Uneven Enforcement of Data Protection Laws

Puts Data Subjects' Rights at Risk in Uganda's 2026 Polls

A DATA PROTECTION ELECTION WATCH REPORT

UNWANTED WITNESS

"Amplifying Voices, Changing lives"

Uneven Enforcement of Data Protection Laws

Puts Data Subjects' Rights at Risk in Uganda's 2026 Polls

A DATA PROTECTION ELECTION WATCH REPORT

The Unwanted Witness

Bulange Mengo, Block 381, Plot 26, Nsibambi Village, Sentema Road, P.O.BOX 71314 Clock Tower Kampala – Uganda

Mob: +256-414 697635 Email: info@unwantedwitness.org
Website: unwantedwitness.org

Table of Contents

List of Acronyms

AI	Artificial Intelligence
APC	Association for Progressive Communications
BVV	Biometric Voter Verification
BVVK	Biometric Voter Verification Kit
BVVS	Biometric Voter Verification System
Cap	Chapter (of the Laws of Uganda)
DPIA	Data Protection Impact Assessment
DPPA	Data Protection and Privacy Act, 2019
DPO	Data Protection Officer
EC	Electoral Commission
ICT	Information and Communications Technology
NIN	National Identification Number
NIRA	National Identification and Registration Authority
PDPO	Personal Data Protection Office
SI	Statutory Instrument
SMS	Short Message Service
X	Social media platform formerly known as Twitter

Glossary

Term	Definition
Accountability (Data Protection)	The obligation of data controllers and processors to demonstrate compliance with data protection principles, including lawful processing, security safeguards, and transparency.
Artificial Intelligence (AI)	Computational systems capable of performing tasks that typically require human intelligence, including pattern recognition, predictive analytics, and generative content creation.
Biometric Data	Personal data resulting from specific technical processing relating to physical or behavioral characteristics, such as fingerprints or facial images, used for identification.
Biometric Voter Verification Kit (BVVK)	A device deployed at polling stations to authenticate voter identity using fingerprint or facial recognition technologies.
Biometric Voter Verification System (BVVS)	The nationwide infrastructure supporting biometric authentication of voters during elections.
Consent (Data Protection)	A freely given, specific, informed, and unambiguous indication of a data subject's agreement to the processing of their personal data.
Cross-Border Data Transfer	The transmission or storage of personal data outside Uganda, subject to adequacy and consent requirements under the Data Protection and Privacy Act.
Data Breach	Unauthorized access, disclosure, alteration, destruction, or loss of personal data.
Data Controller	A person or institution that determines the purposes and means of processing personal data.
Data Minimization	The principle requiring that only personal data necessary for a specified purpose be collected and processed.
Data Processing	Any operation performed on personal data, including collection, storage, retrieval, transmission, alteration, or deletion.
Data Processor	A person or entity that processes personal data on behalf of a data controller.
Data Protection Impact Assessment (DPIA)	A structured risk assessment required for high-risk data processing activities to evaluate potential impacts on rights and freedoms.
Deepfake	AI-generated synthetic media (audio, video, or images) that convincingly imitates real individuals.
Digital Voter Portal	An online platform allowing voters to verify registration details and polling station information.
Electoral Data Governance	The framework of laws, policies, technical safeguards, and oversight mechanisms regulating the handling of voter and election-related data.
Encryption	The process of converting information into coded form to prevent unauthorized access.
Function Creep	The gradual expansion of data use beyond the original purpose for which it was collected.
Generative AI	Artificial intelligence systems capable of producing synthetic text, audio, images, or video content.
Interoperability	The ability of different systems or databases (e.g., EC and NIRA systems) to exchange and use data.
Lawful Basis	A legally recognized justification for processing personal data, such as consent, public duty, or legal obligation.
National Identification Number (NIN)	A unique identifier assigned by the National Identification and Registration Authority (NIRA) used in civil and electoral verification processes.

Personal Data	Any information relating to an identified or identifiable natural person.
Personal Data Protection Office (PDPO)	The regulatory authority mandated to oversee compliance with Uganda's Data Protection and Privacy Act.
Political Profiling	The processing of personal data to analyze or predict political opinions, preferences, or behaviors.
Purpose Limitation	The principle that personal data must be collected for specific, explicit, and legitimate purposes and not further processed incompatibly.
Results Transmission System	Electronic processes used to capture, transmit, or archive election results data.
Sensitive Personal Data	Categories of personal data requiring heightened protection, including biometric data and political opinions.
Selective Enforcement	Uneven or disproportionate application of regulatory or criminal enforcement measures.
Transparency (Data Governance)	The requirement that data subjects be informed about how their personal data is collected, used, stored, and shared.
Vendor Lock-in	Dependency on proprietary technology providers that limits independent auditing or system flexibility.
Voter Register	The official database of individuals eligible to vote in an election.

