police and courts also play a role in regulating data. The Cybercrimes Act¹⁵¹ empowers the police to demand data and to arrest individuals for false online content. Courts are a potential avenue for accountability through judicial review or constitutional petitions.

3.2.5. Civil Society and Media Houses

Non-governmental organizations, journalists, and tech platforms form the last line of accountability. Mainstream media in Tanzania have also struggled with restrictions on reporting. The atmosphere is not very conducive to whistleblowing; indeed, journalists have been arrested for covering election results in violation of the Statistics Act.¹⁵² This environment means that any accountability through social channels is weak.

¹⁵⁰ *Ibid*, section 7.

¹⁵¹ Act 14 of 2015.

¹⁵² Chapter 351 R.E. 2019.

4. Challenges of Digital Disinformation in Tanzanian Elections

Even with the laws in place, disinformation is still a challenge during election processes. The challenges entail the following;

4.1. Data Weaponization during Election Campaigns

Election campaigns are peak times for exploiting personal data. Voter lists and identity databases can be used by parties or third parties to micro-target voters with tailored messages. Because of limited data literacy, many citizens may not know when their data is being used or misused or whom to complain to. The PDPC has warned that during campaigns “personal data tends to be most at risk some individuals weaponize personal data for political ends”.¹⁵³ Whether this warning translates into concrete action is unclear, but it shows that data use is on people’s minds. The difficulty in elections is tracing illicit data use: if disinformation spreads, it often comes without a clear chain of custody or obvious violator.

4.2. Regulatory Uncertainty

The Independent National Electoral Commission has no audit requirement which pave the way for people’s privacy and their personal data to be interfered with or used illegally during election process.

4.3. Government Information Controls and Internet Shutdowns

The government has been rigid by controlling information and initiating media blackouts during sensitive periods. This environment restricts free debate, making it harder for voters/ citizens to access truthful information. A good example is the government's internet shutdowns during the 2020 and 2025 elections which made it easier for disinformation to spread. When people could not access news or verify information online, false stories and rumors filled the gap. In 2020 the internet was restricted for 11 days¹⁵⁴, and the same

¹⁵³ PDPC statements reported in The Citizen, “Why Safeguarding Online Space Matters During Election Season” (2025).

¹⁵⁴ Internet Society Pulse (2020), Shutdown United Republic of Tanzania. Available at <https://pulse.internetsociety.org/shutdowns/country/tanzania>. See also, Bhalla, Nita. "How an Internet

happened in 2025 election where the internet was shut down for 5 days¹⁵⁵. These internet shutdowns created the vacuum that allowed misleading information to spread quickly because citizens had no way to check what was true or otherwise.¹⁵⁶

4.4. Public Awareness and Trust

Many Tanzanians may not be fully aware of their privacy rights or how to exercise them. Trust in institutions also matters, if people believe regulators are politically influenced, they may not trust complaints will be handled fairly. If a ruling party in government were suspected of misusing data, opposition voters may feel there is no impartial recourse.

4.5. Digital Divide and Vulnerabilities

Not all citizens are online, but those who are may be less media-savvy. Disinformation tends to target emotions and can spread rapidly among groups with limited access to fact-checking. In Tanzania, disinformation often spreads via WhatsApp chains or local media including radio. The mix of high mobile penetration with limited user awareness creates fertile ground for rumors and disinformation.

4.6. Enforcement Challenges in Electoral Data Protection

Enforcing data protection obligations during elections in Tanzania faces several critical difficulties. Although the PDPC is empowered to investigate and sanction violations, its actual capacity particularly in politically sensitive electoral contexts remains unproven. There are concerns also on the PDPC's independence, especially during election periods when impartial oversight is most needed. Additionally, the available legal remedies under the PDPA may not effectively address the unique harms caused by electoral disinformation. Many affected individuals lack awareness, access to legal support, or the resources to pursue timely recourse rendering post-election remedies largely ineffective. The political

Blackout Affected Tanzania's Election." Context (Thomson Reuters Foundation), November 5, 2025. <https://www.context.news/digital-rights/how-an-internet-blackout-affected-tanzanias-election>.

¹⁵⁵ African Commission on Human and People's Rights (November 1, 2025) Press release on the national wide internet outage on election day. Available at <https://achpr.au.int/en/news/press-releases/nationalwide-internet-outage-tanzania>.

¹⁵⁶ *Ibid.*

nature of electoral disinformation further complicates enforcement. Regulatory bodies may hesitate to act on sensitive cases for fear of appearing partisan, while delays in enforcement either before or after elections can undermine both credibility and impact.

5. Recommendations and Policy Implications

Based on the analysis of Tanzania's current framework and the identified gaps, several key recommendations emerge to strengthen the country's capacity to address electoral disinformation through improved data protection mechanisms and institutional reforms.

5.1. Legal Framework Reforms

Tanzania urgently needs comprehensive legal reforms to address the identified gaps in its data protection and electoral frameworks. The PDPA should be amended to include specific provisions governing electoral data processing, establishing clear standards for political parties' use of voter data, requirements for explicit consent before processing personal data for political purposes, mandatory transparency reporting on data collection and use during electoral periods, and enhanced protections for biometric data collected through voter registration.

5.2. Institutional Strengthening

The PDPC, The National Electoral Commission, TCRA and other relevant institutions must work together in making sure that they limit disinformation during election by making sure that the public is aware of the laws (providing education), training within institutions on human rights, and ensuring independence of these institutions to make sure that the discharge of their mandate are free from political influence in order to maintain election integrity and data protection during election processes.

5.3. Enforcement Mechanisms

Tanzania needs stronger enforcement mechanisms that can effectively address electoral disinformation while respecting democratic principles. This includes establishing specialized courts or procedures for handling digital rights cases, particularly those involving electoral contexts, training programs for judges and prosecutors on digital

evidence and data protection law, expedited procedures for addressing electoral disinformation during campaign periods, and meaningful remedies for individuals and communities affected by data protection violations in electoral contexts.

5.4. Multi-Stakeholder Engagement

Addressing electoral disinformation requires engagement from various stakeholders beyond government agencies. Civil society organizations play crucial roles in monitoring, exposing, and countering disinformation, and they need support to build capacity for these activities. This includes funding for digital literacy programs, training for civil society monitors to support their ability to identify and document disinformation, and protection for civil society actors who face threats due to their monitoring activities.

5.5. Monitoring and Evaluation

The effectiveness of these recommendations requires robust monitoring and evaluation mechanisms. Regular assessments to evaluate the implementation of legal reforms, the capacity and independence of regulatory agencies, the effectiveness of enforcement actions, and the overall impact on electoral integrity is crucial. These assessments should involve multiple stakeholders and should be transparent and publicly available.

6. Conclusion

This analysis shows that Tanzania’s newfound data protection framework holds potential to safeguard democratic processes, but only if the identified gaps are addressed. The PDPA¹⁵⁷ is an important step, enshrining principles like consent and transparency. Yet the PDPA’s broad “public interest” carve-out and imprecise terms leave room for abuse. Without narrowing these exemptions and clarifying the law (as the courts have urged), political actors can exploit personal data without effective oversight or remedies for the data subjects. In practice, Tanzania’s regulators have already used heavy-handed measures during elections (internet shutdowns, media restrictions) that raise serious rights concerns.

¹⁵⁷ Act No.11 of 2022

To turn the tide, reforms are needed. These include tightening the legal text, bolstering an independent data protection authority, and explicitly integrating privacy safeguards into electoral administration. Election officials should adopt clear data protocols, and be held accountable for how they collect and use voter information. Civil society and the international community can also play a role by monitoring elections for data abuses and advocating for transparency.

In the digital age, data is powerful and can be used for good or ill. Tanzania's experience illustrates the dilemma of contemporary elections: technology enables greater voter engagement, but also new avenues for manipulation. Accountability is the fulcrum. If legal and institutional arrangements can be strengthened so that misuse of personal data is not left unchecked, then Tanzania can better protect both individual privacy and the integrity of its elections. Otherwise, the very tools of digital democracy may undermine the democratic process itself.

Politicisation Risks in Cross-Border Transfers of Personal Electoral Data in Tanzania

Amiri Sharifu*

Abstract

*The 2025 general elections in Tanzania marked a significant milestone for personal data protection, as they were the first elections conducted following the enactment of the stand-alone Personal Data Protection Act (“PDPA”). This article examines the intersection between Tanzania’s electoral processes and the PDPA framework, with particular focus on how the Act regulates cross-border transfers of electoral data. It observes that although the Personal Data Protection Commission (“PDPC”), responsible for implementing the PDPA, is vested with extensive statutory powers, it lacks formal institutional independence. This raises concerns about its ability to impartially determine applications for cross-border transfers of personal electoral data. A comparative review shows that, unlike Tanzania, jurisdictions such as Kenya, Uganda, South Africa, and Nigeria at least provide for the theoretical independence of their data protection authorities, signaling some degree of commitment to safeguarding regulatory autonomy. The concerns regarding the independence of the PDPC, also reflected in *Tito Magoti v. Attorney General*, Misc. Civil Cause No. 18 of 2023, underscore the risk of external influence over its decisions. The article concludes by proposing reforms to strengthen the PDPC’s independence in assessing requests for cross-border transfers of personal data, including personal electoral data.*

* Amiri Sharifu, Principal Associate at A&K Tanzania; Business Law and Business Management Tutor at DSM CPA Review Center; and Lead at Tanzania M&A Tracker. Email: amiri.sharifu@alnafrica.co.tz.

1. Introduction

Tanzania holds its presidential and parliamentary general elections every five years. The 2025 general elections are considered monumental for expert assessments of the intersection between electoral processes and the legal framework for personal data protection. This is because they were the first elections held since Tanzania enacted a distinct personal data protection law. The Personal Data Protection Act (“**PDPA**”), enacted in 2022 as stand-alone data protection legislation, which came into effect on the 1st May 2023, following a commencement notice issued on the 28th of April 2023, by the Minister responsible for the Ministry of Communication and Information Technology.

The PDPA defines what amounts to personal data, provides for the obligations of those who collect and process personal data, and sets out the requirements for cross-border personal data transfers. It also establishes the PDPC. This article goes through the powers of the PDPC, including its authority to approve the transfer of personal data outside Tanzania; monitor compliance by data controllers and data processors; receive, investigate, and deal with complaints about alleged violations of the rights related tied to personal data and the privacy of; and inquire into, and take measures against any matter that appears to the PDPC to affect the protection of personal data and the privacy of persons.

The manner in which personal data is defined under section 3 of the PDPA means that all voter information falls within the scope of personal data, since they constitute personal identifiers. In that regard, all personal electoral data is regulated by the PDPA and its attendant regulations. With this nexus, the powers of the PDPC, including its discretionary authority to approve each transfer of personal data outside Tanzania, extend to personal electoral data. Consequently, if the PDPC’s independence is compromised, the likelihood that it may invoke its discretionary mandate to deny approval for the transfer of personal electoral data, thereby negatively impacting the democratization of elections, is high.

This article is structured into three main parts. It begins with an introduction, followed by the main body, which starts with preliminary matters such as the legislative background and definitions of key terms and concepts. The main body then includes a core section that discusses cross-border data transfers in Tanzania. Finally, the article concludes with remarks and offers certain recommendations.

2. Legislative Background

Prior to the coming into force of the PDPA, the provisions related to the protection of personal data were scattered across various legislations, most of which were sector specific. In addition to being dispersed among different laws, these provisions were inconsistent and varied across sectors. For example, the requirements under telecommunications laws were not aligned with those under banking and finance laws.

Since the enactment of the PDPA, the Government of Tanzania has been actively working on its operationalisation, including the publication of what this article refers to as the “twin Data Protection Regulations.” These regulations are the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, and the Personal Data Protection (Complaints Settlement Procedures) Regulations, 2023. Together, the twin Data Protection Regulations play a significant role in the effective implementation of the PDPA.

The objectives of the PDPA include providing for principles of protection of personal data that establish minimum requirements for the collection and processing of personal data, providing for establishment of PDPC, to reinforce the PDPA to ensure protection of personal data processed by public and private bodies. In cognizant with the foregoing objectives, the PDPA imposes various obligations on data controllers and data processors when undertaking their activities.¹⁵⁸

3. Personal Data versus Personal Electoral Data

The PDPA defines personal data as data about an identifiable person that is recorded in any form, including data relating to a person’s race, national or ethnic origin, religion, age, marital status, address, name, or correspondence of a private or confidential nature that reveals a person’s views or opinions. The Tanzanian electoral laws¹⁵⁹ do not define what amounts to personal electoral data. However, what constitutes such data may be inferred from the nature of the information required for a person to be registered as a voter under the law, and as indicated in the voter registration form

¹⁵⁸ Data controllers are defined as natural or legal persons who alone or jointly with others determine the purposes and means of processing personal data. The purpose of collecting personal data may include the collection of personal data for security purposes, execution of the contract, tax returns, employment, KYC, and for purposes of obtaining services and procuring goods. On the other hand, data processors are defined as natural or legal persons who process personal data for and on behalf of the data controllers.

¹⁵⁹ Some primary principal and subsidiary legislation include the National Elections Act, Cap 343 R.E 2023; the Presidential, Parliamentary, and Councillors’ Elections Act, Act No. 1 of 2024; the Electoral Code of Conduct for Presidential, Parliamentary, and Councillors’ Elections, 2025; the Independent National Electoral Commission Act, Act No. 2 of 2024; and the Local Authorities (Elections) Act, Cap 292 R.E 2023.

(Form No. 1). When it comes to registration, anyone who wants to register as a voter is required to fill out Form No. 1.

The form requires applicants to provide a range of personal details. These include their first, middle, and last names; gender; date of birth; and full residential address, covering the house number, street or village, ward, shehia, constituency, and district or town council. Applicants must also provide their postal address, occupation, and citizenship status, indicating whether they are citizens by birth or through naturalization and, where applicable, providing the date, certificate number, and place of naturalization. In addition, the form requires information on any disability, such as hearing impairment.

Once these sections are completed, the applicant must also submit biometric data. All of this information falls within the scope of personal data. As such, personal electoral data clearly falls under the PDPA and must be handled in accordance with its requirements and restrictions.

4. Establishment of the Personal Data Protection Commission and its Powers

The PDPC is established under section 6 of the PDPA. The official inauguration of the PDPC took place on 3 April 2024. The inauguration triggered a suite of data protection related compliance obligations under the PDPA, and the publication of twin Data Protection Regulations, as well as the requirement for data controllers and data processors to register with the PDPC. This also triggered the implementation of data protection policies covering various aspects such as the purpose for which personal data is collected, processed, shared, transferred and retained by an organisation.

The functions of the PDPC include to: (a) monitor compliance by data controllers and data processors; (b) register data controllers and data processors; (c) receive, investigate and deal with complaints about alleged violations of the protection of personal data and privacy of persons; (d) inquire into and take measures against any matter, that appears to the PDPC to affect the protection of personal data and infringe privacy of the individuals; (e) educate the public as may be appropriate; (f) undertake research and to monitor technological developments in data processing; (g) establish mechanisms of cooperation with other data protection authorities from other countries, and (h) advise the Government on matters relating to data personal protection, as listed under section 7 of the PDPA.

A critical function of the PDPC, which is subject of this article, is its role in approving cross-border data transfer. This article covers the procedures for cross-border data transfer pursuant to the PDPA, including the requirement for PDPC's approval.

5. Framework for Cross-Border Data Transfer

The PDPA uses the term “transborder flow” of data to refer to any international cross-border movement of personal data, whether by electronic transmission or other means.¹⁶⁰ However, for purposes of this article the phrase “cross-border data transfer,” is used as it is more familiar. Despite the difference in terminology, the meaning remains the same.

Literature defines cross-border data transfer to mean movement or transfer of data between servers across the borders of countries, i.e., from within the boundaries of one geographic unit to another, via networking equipment that enables such transmission.¹⁶¹ Data flows across borders when individuals, firms or governments authorise data to be transferred from one country (the source of the data) to another country where the data may be processed or used in other ways.¹⁶²

In the past, cross-border data transfer often occurred when there was an explicit intent to transfer data internationally (this is to say, when a computer file was deliberately sent to a specific location in another country). Nowadays, the architecture of the internet means that even a transfer to a party in the same country may result in message or file transiting via other countries, without the transferor ever being aware of this.¹⁶³

5.1. Cross-Border Electoral Data Transfer Approval: Tanzania

To the extent that certain personal electoral data needs to be transferred outside Tanzania, the transferor will need to obtain a permit from the PDPC, as per Regulation 20 of the Personal Data Protection (Personal Data Collection and Processing) Regulations of 2023. Personal data can only be transferred outside Tanzania electronically or physically if the PDPC has granted an approval.

¹⁶⁰ Section 3 of the PDPA.

¹⁶¹ Beyleveld, A. & Sucker, F. (2023). *Cross-border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital trade*. SSRN. <https://ssrn.com/abstract=4278748>. Sucker, F. & Beyleveld, A., “Cross-border Data Flows in Africa: Policy Considerations for the AfCFTA Digital Trade Protocol,” available at <https://dx.doi.org/10.2139/ssrn.4278748> (accessed 25 September 2025).

¹⁶² *Ibid.*

¹⁶³ Kuner, C., “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future,” OECD Digital Economy Papers No. 187, available at https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/12/regulation-of-transborder-data-flows-under-data-protection-and-privacy-law_g17a2074/5kg0s2fk315f-en.pdf (accessed 25 March 2026).

The PDPA and the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023, provide for the following conditions which a transferor must satisfy for the PDPC to grant approval:

- (a) presence of appropriate safeguards to ensure that the data subject's legitimate interests are not prejudiced;
- (b) existence of a legitimate purpose and the necessity to transfer the personal data;
- (c) the data subject has consented to the transfer of their personal data;
- (d) the transferor proving that the country receiving the personal data has ratified an international agreement providing requirements for the protection of personal data;
- (e) there is an agreement between Tanzania and the country receiving personal data regarding the protection of personal data; or
- (f) there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside Tanzania.

Section 31(1) of the PDPA empowers the PDPC to prohibit the transfer of personal data to any place outside Tanzania. Under this section, the PDPC may reject an application for approval of a cross-border transfer of personal data for reasons including when: (a) the transfer of personal data endangers national security; (b) the PDPC is satisfied that there is no adequate protection of personal data in the recipient country; (c) the transfer of personal data is restricted by other written laws; and (d) other reasonable grounds that the PDPC may deem necessary in the public interest.¹⁶⁴

Independence of the PDPC is crucial to ensure that it is not unduly influenced or politically motivated to prohibit the transfer of personal electoral data outside Tanzania under the guise of national security or other reasons labeled as “public interest.” According to the Collaboration on International ICT Policy for East and Southern Africa (“CIPESA”), most autocratic governments are reluctant to be more open to cross-border data transfers. The reluctance is based on unfounded fears that sending their citizens' data abroad could increase vulnerability to serious security and privacy threats from foreign actors.¹⁶⁵ A concern that is valid and which may be misused in this context. With the framing of the PDPA, this may indeed be the case where the transfer of personal

¹⁶⁴ The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

¹⁶⁵ Collaboration on International ICT Policy for East and Southern Africa, “Advancing Sustainable Cross-Border Data Transfer Policies and Practices in Africa”, 2024, available at: <https://cipesa.org/2024/04/advancing-sustainable-cross-border-data-transfer-policies-and-practices-in-africa/> (accessed 20 September 2025).

electoral data is involved, and in situations where the PDPC becomes influenced. This remains a wait-and-see scenario.

Furthermore, the PDPA appears to be drafted in a way that limits public scrutiny of PDPC's decisions. A review of the PDPA and the twin Data Protection Regulations reveals that PDPC is not obligated to publish the reasons for its decisions. As a result, any decision to disapprove the transfer of personal electoral data remains known only to PDPC and the applicants.

5.2. Statistics of the Cross-Border Data Transfer Approvals

The Budget Speech delivered by the Minister of Communication and Information Technology to the National Assembly on 16 May 2025 for the 2025/2026 fiscal year, indicates that the PDPC had received 12 applications for cross-border data transfer. The speech further explains that only 5 out of the 12 applications were approved after complying with all cross-border data transfer requirements.