Acknowledgements

This report is the product of collective effort, institutional courage, and principled commitment to democratic accountability.

Unwanted Witness extends its deep appreciation to the members of the ***Data Protection Election Watch team,*** field observers, researchers, legal analysts, and technical advisors who worked tirelessly throughout the ***2025–2026 electoral cycle*** to document, analyze, and verify findings under often challenging conditions.

We are grateful to electoral stakeholders, civil society actors, journalists, technology practitioners, and citizens who shared information, insights, and experiences that informed this investigation. Their willingness to engage constructively strengthened the depth and credibility of this work.
We particularly acknowledge the participation of representatives from the Electoral Commission, political parties, and other institutions who attended the ***July 2025 national training workshop*** on safeguarding electoral integrity through ethical data practices. That engagement reflected a shared recognition that data protection and electoral credibility are inseparable.

Unwanted Witness also acknowledges the financial support provided by the Association for ***Progressive Communications (APC),*** whose commitment to advancing digital rights, privacy, and democratic governance made this investigation possible. APC's support enabled the deployment of the ***Data Protection Election Watch tool,*** stakeholder engagement activities, and the production of this report. The findings and conclusions, however, remain the independent analysis of ***Unwanted Witness.***

Finally, we recognize the broader community of digital rights defenders and democratic accountability advocates across Africa and beyond whose work continues to inspire the pursuit of transparent, rights-respecting, and inclusive digital governance.

Executive Summary

This report, "***Uneven Enforcement of Data Protection Laws Puts Data Subjects Rights at Risk in Uganda's 2026 Polls***", presents a systematic assessment of how personal data were governed across Uganda's most technologically intensive electoral cycle to date. Using the ***Data Protection Election Watch Tool***, the investigation evaluated compliance with Uganda's ***Data Protection and Privacy Act, 2019 (DPPA)***[1], its ***2021 Regulations***[2], electoral laws, and applicable international data protection principles.

The findings reveal that while Uganda entered the 2026 elections with a formal legal framework in place, compliance was operationally under-embedded, oversight uneven, and data governance safeguards inconsistently applied across institutions.

a) Key Findings on Personal Data Handling Across the Electoral Cycle

Throughout voter registration, campaigning, polling-day verification, and post-election processes, personal data played a central and structuring role in the conduct of the elections.

i. Biometric and Identity-Linked Processing:

The 2026 elections involved the procurement and deployment of ***109,142 Biometric Voter Verification Kits (BVVKs)***[3] by the Electoral Commission, alongside the deep integration of the ***National Identification Number (NIN)*** system into voter registration and verification processes. This configuration created a consolidated ecosystem linking civil identity data with electoral eligibility[4]. However, no publicly *accessible* ***Data Protection Impact Assessments (DPIAs)*** were demonstrated for these high-risk processing operations.

ii. Institutional Compliance Gaps:

- The ***Electoral Commission (EC)*** registered with the ***Personal Data Protection Office (PDPO)*** only after the elections ***(21 January 2026).***
- No political party registered with the ***PDPO*** during the electoral cycle.
- No publicly available privacy notices or structured retention policies were demonstrated for large-scale voter data processing.

iii. Campaign-Era Data Practices:

Political campaigning increasingly relied on bulk SMS messaging, decentralized phone-call mobilization, social media targeting, and analytics-based segmentation. These activities occurred without clearly articulated lawful bases, transparent consent mechanisms, or identifiable data controllers.

iv. Digital Voter Portals and Exposure Risks:

Digital voter verification portals processed and displayed personal data at scale. The FANON[5] incident illustrated how large datasets could potentially be scraped, aggregated, or repurposed, highlighting weaknesses in authentication controls, rate limiting, and system governance.

v. Storage Limitation and Retention Ambiguity:

The statutory obligation not to retain personal data *"longer than necessary"* was not transparently operationalized. Defined deletion triggers, archival timelines, or post-election disposal policies were not publicly demonstrated.

---

1 *Data Protection and Privacy Act, 2019* (Uganda), Act No. 9 of 2019
2 Data Protection and Privacy Regulations, 2021 (Statutory Instrument No. 21 of 2021), *Uganda Gazette*, 12 March 2021
3 "Statement by the Chairperson, Electoral Commission on the Progress of Implementation of Activities under the Roadmap for General Elections 2026," Electoral Commission, December 17, 2025
4 Electoral Commission of Uganda, *Press Statement on the Extension of the General Update of the National Voters Register* (10 February 2025)
5 *"Exposed: Voter App Blocked Days Before Uganda Polls"* The Kenya Times

b) Summary of Major Risks, Violations, Weaknesses, and Positive Practices

i. Major Risks and Weaknesses

- **Function Creep:** Integration of NIN and voter systems risks repurposing civil identity data for electoral or ancillary uses beyond original scope.
- **Centralization and Breach Impact:** Biometric data and NIN-based identifiers are irreversible credentials; any compromise carries long-term consequences.
- **Opaque Interoperability:** No codified, publicly accessible framework governed EC–NIRA data exchange.
- **Selective Enforcement Concerns:** Criminal enforcement actions against individual actors occurred alongside documented institutional non-compliance, raising proportionality and rule-of-law concerns.
- **AI-Enabled Disinformation:** Generative AI tools amplified risks of deepfakes, synthetic political messaging, and manipulation using biometric likenesses.
- **Cross-Border Exposure:** Potential offshore hosting and data routing introduced sovereignty and adequacy concerns.