Other than this general statement, there has been no further breakdown of the specific reasons why the remaining 7 applications for approval were not granted. The most probable reason for non-disclosure of the grounds for rejecting cross-border data transfers is that the law does not require PDPC to publish the reasons for its decisions.

The non-disclosure of these reasons underscores the difficulty highlighted in this article. The public cannot understand the basis for refusal unless such information is obtained directly from the affected applicants. This lack of transparency limits public scrutiny and accountability when certain motives are framed to appear consistent with legally valid grounds for blocking the intended transfer of personal electoral data.

5.3. Cross-Border Data Transfer Approval: Other Countries

5.3.1. Uganda

Unlike the position in Tanzania where the approval or permit for the cross-border data transfer is required, in Uganda the position is different. In Uganda, cross-border data transfer is not subject to the approval from the Ugandan Personal Data Protection Office ("PDPO"). This position is reinforced by the recent decision delivered by the PDPO on 18 July 2025 in Complaint No. 08/11/24/6683, between *Ssekamwa Frank, Leni Sharon Pamela, Amumpaire Raymond, and Awino Mercy* ("Complainants") v. *Google LLC* ("Google").

By way of background, on 8 November 2024, the PDPO received a complaint filed by the Complainants against Google, alleging that Google violated Uganda’s Data Protection and Privacy Act, and the Data Protection and Privacy Regulations (the “Ugandan Data Protection Laws”). In particular, the Complainants asserted mainly that:

- (a) Google, as a data collector, controller, and processor failed to register with PDPO as required under the Ugandan Data Protection Laws; and
- (b) Google unlawfully transferred the Complainants personal data outside Uganda without meeting the legal conditions enshrined in the law, (including failure to acquire prior approval of the PDPO for the transfer outside Uganda) contrary to the Ugandan Data Protection Laws.

The PDPO framed five issues for determination. Among these, the only issue worth mentioning in connection with this article is “whether Google transferred the Complainants’ personal data to jurisdictions outside Uganda without obtaining prior approval from the PDPO, amounts to a violation of the Ugandan Data Protection Laws.”

In substantiation, the Complainants submitted that Google, while not registered with the PDPO, collects, processes and transfers the personal data of Ugandan citizens to jurisdiction outside Uganda without obtaining the required prior approval from the PDPO. They contended that this conduct contravenes various provisions of the Ugandan Data Protection Laws. In response, Google refuted breaching any statutory provisions as there is no requirement to seek prior approval from the PDPO for its international data transfers.

Determining on this issue, the PDPO made it clear that the Ugandan Data Protection Laws does not require a data controller or processor to seek advance permission before each cross-border transfer or storage of personal data. Rather, the PDPO expects that the entity maintains proper records and accountability of the legal basis, safeguards, and justification for such transfers. These records must be available for inspection during audits, compliance checks, or investigations.

At the end, the PDPO dismissed the Complainants’ position regarding the requirement for prior approval for the cross-border transfer of data relating to Ugandan individuals. However, it found Google to be in breach because it failed to provide adequate records of international data transfers or evidence demonstrating compliance.

5.3.2. *Kenya*

The Kenyan Data Protection Act, 2019 (KDPA) allows a data controller or data processor to transfer personal data to another country only where certain conditions are satisfied. These include situations where the data controller or data processor has demonstrated to the Data Commissioner that appropriate safeguards are in place to ensure the security and protection of the personal data, including where the recipient jurisdiction has data protection laws that provide a comparable level of protection. A cross-border transfer may also be permitted where it is necessary for the performance of a contract between the data subject and the data controller or data processor, or for the implementation of pre-contractual measures taken at the request of the data subject, as well as for the conclusion or performance of a contract entered into in the interest of the data subject between the controller and a third party. Further, such transfers may be justified on grounds of public interest, for the establishment, exercise, or defense of legal claims, to protect the vital interests of the data subject or other persons where the data subject is physically or legally incapable of giving consent, or for purposes relating to compelling legitimate interests pursued by the data controller or data processor, provided that such interests are not overridden by the rights, freedoms, or interests of the data subjects.

The processing of sensitive personal data outside Kenya is conditional upon obtaining consent of a data subject and confirmation of appropriate safeguards of such data in the respective country. The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of security safeguards in that country or the existence of compelling legitimate interests. In relation to this, the Data Commissioner is given discretionary power to prohibit, suspend or subject the transfer to such conditions as may be determined. According to the KDPA, the Data Commissioner can only invoke its power to prohibit, suspend, or conditionally approve the transfer to protect the rights and fundamental freedoms of data subjects.

While both the PDPA and the KDPA grant their respective data protection authorities the mandate to prohibit data transfers beyond their respective countries, a comparison of the two legislations reveals that the KDPA is more explicit regarding the grounds on which a cross-border data transfer may be prohibited. According to section 49(3) of the KDPA, the basis for prohibiting data transfer is the protection of the rights and fundamental freedoms of the data subjects concerned. Unlike PDPA, the KDPA guides the Data Commissioner towards prioritising interests of the data subjects. This conclusion raises an important question. Is the PDPC truly independent? The article examines this issue below.

6. Independence of Data Protection Authorities (DPAs)

6.1. Regulatory Independence

Professor Mark J. Mwandosya, renowned for his role in establishing several key regulatory authorities in Tanzania such as Tanzania Communications Regulatory Authority has made significant contributions to the country's regulatory landscape. In his book "Regulatory Challenges in Africa: An Empirical Analysis" he emphasizes the importance of ensuring that regulatory authorities remain independent. His reasoning is relevant and applies to the PDPC, the regulatory authority for all matters relating to protection of personal data in Tanzania.

According to Professor Mwandosya, independence is the most important pillar, which enables the regulator to perform her duties effectively. He points out that before the restructuring of the economy and adoption of the policy on regulation of public utilities, sector Ministers in Tanzania were essentially the regulators. As a result, the regulatory mandate was used to further political rather than national interests.

To ensure that regulatory authorities are able to exercise their legal duties with full autonomy and without fear or favour, corresponding laws establishing regulatory authorities are deliberately crafted to safeguard their institutional independence. The legal architecture is intended to insulate regulatory authorities from political or commercial pressure. This enables them to perform their statutory functions objectively, transparently, and in the public interest. The language used is typically self-explanatory as demonstrated below:

*'The Minister may from time to time as the occasion necessitates, give to the Authority direction of specific or general character on specific issues, other than in relation to the discharge of the regulatory functions arising in relation to any sector, for the purposes of securing effective performance by the authority of its policy, functions and compliance with the code of conduct.'*¹⁶⁶

6.2. Independence of Data Protection Authorities

Based on the nature and sensitivity of the enormous tasks that DPAs, including the PDPC perform, they are required to be completely independent. Independence is considered crucial for the

¹⁶⁶ Mwandosya, M., *Regulatory challenges in Africa: An empirical analysis*, Dar es Salaam: Mkuki na Nyota, 2021, pp. 21-2.

effectiveness of the DPA as the nature of its functions sometimes requires it to stand up against the power of private entities and the government.¹⁶⁷

Lukman views that in determining the extent of independence, the first place to look to is the statutes establishing the DPAs, which are the data protection laws of a country. Since international standards are now tilting towards detailed provisions, one can safely assume that the more detailed a statutory provision on independence, the better for independence.¹⁶⁸ According to him, the attributes of independence can be broadly categorised into four groups. These are the attributes that relate to functions and powers; the mode of appointment, tenure, and qualifications of office holders; adequate resources; and accountability. The attributes that relate to the functions and powers of DPAs include a stipulation that the DPA must be established by legislation; freedom to exercise its powers without interference; and immunity from lawsuits.¹⁶⁹

The second category concerns the mode of appointment and tenure. These include provisions on the mode of appointment, terms of office, mode of removal, and qualifications. The third category consists of attributes relating to sufficient resources. In this regard, there are specifications that protect DPAs from any form of control in terms of resources (financial or personnel), which invariably means that they must have adequate resources. Finally, accountability provisions enable the powers of DPAs to be kept in check. These include provisions subjecting their finances to budgetary control and the right of appeal to the courts against their decisions.¹⁷⁰

The statutory approach of African countries regarding the nature and scope of provisions on the independence of DPAs is categorised into four groups: minimalist, moderate, robust, and extreme. The last category represents the extreme end of the spectrum.¹⁷¹ Robust category are countries with data privacy frameworks that provide for most of the international data privacy standards on independence contained in the General Data Protection Regulation 2016/679. The minimalist countries merely provide for independence without elaboration of its basic attribute. The moderate

¹⁶⁷ Abdulrauf, L.A “Independence of Data Protection Authorities in Africa: Trends and Challenges”, in Abdulrauf, L.A and Dube, H. (eds.) *Data Privacy Law in Africa: Emerging Perspectives*, Pretoria: Pretoria University Law Press, 2024, pp. 355-6.

¹⁶⁸ Abdulrauf, L.A “Independence of Data Protection Authorities in Africa: Trends and Challenges”, in Abdulrauf, L.A and Dube, H. (eds.) *Data Privacy Law in Africa: Emerging Perspectives*, Pretoria: Pretoria University Law Press, 2024, pp. 355-6.

¹⁶⁹ *Id.*, p.362.

¹⁷⁰ *Ibid.*

¹⁷¹ *Ibid.*, pp.366 – 7.

falls in between both. At the extreme end are countries that do not provide for independence at all or do not have a separate supervisory body for data protection.¹⁷²

As per Lukman's assessment, South Africa has the most elaborate incorporation of the international principles on independence, with Kenya grouped into a moderate category in its treatment of independence under the KDPA.¹⁷³ Ghana, which closely mirrors the position of Tanzania, is categorised as a minimalist group regarding the substance and detail on the independence of its DPA. In the extreme category is Uganda, which arguably does not make any provision for the independence of its DPA.¹⁷⁴ However, in relation to Uganda, Lukman's assessment may not be fair, because, as discussed below, Ugandan law clearly provides that, in performing its functions, the PDPO shall not be under the direction or control of any person or authority.

It should be clear that the independence of the PDPC and other DPAs is examined solely from a legal perspective, as opposed to both legal and practical points of view. The assessment is based on what the statutory provisions state, and not on how they are or would be implemented in practice. The assessment is also a limited legal assessment of the independence of the PDPC and other DPAs, because not all relevant provisions will be analysed.

6.3. Independence of the Personal Data Protection Commission of Tanzania

It is unfortunate that neither the PDPA nor its twin Data Protection Regulations contain detailed provisions on the independence of the PDPC. The only provision addressing the impartiality of the PDPC is section 8(4) of the PDPA, which states that, in order to maintain impartiality and avoid conflicts of interest, a person shall not qualify for appointment as a board member of the PDPC if, by virtue of the office they hold, they are likely to exert influence on the PDPC.

This provision merely prohibits the appointment of individuals who could internally influence the PDPC's decisions. However, the PDPA does not consider or address scenarios where the PDPC's decisions may be subject to external influence. It completely fails to account for external pressure and significantly downplays the risk of external interference in the PDPC's decision-making, including potential influence from appointing authorities and the relevant ministry under which it

¹⁷² Abdulrauf, L.A. "Independence of Data Protection Authorities in Africa: Trends and Challenges", in Abdulrauf, L.A and Dube, H. (eds.) *Data Privacy Law in Africa: Emerging Perspectives*, Pretoria: Pretoria University Law Press, 2024, p.367.

¹⁷³ *Ibid*, p.369.

¹⁷⁴ *Ibid*, p.371.

operates. in cases involving the transfer of personal electoral data that may not please, or may appear to threaten, the appointing authority.

The PDPA states that the PDPC is a body corporate with perpetual succession and a common seal and, shall in its own name be capable of: (a) acquiring and holding movable and immovable property, to dispose of property and to enter into any contract or other transaction; (b) suing and being sued; and (c) performing any other acts which a body corporate may lawfully perform, for the proper performance of its functions. The PDPC is headed by the Director General who is a Presidential appointee. A person may be appointed as Director General if he or she holds at least a bachelor's degree from a recognised university in the fields of ICT, engineering, law, economics, finance, or administration; has a minimum of ten years' experience in any of these fields; and possesses the requisite knowledge and expertise in personal data protection.

The tenure of the Director General is five years and may be reappointed for one further term. Officers and employees of the PDPC are appointed, in such number as may be necessary for the effective discharge of the functions of the PDPC, pursuant to the laws governing the public service. The PDPC is empowered to appoint consultants and experts in various disciplines on such terms and conditions as it may determine.

The provisions of the PDPA that raise questions about the independence of the PDPC have not gone unchallenged. In *Tito Magoti v. The Honourable Attorney General*, Miscellaneous Civil Cause No. 18 of 2023 (Tito's Case)¹⁷⁵, the independence of the PDPC was brought into question before the High Court of Tanzania, as explained in the section below.

In this case, Advocate Magoti challenged the constitutionality of several provisions of the PDPA. These include sections 8(1)(2)(3), 11(1), 14(5), 19, 20, 22(3), 23(3)(c)(d)(e), 25(2)(e)(f), 26, 30, 31(2), 33(2), and 34. This article does not intend to analyze the entire set of provisions that Advocate Magoti challenged. The focus is solely on those grounds that question the autonomy of the PDPC. For that reason, the relevant provisions for consideration are sections 8(1)(2)(3) and 11(1). Advocate Magoti argued that the provisions of section 8(1)(2)(3), which grant the President of Tanzania the power to appoint the Chairman and Vice Chairman of the PDPC Board without any prescribed qualifications, procedures, or conditions for such appointments, contravene Articles 12(2), 13(1)(2)(6)(a), 16(1), 21(2), and 29(1) of the Constitution of Tanzania, and are therefore, unconstitutional. He also challenged all provisions empowering the Minister of Communication and Information Technology to appoint Board Members of the PDPC, arguing that the absence of

¹⁷⁵ The judgment of this case was delivered on 8 May 2024.

clear procedures for these appointments allows for arbitrary decision-making and undermines the principle of equality before the law.

The basis of this argument is that the lack of statutory procedures, qualifications, and conditions for appointing the Chairman, Vice Chairman, Board Members, and Director General exposes these appointments to potential bias or partiality, ultimately undermining the independence and authority of the PDPC. As expected, the Attorney General discredited the arguments advanced by advocate Magoti. In the Attorney General's view, the appointment procedures for the PDPC's top leaders are unique and do not follow traditional recruitment processes. The High Court agreed with the Attorney General's arguments, refuting advocate Magoti's grounds, and held that appointments by the President do not follow a standard recruitment process open to all citizens because such appointments are unlike typical employment opportunities.

Several issues keep the High Court's decision open to debate. For example, the link between presidential appointments and the impartiality of decisions, especially where those decisions may involve protecting the interests of the appointing authority, was not clearly addressed by the High Court, making it difficult to understand its final position on these concerns. While this article does not intend to dwell on that point, the potential for influence or external pressure on the PDPC's decisions should be examined beyond the appointment stage.

Reading the entire PDPA and the twin Data Protection Regulations, one will not find any provision stating that the PDPC is independent. It is unclear whether this omission was intentional or was simply an overlook. To understand how other countries have framed provisions related to the independence of their DPAs, data protection legislations from four African countries were reviewed, as outlined hereinafter.

6.4. Independence of DPAs: Comparative Overview

Noting that there may be some practical variations in implementation, the independence of DPAs in the countries mentioned here is assessed solely on the basis of what their establishing legislation provides, rather than on what is happening in practice. The assessment is limited to selected provisions that directly state that the relevant DPA is independent or that contain related provisions which, by their nature, suggest that the independence of the DPA is addressed in the law.

6.4.1. Kenya

The data protection authority in Kenya is called the Office of the Data Protection Commissioner ("ODPC"). It is established under section 5 of the KDPA as a body corporate and a state office with

perpetual succession and a common seal. In its corporate name, it is capable of: (a) suing and being sued; (b) taking, purchasing, or otherwise acquiring, holding, charging, or disposing of movable and immovable property; (c) entering contracts; and (d) performing such other legal acts as may be necessary for the proper performance of its functions.

The KDPA is quite detailed in how appointments to various positions within the ODPC are made, including the interview procedures. The Data Commissioner, who heads the ODPC, is a Presidential appointee but is subject to approval by the National Assembly. This is unlike the position in Tanzania, where no procedures are set out in the law, and the appointment is made exclusively by the President.

An especially notable provision is section 8(3) of the KDPA, which clearly states that the Data Commissioner shall act independently in the exercise of powers and the performance of functions under the KDPA. No similar provision exists under the PDPA. In view of Lukman, Kenya belongs to the moderate category in the treatment of independence in the Data Protection Act 2019.

6.4.2. *Uganda*

The data protection authority, the PDPO is established under section 4(1) of the Data Protection and Privacy Act, 2019 (“DPPA”), and is headed by a National Personal Data Protection Director. Section 5(3) of the DPPA sets it clear that in performing its functions as a data protection authority, the PDPO shall not be under the direction or control of any person or authority.

6.4.3. *Nigeria*

The Nigeria Data Protection Act, 2023 (“NDPA”), establishes the Nigeria Data Protection Commission (“NDPC”) as its data protection authority. The NDPC is a corporate body with perpetual succession and a common seal. As a corporate entity, the NDPC may sue and be sued in its corporate name and may acquire, hold, and dispose of property. The independence of the NDPC is guaranteed under section 7 of the NDPA, which provides that the NDPC shall be independent in the performance of its functions.

6.4.4. *South Africa*

The South African data protection authority is the Information Regulator (“IR”). According to section 39 of the Protection of Personal Information Act, 2013, the IR has jurisdiction throughout South Africa, is independent, and is subject only to the Constitution of South Africa and the law. It is impartial and performs its functions and exercises its powers without fear, favour, or prejudice, and is accountable to the National Assembly.

6.4.5. Assessment

A review of other countries' legislation on the independence of their DPAs reveals that countries such as South Africa have deliberately framed their data protection laws to explicitly affirm the independence of these authorities. This approach leaves no room for assumptions or speculation about their autonomy. By embedding independence as a statutory principle, these jurisdictions signal a strong commitment to impartiality and regulatory integrity.

Even though actual practice may sometimes divert from what the law prescribes, the presence of clear and specific provisions in enabling legislation serves an important purpose. This is also supported by Lukman whose assessment is that South Africa has the most elaborate incorporation of the international principles on independence.¹⁷⁶

The IR establishes a legal benchmark against which compliance can be measured and provides a foundation for accountability. Moreover, such provisions enhance public trust in the regulatory framework by demonstrating that independence is not merely aspirational but a legal requirement. In contrast, the absence of explicit guarantees of autonomy can create ambiguity, leaving space for undue influence and undermining confidence in the regulator's impartiality.

6.5. Implications of the Current Legal Position

If the PDPC is not independent, it may jeopardize its function as an authority that protects the interests of data subjects and instead become a tool for advancing or protecting certain partisan agendas. Every effort must be made to ensure that DPAs are not used as instruments of state or economic control. Without proper safeguards, states may manipulate these authorities to serve their own interests rather than those of the individuals whose personal data is subject to protection.

In the context of electoral data, transparency is a key requirement for genuine, competitive, and democratic elections. It forms the foundation of public confidence in the electoral process. The goal of transparency in elections is to enhance electoral integrity and accountability.

¹⁷⁶ Abdulrauf, L.A. "Independence of Data Protection Authorities in Africa: Trends and Challenges", in Abdulrauf, L.A and Dube, H. (eds.) *Data Privacy Law in Africa: Emerging Perspectives*, Pretoria: Pretoria University Law Press, 2024, p. 367.

7. Conclusion and Recommendations

The analysis undertaken in this article demonstrates that the current legal framework governing cross-border transfers of personal electoral data in Tanzania presents genuine risks of politicisation. These risks stem not from the substantive standards set out in the PDPA themselves, but from the absence of express statutory guarantees of institutional independence for the PDPC. Given the central role of the PDPC in approving or prohibiting cross-border transfers of personal data, including sensitive electoral data, this gap in the legislative architecture is significant.

As shown, the PDPC is vested with wide discretionary powers, including the authority to deny cross-border transfers on broad and loosely defined grounds such as national security or public interest. In a context where the PDPC lacks explicit legal insulation from political or executive influence, these discretionary powers may be susceptible to use in a manner that undermines transparency, accountability, and, ultimately, the integrity of the electoral process. The risk is particularly acute where decisions relate to personal electoral data, the handling of which has direct implications for electoral credibility and democratic participation.

Comparative analysis underscores this concern. Other African jurisdictions examined in this article, including Kenya, South Africa, Nigeria, and Uganda, have all adopted legislative approaches that, to varying degrees, expressly recognise the independence of their data protection authorities. While statutory guarantees do not, on their own, eliminate the possibility of improper influence, they nevertheless establish a clear legal benchmark, against which both conduct and accountability can be measured. Tanzania's PDPA, by contrast, remains silent on this point, creating avoidable ambiguity and weakening confidence in regulatory neutrality.

Against this backdrop, this article recommends targeted legislative reform. First, the PDPA should be amended to expressly affirm the institutional independence of the PDPC in the performance of its functions, particularly in relation to cross-border data transfer approvals. At a minimum, the law should clarify that the PDPC shall exercise its powers free from direction or control by any person or authority, except as provided by law. Such a provision would align Tanzania's framework with regional and international best practice and reinforce the credibility of the PDPC as an impartial regulator.

Second, the PDPA should be amended to require the PDPC to provide written reasons for decisions approving or refusing cross-border transfers of personal data. Subject to appropriate confidentiality safeguards, these reasons should be made publicly accessible, for example through publication in the Government Gazette or another official medium. Transparency in decision-making is essential

to meaningful accountability, particularly where refusals may have significant public interest implications, as is the case with personal electoral data.

Finally, greater procedural clarity should be introduced around the criteria used by the PDPC when invoking grounds such as national security or public interest to deny cross-border transfers. Narrowing and clarifying these grounds would reduce the scope for arbitrary decision-making and help ensure that restrictions on data transfers are proportionate, justified, and consistent with the underlying purpose of data protection laws.

Strengthening the PDPA in these respects would not only enhance the protection of personal data but would also contribute to safeguarding electoral transparency and democratic legitimacy. In an era where data governance and democratic processes are increasingly intertwined, ensuring the independence and accountability of data protection authorities is no longer optional; it is essential.



Voters' Right to Access Cross-Border Personal Electoral Data in Kenya

Timothy Samson Ayuo*

Abstract

Electoral transparency and democratic accountability are inseparable from lawful and accountable processing of voters' personal data in line with the Data Protection Act, 2019. In a situation where personal data protection is secondary to electoral technology contracts, and for commercial and intellectual property interests of foreign technology vendors undermine this foundation. Drawing on Kenya's 2017 and 2022 general elections, this paper demonstrates how election technology providers processed and stored personal voter data, including biometric identifiers, on offshore servers with restricted supervised access in forgetfulness of data sovereignty. Consequently, this undermines voter's autonomy, rights, and the security and trust in cross-border data transfer regulations. The paper used is doctrinal approach to analyse electoral contracts, judicial interventions, and the evolving Kenyan data protection framework, including the Data Protection Regulations and sector-specific guidance on electoral and biometric data. In the end, several recommendations are drawn, including the need for a robust compliance framework placing clear obligations on the Independent Electoral and Boundaries Commission, as Data Controller, to ensure that all third-party processors comply with Kenyan data protection law before any cross-border data transfer occurs. It further calls for mandatory involvement of the Data Protection Commissioner in authorizing such transfers, and insists that no transfer should diminish the level of protection guaranteed under Kenyan law. Adequacy protection is the yardstick. In recommendations, the paper advocate reforms aimed at doing a risk assessment, restoring digital sovereignty,

* Timothy Samson Ayuo is a Research Assistant to the V.C. at Moi University and a Data Privacy Expert-Africa with PrivacyPulse Consulting Inc. He holds an LL. B from Moi University (Kenya), a Postgraduate Diploma in Legal Practice from ILPD (Rwanda); M.A. Governance & Ethics (candidate) and an ECPC-B DPO certified Data Protection Officer. Worked as a DPO handling healthcare data, fintech and academic data. He has also tutored at JKUAT University and Mount Kenya University. Currently involved in data privacy consultancy, research and has published in the Rwanda Law Journal, SSRN and Strathmore JIPIT Journal and contributed legal articles to the Daily Nation newspaper. He can be contacted via email at: timothyayuo@gmail.com

strengthening electoral integrity, and affirming the primacy of voters' rights to privacy and data protection.

1. Introduction

Transparency is a key pillar in the integrity of elections. In tandem with the Data Protection Act 2019, voters have a right to know who is processing their data and for what purpose. Public expectations are evolving; voters value ethical data use and demand accountability from any custodian of their personal data. The Kenyan electoral law was amended to explicitly include biometrics (definition)¹⁷⁷, biometric voter registration, biometric voter verification and biometric voter identification. Unrestrained use of voters' personal data is waning. Kenyan voters value their electoral data and there is a rich background to that. Justice Johan Kriegler-Chair of *the Commission of Investigation into the Post Election Violence in Kenya between 2007-2008* made a report loosely dubbed the '*Kriegler Report*' that recommended that Kenya puts in place an *effective, transparent and efficient* electoral system to ensure that the elections are credible, free and fair. *The Kriegler Report* justified limited, phased electoral automation (not electronic voting *per se*) as a response to administrative failures in the 2007 elections, while conditioning its legitimacy on transparency, verifiability, and institutional control principles that later underpin data protection and electoral technology governance. It endorsed electronic voter registration and results management as accountability tools, not blanket electronic voting, and only within a framework of strong safeguards and oversight.

The gap between *the Kriegler Report (2008)* and *Kenya's Data Protection Act, 2019* provides the historical foundation upon which contemporary data protection concerns arise. The *Kriegler Report* documented systemic failures in electoral administration, including opaque voter registration processes, weak institutional accountability, and limited public trust in electoral technologies. While it did not address data protection explicitly, it identified structural deficits in transparency and oversight that later became technologically mediated through digitised voter registers and biometric systems. As

¹⁷⁷ Sect.2 of the Election Laws Amendment Act of 2016 defines biometrics as unique identifiers and attributes.

Kenya transitioned from largely manual elections to technology-driven processes, these same accountability deficits migrated into the digital domain. By 2017 and 2022, voter registration, verification, and transmission of results depended heavily on personal and biometric data processed by private vendors. The Data Protection Act, 2019 responds to this evolution by legally articulating safeguards such as lawfulness, transparency, accountability, and adequacy that were absent in 2008, but directly address the risks foreshadowed by the *Kriegler Report*.

The linkage, therefore, is evolutionary rather than chronological. The *Kriegler Report* diagnosed democratic harms caused by opaque electoral systems; the Data Protection Act, 2019 provides the legal tools to prevent those harms from re-emerging in digital form. In this sense, data protection law operationalises the Report's call for credible, transparent, and accountable elections by imposing enforceable obligations on how voter data is collected, processed, stored, and transferred. The report thus functions as a normative baseline, while the 2019 framework supplies the contemporary legal mechanisms to address the same underlying governance failures in a data-driven electoral environment.

In Kenya, Parliament debates have recurrently featured petitions by members of the Legislative Assembly in the exercise of their constitutional mandates of accountability and oversight functions regarding the prospect of “*opening the servers*,” a phrase commonly understood to denote access to electronically stored electoral data, including data allegedly hosted on servers located outside the country. Simply put, the allegations are referred to electoral data stored in servers abroad as a dossier of electoral malpractice. Digital technologies for elections were introduced in Kenya with a vision that they would bring election reforms through increasing administrative efficiency, reducing long-term costs, and by enhancing transparency in the electoral process which would enhance citizenry inclusivity.¹⁷⁸ However, as argued by Omwoha that there has been a paradox in the use of technology in elections in Kenya.¹⁷⁹ The paradox is a manifestation of the fact that digitization did not only subvert the democratic intentions for elections in Kenya but also

¹⁷⁸ Omwoha, J. (2022). ‘Open the Servers.’ *Africa Development / Afrique et Développement*, 47(2 special issue), 147–160. <https://www.jstor.org/stable/48682669>

¹⁷⁹ Omwoha, J. (2022). ‘Open the Servers.’ *Africa Development / Afrique et Développement*, 47(2 special issue), 147–160. <https://www.jstor.org/stable/48682669>

failed the test of verifiability and transparency. According to *Omwoha*, since 2013, the voting exercise has never taken place ‘without a hitch’. For example, in 2017, the opposition party dismissed the general elections as a ‘fraud’, leading to the nullification of results by the Supreme Court. In general, the digital system of elections has not only failed but has also disappointed the citizens as the results get repeatedly ‘dismissed’ by different stakeholders calling on the elections body “to open the servers”. In *Raila Amolo Odinga & another v Independent Electoral and Boundaries Commission & 7 others*¹⁸⁰ the Supreme Court held that the credibility of a technology-driven election depends on verifiability and full access to electoral systems by the Court and parties.

At paragraphs 82–83, the Court made the finding that IEBC failed in its duty of transparency by declining to grant meaningful access to its ICT infrastructure. The Court stated, verbatim:

“The IEBC was not forthcoming in disclosing information when it was required to do so. It failed to open its servers for scrutiny, despite the Court’s orders. This refusal cast serious doubt on the integrity of the electoral process.”

The Court further observed:

“Where technology is deployed in an election, the system must be simple, accurate, verifiable, secure, accountable and transparent.”

On the issue of servers, the Court’s reasoning while partly obiter was unequivocal. It rejected IEBC’s argument that opening servers would compromise security or intellectual property, holding instead that once technology is adopted for a constitutional process, it must submit to judicial scrutiny. The refusal to grant access shifted the evidentiary balance against the Commission and undermined public confidence in the results.

In summary, the Court did not merely request access to servers as a procedural matter; it treated the failure to open servers as a substantive breach of transparency and

¹⁸⁰ [2017] KESC 6 (KLR).

accountability, reinforcing that electoral technology cannot operate beyond the reach of constitutional oversight.

However, a major question that lingers is, where do we process our election data as a country? Is the transfer safe? The Data Protection Act, 2019 which now establishes *adequacy* requirements gives data subjects control on how their personal data is processed.¹⁸¹ Independent Electoral and Boundaries Commission is under the spotlight to comply with the framework on cross-border transfer of electoral data. Personal data shall not be transferred outside Kenya unless there is proof of adequate data protection safeguards or consent from the data subject. The Data Protection Act has both *territorial and extraterritorial* scope of application when it comes to transfer of Kenyans' personal data outside the country. In Kenya, we ought to implement a "restricted" transfer if personal data is to be transferred to a third country or organization; putting very stringent measures on this procedure. Electoral data has voters' biometrics thus sensitive personal data;¹⁸² it requires stringent data protection measures.

IEBC forms 34As that are all over the portal expose phone numbers, IDs/ passport numbers and full names of Agents and officials in blatant breach of privacy laws.¹⁸³ However, no formal complaints have reached the ODPC's office. It is argued that towards achieving a lawful end such breaches are excused, but how useful is an Agent's phone number for public consumption? Does it outweigh the risks and dangers to their person? It is possible to have both privacy and security in a full functionality model. IEBC had an option of compelling Smartmatic company to conceal some digits in the phone contacts and ID/passport numbers by embracing *privacy by design* in the KIEMs kits. Privacy embedded into the design and architecture of their information technology systems. Privacy by design under section 41 of the DPA, 2019 practised as a technical measure by IEBC can cure some cross-border challenges it faces every electoral cycle.

¹⁸¹ Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR

¹⁸² "Sensitive Personal Data" means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

¹⁸³ <https://nation.africa/kenya/blogs-opinion/blogs/electoral-agency-has-a-duty-to-protect-kenyans-personal-data-3927726>

2. Legal Framework for Technology Integration in Elections

*The Constitution*¹⁸⁴ sets out the constitutional principles that govern election processes. Articles 81 and 86 of the Constitution of Kenya do not mention “data protection” expressly, but impose substantive, justiciable obligations that translate directly into data protection duties once elections are digitised. Their force lies not in abstraction, but in how they regulate *process integrity* in a data dependent electoral system.

Article 81(e) is succinct on qualitative standards for elections: freedom, fairness, transparency, accuracy, verifiability, security, and accountability. In a biometric and ICT-driven election, each of these standards is operationalised through personal data. On the one hand, accuracy and verifiability depend on the integrity of voter registers and biometric identifiers, on the other hand, security requires protection against unauthorised access, manipulation, or exfiltration of voter data. Furthermore, accountability presupposes traceability of data processing decisions across the electoral lifecycle. Once voter identity and results are mediated through databases and servers, failures in data governance become constitutional failures, not merely technical lapses. Article 81(e), therefore, converts data integrity and confidentiality into constitutional imperatives.

Article 86 it imposes procedural obligations on the IEBC. The duty to ensure that voting methods are “simple, accurate, verifiable, secure, accountable and transparent”. It demands demonstrable control over data flows, storage locations, and access rights. The obligation to “safeguard the election materials” extends, in a digital election, to safeguarding databases, servers, and transmission systems containing personal and biometric data. Moreover, the requirement for “prompt” and “accurate” collation and transmission of results presupposes lawful, controlled processing and retention of electoral data, capable of audit and judicial scrutiny.

In a digital electoral environment where biometric registration, electronic transmission of results, and cloud storage are common, voters’ personal electoral data often moves beyond national borders. The Data Protection Act, 2019 ensures that such cross-border transfers are subject to adequate safeguards and legal protections. By protecting voter information,

¹⁸⁴ Articles 81 and 86.

the Act reinforces ballot secrecy, promotes transparency, and strengthens public confidence in elections. In essence, data protection is not separate from electoral integrity; it is a constitutional mechanism that actualizes Articles 81 and Article 86 in practice.

The Elections Act, 2011 permits the public to inspect the voters' register. The IEBC is thus under a duty to open the register for inspection within 90 days of the date of a general election, for the Public to inspect the register.¹⁸⁵ The period reserved for inspection cannot be less than 30 days.

By dint of section 6A (1) of the Elections Act, 2011 the same period of inspection applies to the biometric register. Voters are free to verify their biometric data at their polling station; following which the IEBC has to revise the Register taking into account such changes that may have been availed by voters.¹⁸⁶ This meaning data subject requests are rights that are to be responded to by the Data Controller / Processors.

The IEBC currently deploys technology systems in its administration of elections and referenda in seven ways. They are: a. Biometric Voter Registration (BVR) b. Electronic Voter Identification (EVI) c. Results Transmission System (RTS) d. Kenya Integrated Elections Management System (KIEMS) e. Candidates Registration System (CRS) 19 f. Online publication of the Register of Voters g. Publishing polling result forms of presidential elections in a public access online portal.

A case in point that highlighted I.E.B.C.'s deployment of technology in electoral data transmission: *Raila Amolo Odinga & 5 Others v Independent Electoral and Boundaries Commission & 4 Others* (Consolidated Petitions 3, 4 & 5 of 2013) [2013] KESC 6 (16 April 2013). The Apex Court took note of the scrutiny orders it had made directing the IEBC to avail the result declaration forms and allow the parties read-only access to its election technology systems. After finding that the I.E.B.C. had not complied with the Court orders and failed to discharge the shifted evidential burden of proof, the Court held:

"It is trite law that failure to comply with a lawful demand, leave alone a specific Court Order, leaves the Court with no option but to draw an adverse inference

¹⁸⁵ Section 6.

¹⁸⁶ *Ibid* note 28 at p.65.

against the party refusing to comply. In this case, I.E.B.C.'s continuous disobedience of this Court's Order of 28th August, 2017 in critical areas leaves us with no option but to accept the petitioners' claims that either I.E.B.C.'s IT system was infiltrated and compromised and the data therein interfered with or I.E.B.C.'s officials themselves interfered with the data or simply refused to accept that it had bungled the whole transmission system and were unable to verify the data."

These findings resulted in the Supreme Court of Kenya nullifying the presidential results, by majority. It should be noted that, the Supreme Court of Kenya agreed that the process of voter registration, voter identification, manual voting and vote counting had not been challenged; but only the process that followed (transmission, tallying and verification) had been credibly impugned. The Supreme Court of Kenya's decision, in *the Raila Odinga, 2017 case* cemented the place of result transmission in presidential elections.

Access to electoral data including personal data is a huge tenet of transparency in the election process. *The African Commission on Human and Peoples Rights has Guidelines on Access to Information and Elections in Africa* drafted by a Special Rapporteur in 2017.¹⁸⁷ *Resolution ACHPR/Res.307 (EXT.OS/XVIII) (2015)* and the *African Commission's Guidelines on Access to Information and Elections in Africa* are relevant to Kenyan jurisprudence not as binding law, but as authoritative interpretive standards that Kenyan courts increasingly rely on when construing constitutional rights in a digital and electoral context.

Resolution 307 is significant because it formally recognised that access to information is indispensable to democratic participation and electoral integrity in Africa. By mandating the Special Rapporteur on Freedom of Expression and Access to Information to develop normative guidance on elections, the Commission acknowledged that electoral credibility depends on transparency, disclosure, and accountability particularly where state institutions deploy complex administrative or technological systems. This framing directly

¹⁸⁷ Resolution ACHPR/Res.307 (EXT.OS/ XVIII) 2015. This Resolution requested the Special Rapporteur on Freedom of Expression and Access to Information in Africa

resonates with Kenya's constitutional architecture under Articles 35, 81, and 86, which courts have interpreted purposively rather than textually.

The *Guidelines on Access to Information and Elections in Africa* operationalise this resolution by articulating concrete state obligations during electoral cycles. They emphasise proactive disclosure by electoral management bodies, public access to information on voter registration, results management, and the use of technology, and the duty to prevent secrecy that undermines public confidence. Importantly, the Guidelines recognise that information asymmetries especially where technology vendors or state agencies control electoral data pose structural risks to free and fair elections.

In Kenyan jurisprudence, these instruments function as persuasive authority under Article 2(5) and (6) of the Constitution and have normative weight in constitutional interpretation. They reinforce judicial reasoning seen in cases such as *Raila Odinga v IEBC (2017)*, where the Supreme Court linked electoral transparency to access to information and system verifiability. In the data-driven electoral era, the Resolution and Guidelines also bridge access to information with data protection, supporting the view that transparency over electoral data processing is a prerequisite for accountability, not a threat to it.

For elections to be free, fair and credible, the electorate must have access to information at all stages of the electoral process. Without access to accurate, credible and reliable information about a broad range of issues prior, during and after elections, it is impossible for citizens to meaningfully exercise their right to vote in the manner envisaged by Article 13 (1) of the African Charter. The importance of access to information in the electoral process and for democratic governance is recognised in the African Charter on Democracy, Elections and Governance, as well as other sub-regional treaties and standards.¹⁸⁸

A cardinal principle at the heart of the right of access to information is that of proactive disclosure. The principle of proactive disclosure requires that those who hold information of public interest must routinely provide such information to the public without being requested to do so. Such information must be provided in easily accessible formats and it

¹⁸⁸ The African Commission on Human and Peoples Rights has Guidelines on Access to Information and Elections in Africa at p.4.



must consider the needs of its intended users. Proactive disclosure of election related information is thus a tool for fostering accountability and transparency of key election stakeholders and for guaranteeing the credibility and integrity of the electoral process. In line with Article 1 of the African Charter, which requires State Parties to adopt legislative or other measures to give effect to the rights, duties and freedoms enshrined in the Charter, State Parties must thus ensure that all stakeholders in the electoral process fulfil the responsibility of proactively disclosing information about the electoral process.¹⁸⁹

Further, election management bodies are mandated under Article 13 of the Guidelines to facilitate access to information, and shall, as part of their operations, create, keep, organize and maintain records in a manner that facilitates access to information, including for vulnerable and marginalized groups; and formulate clear procedures for making requests for information, which must include the required format of requests, costs for reproduction, timeframes and formats for providing requested information. Among other obligations.

3. Analysis and Discussion

3.1. Electoral Data as Personal Data under Kenyan and EU GDPR Law

Voters' personal electoral data unequivocally qualifies as personal data under both international and Kenyan data protection frameworks. Globally recognised legal instruments such as the GDPR define personal data broadly as any information relating to an identified or identifiable natural person. Kenya's Data Protection Act, 2019 adopts an almost identical definition, extending protection to any data from which an individual may be directly or indirectly identified.

Electoral data names, national ID numbers, dates of birth, addresses, polling station details, voter registration history, and biometric identifiers such as fingerprints or facial images falls squarely within this definition. Identification need not be absolute. As privacy scholars such as Daniel Solove and Paul Ohm demonstrate, data that enables identification through inference or cross-referencing is still personal data. Latanya Sweeney's empirical

¹⁸⁹ *Ibid* at pp.5 & 6.

research¹⁹⁰ further confirms that minimal datasets can uniquely identify individuals, a risk amplified in voter databases that often contain multiple identifiers.

The sensitivity of electoral data is heightened by its civic and political context. Privacy scholars emphasize contextual integrity, arguing that the sensitivity of data is often defined by the social or institutional context.¹⁹¹ Electoral data is collected to enable democratic participation, yet its misuse can facilitate voter profiling, political discrimination, or suppression. A case in point is the Cambridge Analytica¹⁹². Under the GDPR, political opinions constitute special category data, while Kenya's DPA similarly classifies political affiliation and biometric data as sensitive. This elevates the applicable protection threshold and triggers heightened obligations such as Data Protection Impact Assessments.

Consequently, institutions such as the IEBC, when deploying systems like KIEMS or Biometric Voter Registration, act as data controllers and are bound by principles of transparency, purpose limitation, minimisation, accuracy, and security under Section 25 of the DPA.

3.2. The Adequacy Standard in Cross-Border Transfers

The adequacy principle governs whether personal data may lawfully be transferred outside a jurisdiction. Under the GDPR, data may only be transferred to a third country where that country ensures a level of protection essentially equivalent to EU standards. This equivalence is functional rather than formal; laws need not be identical, but must be effective in practice. The Schrems II judgment underscores that adequacy is substantive and that contractual assurances cannot compensate for structural legal deficiencies in the recipient country.

¹⁹⁰ Sweeney, L. A. (2000). "Uniqueness of individuals identified by three data points: ZIP code, birth date, and gender." *Journal of Privacy and Confidentiality*, 1(1), 44-58.

¹⁹¹ Nissenbaum, H. (2004). *Privacy as contextual integrity*. *Washington Law Review*, 79(1), 119–157.

¹⁹² The Cambridge Analytica data breach involved the unauthorized harvesting of personal data from over 87 million Facebook users in 2014 without their consent. Data collected via a third-party app, originally intended for academic research, was repurposed by Cambridge Analytica to build psychological profiles and target political ads, notably during the **2016 U.S. presidential election** and the **Brexit referendum**. The scandal sparked global outrage, investigations, and significant regulatory scrutiny, highlighting major flaws in data privacy governance on social media platforms. See <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Kenya's Data Protection Act embeds the same logic. Section 48 requires that cross-border transfers occur only where the Data Protection Commissioner is satisfied that the receiving country provides adequate protection. The accompanying regulations require prior legal assessment, enforceable safeguards, and effective remedies for data subjects. Where adequacy is absent, transfers may proceed only under narrowly defined exceptions such as informed consent or compelling public interest.

3.2.1. Applying Adequacy to Kenyans' Electoral Data

When applied to voter data, adequacy demands more than contractual language. The IEBC must demonstrate that offshore processing arrangements preserve voter rights to access, rectification, and accountability, and that regulators and courts retain effective supervisory control. Where foreign vendors deny access to servers or invoke foreign law or intellectual property to resist oversight, the adequacy threshold is not met. Ultimately, adequacy functions as a safeguard of democratic integrity. It ensures that Kenyan voters do not lose constitutional and statutory protections merely because their data crosses borders.

Before reliance on an appropriate safeguard to make a transfer, the Data Protection Commissioner must be satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the Kenya Data Protection Act, 2019 regime.¹⁹³ This is only possible through a risk assessment which at a minimum level assesses the necessity and proportionality of the processing. Further, it examines the risks to individuals and how these risks are to be addressed. Consent of data subject is paramount.¹⁹⁴ In a scenario where assessment of the appropriate safeguard and legal framework of the country does not provide the required level of protection, the IEBC would have to add additional measures.

However, the data recipient country must not necessarily have identical data protection safeguards. The Court of Justice of the European Union found that adequacy does not require a finding of an identical level of protections. In particular, the means to which the third country in question has recourse for protecting personal data may differ from the ones

¹⁹³ Section 48(a), (b) of the Kenyan Data Protection Act, 2019.

¹⁹⁴ Section 49 of Kenyan Data Protection Act, 2019.

employed in the European Union, as long as they prove, in practice, effective measures for ensuring an adequate level of protection.¹⁹⁵ The adequacy standard, therefore, does not require a point-to-point replication of union rules. The test lies in whether, though the substance of data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection.¹⁹⁶ As explained in the *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems C-311/18 (Schrems II)*¹⁹⁷

The Schrems II precedent is instructive for Kenya because it establishes that cross-border data transfers are lawful only where personal data continues to enjoy protection that is substantively equivalent to domestic constitutional and statutory guarantees. Although decided under EU law, the case articulates principles of data sovereignty, effective oversight, and enforceable rights that resonate strongly with Kenya's electoral context.

In Schrems II, the Court held that contractual assurances cannot compensate for structural weaknesses in a foreign legal system that permit disproportionate access to personal data. This reasoning is directly relevant to Kenya where the IEBC has engaged foreign technology vendors to process and store voter data, including biometric identifiers, on offshore servers. Where foreign legal regimes, intellectual property claims, or contractual secrecy limit supervisory or judicial access, the protection promised to Kenyan voters becomes illusory.

The judgment also clarified that adequacy is a substantive test, not a formal one. Data exporters and regulators must assess whether transferred data remains subject to protections essentially equivalent to those guaranteed under domestic law, and must suspend transfers where this threshold is not met. This mirrors the adequacy requirement under Kenya's Data Protection Act, 2019.

Finally, Schrems II underscores the duty of regulators and courts to actively protect data subject rights. Applied to Kenya, it supports the argument that electoral data transfers that

¹⁹⁵ Case C-362/14, *Schrems* ("Schrems I"), ECLI:EU:C:2015:650, paragraph 74.

¹⁹⁶ See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM (2017)7 of 10.1.2017, section 3.1, pages 6-7.

¹⁹⁷ [The ECJ's full judgement in Case C-311/18](#) last visited 20/09/2024.

escape effective oversight undermine voter privacy, electoral integrity, and democratic accountability.

The *Data Protection (General) Regulations, 2021* establishes the due diligence required of data controllers before they transfer personal data outside the country. Data controller must ascertain that the recipient is bound by legally enforceable data protection obligations comparable to the Act and Regulations under it; the data subject has consented to the transfer; it has taken all reasonable steps to prevent unauthorized use or disclosure by the recipient; and the rights of the data subject are safeguarded. Data subject should be informed of the risks of cross-border transfer and safeguards in place. Obtaining consent deceptively or misleadingly is an offence which on conviction will attract a fine of up to KES 3 million or imprisonment for up to 10 years, or both.¹⁹⁸

A country or territory will be taken as having appropriate data protection safeguards if it has ratified *the African Union Convention on Cyber Security and Personal Data Protection*; or has a reciprocal data protection agreement with Kenya; or it has an adequate data protection law as determined by the Commissioner.¹⁹⁹

The ODPC has succinctly provided regulations that govern transfer of personal data (including electoral biometric data) on the basis of appropriate safeguards as summarized below.

a. Transfer of Personal Data on the Basis of Appropriate Safeguards²⁰⁰

Before any personal data can be transferred outside the country, the data controller or processor must ensure that an adequate level of data security and protection is guaranteed. *Appropriate safeguards* and *deemed appropriate safeguards* are two of the general principles of transferring personal data outside Kenya.

The condition on *appropriate safeguards* would be met in the following instances:

¹⁹⁸ This is the general penalty provided under s.73(1) of the DPA, 2019 for offences without specific penalties

¹⁹⁹ The Data Protection Act, 2019 Sections 49(1) (2) and (3).

²⁰⁰ ODPC Data Protection (General) Regulations, 2021.

- 
1. where a legal instrument, such as a contract binding on both the sender and recipient of the personal data, contains provisions requiring appropriate safeguards for the protection of personal data that are essentially equivalent to the protection under the Act and Regulations; or
 2. the data controller, having assessed all the circumstances surrounding the transfer of that type of personal data to another country or relevant international organization, concludes that appropriate safeguards exist to protect the data. This could include technical and organizational safeguards implemented by the recipient entity.

Under the *principle of appropriate safeguards*, transfer of personal data should be documented and a demonstration of the adequacy of the safeguards and the aforementioned documentation provided to the Data Commissioner upon request. The transfer documentation includes information such as the date and time of the transfer; the name of the recipient; justification for the transfer; and a description of the personal data transferred.

In addition to the above, there are instances where the ODPC, with the guidance on the Act and Regulation will infer that certain safeguards have been met.

This principle is referred to as a *deeming of appropriate safeguards*. This occurs in the following instances:

- (a) where a country has ratified *the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*.
- (b) the recipient country has a reciprocal data protection agreement with Kenya; or
- (c) there are binding corporate rules, approved by the Office, among a concerned group of undertakings or enterprises.

The burden of proof for *appropriate safeguards* lies with the Data Controller or Processor transferring personal data.



A classic case that highlights deficiency of appropriate safeguards in Kenya, is the *Worldcoin case*.²⁰¹ This judgment addressed a judicial review application filed against Worldcoin entities and Kenyan regulators concerning the collection and processing of Kenyan residents' biometric data using the "Orb" device. The Applicants alleged that Worldcoin's actions were unlawful, citing the failure to conduct an adequate Data Protection Impact Assessment (DPIA), obtaining of consent through inducement (cryptocurrency tokens), lack of registration for some Worldcoin entities as data processors or controllers, unlawful cross-border data transfers, and the lack of type approval for the Orb device. The Applicants argued these actions violated Kenyan data protection laws and fundamental rights, including the right to privacy and human dignity. The Court agreed with the Applicants and the Data Protection Commissioner and Communications Authority that Worldcoin entities had violated data protection laws, including failing to conduct an adequate DPIA, obtaining invalid consent (induced by tokens and bundling purposes), processing data without proper registration, transferring data without safeguards, and using the Orb without type approval. The Court issued orders prohibiting further processing under unlawful conditions, quashing the past decisions based on invalid consent or no DPIA, and mandating the permanent erasure and destruction of the unlawfully collected data. Adequacy measures were not met.

In another case, *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)*²⁰² the High Court of Kenya ruled on the constitutionality of the Huduma Namba (NIIMS) digital ID system. The Petitioners argued that it infringed on the right to privacy, equality, and non-discrimination, especially for marginalized communities like the Nubians. The Court held that while the system itself was not unconstitutional, it lacked a comprehensive legal framework on data protection. The rollout was halted until adequate safeguards, including a data protection impact

²⁰¹ Republic v Tools for Humanity Corporation (US) & 8 others; Katiba Institute & 4 others (Exparte Applicants); Data Privacy & Governance Society of Kenya (Interested Party) (Judicial Review Application E119 of 2023) [2025] KEHC 5629 (KLR) (Judicial Review) (5 May 2025) (Judgment) Neutral citation: [2025] KEHC 5629 (KLR)

²⁰² [2020] eKLR High Court of Kenya.

assessment and legal backing, were implemented. It affirmed privacy as a fundamental right.

4. Recommendations

This paper made an assessment on cross-border transfer of personal voters' data and data subject rights thereof. As Kenya's electoral processes increasingly rely on digital systems, the movement of voters' personal data across borders has become both unavoidable and legally sensitive. For the Independent Electoral and Boundaries Commission (IEBC), cross-border data transfers raise fundamental questions about privacy, sovereignty, public trust, and the integrity of elections. This expose illustrates practical and legally grounded approach for managing electoral data transfers in a manner consistent with the Data Protection Act, 2019, electoral laws, and constitutional values. It focuses on adequacy, accountability, and transparency, offering guidance on how IEBC can safeguard voters' personal data while meeting operational and technological demands of modern elections.

Protection of voters' personal electoral data requires the IEBC to adopt a cross-border data transfer compliance framework grounded in the principle of adequacy under the Data Protection Act, 2019 and Kenya's biometric and electoral regulations. Adequacy should operate as the legal threshold, not a procedural formality. The following are recommendations for improvement:

First, IEBC must conduct mandatory Data Protection Impact Assessments before procuring or deploying any electoral technology that involves offshore processing or storage of voters' data. These DPIAs should specifically assess foreign legal regimes, surveillance laws, contractual enforceability, and the practical ability of Kenyan regulators and courts to exercise oversight over voter data. DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.

A DPIA does not have to indicate that all risks have been eradicated. But it should help to document them and assess whether or not any remaining risks are justified. An effective DPIA can also bring broader compliance, financial and reputational benefits, helping

demonstrate accountability and building trust.²⁰³ This is the thread that runs through the fabric of public participation²⁰⁴ as envisaged in the Kenyan Constitution of 2010.

Second, cross-border transfers should be permitted only where the recipient jurisdiction provides protection essentially equivalent to Kenyan law. Where *adequacy* is not established, IEBC must prohibit transfers or require binding safeguards, including data localisation for biometric identifiers, encryption with Kenyan-held keys, and unfettered supervisory access for IEBC, the Data Protection Commissioner, and courts.

Third, electoral contracts must clearly subordinate intellectual property claims to voter data rights. Vendors should be contractually designated as processors, prohibited from asserting ownership or secrecy over electoral data, and obligated to submit to Kenyan jurisdiction. A data controller ought to have a written contract for data transfers. Such a contract unequivocally speaks for the responsibilities and liabilities of both the controller and Processor. In scenarios where a Processor sub contracts another organization to be a sub-processor to assist in processing of personal data for a controller, then a written contract with that sub-processor must be in place. The contracts must set out: the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data categories of data subject; and the controller's obligations and rights. Contracts must also include specific terms or clauses regarding: processing only on the controller's documented instructions; duty of confidence; appropriate security measures; using sub-processors; data subjects' rights; assisting the controller; end-of-contract provisions, audits and inspections. Contracts must bear clear outline of the responsibilities and liabilities of controllers when using a data processor. Controllers must only use data processors that can give sufficient guarantees that they will implement appropriate technical and organizational measures to ensure their processing will meet data protection laws requirements and protect data subjects' rights. Controllers shall be primarily responsible for overall compliance with *Data Protection Act, 2019*, and for demonstrating that

²⁰³ See note 3 at p.240.

²⁰⁴ Public Participation: refers to the process by which citizens, as individuals, groups or communities (also known as stakeholders), take part in the conduct of public affairs, interact with the state and other non-state actors to influence decisions, policies, programs, legislation and provide oversight in service. Article 118 of the Constitution of Kenya, 2010.

compliance. Failure to which, they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

For instance, *Yahoo! Inc. v. Belgian Public Prosecutor*²⁰⁵ This case is significant in data protection and jurisdictional law, where the Belgian Supreme Court held that Yahoo!, despite being based in the U.S. with no physical presence in Belgium, was still obligated to comply with data disclosure orders because it actively targeted Belgian users. The Court emphasized that this obligation did not entail extraterritorial enforcement, as Yahoo! could bring the data within Belgian jurisdiction for compliance.

Fourth, the Office of the Data Protection Commissioner should play an active *ex ante* oversight role by authorising high-risk transfers and auditing compliance throughout the electoral cycle. At all times, no cross-border transfer should lower the level of protection guaranteed to voters under Kenyan law. Adequacy must function as a safeguard for digital sovereignty, electoral integrity, and the primacy of voter privacy.

5. Conclusion

Kenya's *Data Protection Act, 2019*, together with *the Data Protection (General) Regulations, 2021*, *the Guidance Notes for Electoral Purposes (2023)*, and *the Guidance Notes on Processing Biometric Data (2025)*, require electoral data to be processed through data centres or servers located in Kenya, or at minimum for a serving copy to be retained within the country. Acknowledging that, the Data Protection Act has extra-territorial jurisdiction. This approach supports data availability and access, a principle implicitly reinforced by the Supreme Court during the 2017 presidential election petition. IEBC's confirmation in December 2021 that it had established local data centres helps address earlier concerns on transparency and access, while strengthening compliance with the DPA.

Where IEBC transfers electoral data to international organisations, such transfers must be strictly controlled and supported by binding contracts with enforceable safeguards and

²⁰⁵ Cour de cassation [Cass.] [Supreme Court] Belgium, 1 December 2009, No. P.09.1039.F

remedies for data subjects as proposed in the recommendations. At a minimum, adequacy of protection must be demonstrated. Transfers that undermine voters' access to their data contradict the 2023 and 2025 Guidance Notes. Restricted transfers may rely on approved standard clauses, an ODPC-approved code of conduct, or recognised certifications such as ISO 27701, all of which must be lodged with the Data Protection Commissioner.

Alternatively, have a local cloud, employ the services of a local tech company and safeguard our data. As part of the IEBC audit by Klynveld Peat Marwick Goerdeler (KPMG), reviewed controls over database and infrastructure control and made recommendations on strengthening controls over application, database and infrastructure to ensure security of the ROV. The Commission has already commenced implementation of KPMG recommendations with third parties providing Commission with IT support. This includes application of "*Least Privilege Principle*" by disabling all user access rights and only giving them privileges needed to complete their specific tasks.²⁰⁶

Ensuring compliance and integrity is crucial for successful voting systems. IEBC, technology providers, and stakeholders must work collaboratively to adhere to legal and regulatory requirements, privacy laws and data protection standards. Regular audits, transparent processes, and ongoing monitoring help maintain compliance and build trust in voting systems. "Adequacy" in concurrence with the Data Commissioner's approval and consent remain the true north before any mass cross-border data transfer of voters' personal data.

Depending on the availability of data localization resources in Kenya; this paper is not rigid on zero cross-border data transfer of personal electoral data but affirms that any such transfer shall be guided by the adequacy principles grounded in the laws and guiding principles. The argument remains that access to personal electoral data by voters is safeguarded by data protection laws in Kenya.

²⁰⁶ KPMG REPORT ON IEBC PREPAREDNESS DATED JUNE 20TH 2022 under (v)Database Security and Infrastructure Controls at p.5. <https://www.iebc.or.ke/uploads/resources/OG6FL8Nc9b.pdf>



This very first edition of the TPPA Journal brings assessments of different data protection legal and regulatory frameworks in some of the African countries (and in comparative perspectives). This volume is dedicated to articles assessing and discussing one of the most consequential yet underexplored dimensions of democratic integrity in Africa – the protection of election data. Last year, Africa witnessed several countries undergoing their political elections. With a notable increasing use of digital technology to conduct election activities – from the use of digital voter ID cards to digitized semi-digitized ballots. The result is each voting action involves the conversion of voter's data into digital formats – stored, transmitted, or counted electronically.

Although this is an innovation crucial for supporting accuracy, speed, record-keeping and accessibility, it raises concerns around cybersecurity, data protection and privacy. This is especially pertinent when the technology used is a foreign imported technology or when voter information is stored in foreign cloud services.

Contributions in this volume examine how legal systems are responding to these challenges, and offer comparative analysis of data protection frameworks in some of the African countries. They interrogate the extent to which current legal and regulatory frameworks safeguard electoral credibility, transparency, personal data and support public trust. The articles bridge doctrinal analysis and practical realities and invite scholars, practitioners, and policymakers to rethink the role of data protection law and their feasibility in protection personal data in electoral process in Africa.