ii. Violations and Non-Compliance

- Universal non-registration of political parties with the PDPO.
- Delayed EC registration during live processing periods.
- Absence of published DPIAs for high-risk biometric and electoral systems.
- Lack of transparent data retention and deletion protocols.

iii. Positive Practices Observed

- Multi-stakeholder data protection training convened in July 2025.
- Advisory letters issued to electoral stakeholders prior to polling.
- Continued legal recognition of data protection as applicable to elections.

However, these positive measures did not translate into measurable, systemic compliance outcomes.

c) Overview of Electronic Components of the 2026 Electoral System

The 2026 elections were conducted within a dense and interconnected digital ecosystem:

- **Biometric Voter Verification System (BVVS/BVVK):** Mandatory biometric authentication at all 50,739 polling stations.
- **NIN–Voter Register Integration:** Identity validation and polling station assignment linked to NIRA databases.
- **Digital Voter Display Portals:** Online platforms for voter verification and register display.
- **Electronic Results Capture and Archiving:** Digital scanning and storage of declaration forms.
- **Telecommunications-Based Campaigning:** Bulk SMS, automated calls, and decentralized voter outreach.
- **Platform-Mediated Political Communication:** Meta, WhatsApp, TikTok, X, and YouTube as primary narrative battlegrounds.

This architecture centralized identity verification, expanded data-driven political influence, and increased reliance on digital infrastructures whose technical and governance safeguards were not fully transparent.

d) High-Level Stakeholder Compliance Scorecard

Stakeholder	Registration Compliance	DPIA Demonstration	Transparency & Privacy Notices	Data Governance Embedding	Overall Assessment
Electoral Commission	Post-election registration	Not publicly demonstrated	Limited	Partial	Weak operational comp liance
Political Parties	None registered	None demonstrated	Minimal	Informal practices	Systemic non-compliance
PDPO	Operational	No published high-risk list	Limited sector guidance	Reactive enforcement	Under-embedded oversight
NIRA–EC Integration	Formal cooperation	Not publicly assessed	Opaque interoperability	High centralization risk	Governance gap
Private Campaign Actors	Not demonstrated	Not demonstrated	Opaque	Informal profiling	High risk

Overall, the compliance environment reflects a legally established but operationally fragmented data protection regime.

e) Priority Recommendations

i. **To the Electoral Commission (EC)**

- Publish a comprehensive Electoral Data Governance Framework covering data categories, lawful bases, retention schedules, and interoperability safeguards.
- Conduct and publish DPIAs for biometric verification systems and NIN integration.
- Institutionalize independent cybersecurity audits prior to future elections.
- Establish automatic deletion triggers for biometric logs and voter roll extracts.

ii. **To the Personal Data Protection Office (PDPO)**

- Publish binding electoral data protection guidelines at least 12 months before the next election cycle.
- Issue the mandatory high-risk processing list under ***Regulation 12(3),*** explicitly including biometric electoral systems.
- Adopt proactive compliance audits rather than reactive enforcement models.
- Establish a temporary Electoral Data Oversight Unit during election periods.

iii. **To Political Parties**

- Register with the ***PDPO*** at least 12 months prior to elections.
- Appoint ***Data Protection Officers (DPOs).***
- Publish campaign privacy notices and lawful consent mechanisms for bulk messaging.
- Conduct DPIAs for profiling, analytics, and AI-based campaigning tools.

iv. **To Policymakers and Parliament**

- Amend electoral laws to embed mandatory digital safeguards, independent audits, and retention limits.
- Codify an inter-agency electoral data-sharing framework governing EC–NIRA integration.

- Strengthen parliamentary oversight through annual electoral data governance reporting.
- Clarify proportionality and public-interest safeguards in enforcement provisions.

Uganda's 2026 elections did not reveal a legislative vacuum. They revealed an implementation deficit.

As biometric verification, AI-generated political messaging, and integrated identity systems become structural features of electoral administration, data governance must evolve from reactive compliance to embedded democratic infrastructure.

Privacy in elections is not merely an individual right. It is a precondition for trust, fairness, and legitimacy in a digitally mediated democracy.

1. Introduction

1.1 Overview of Uganda's evolving electoral environment and digital transformation

Over the preceding decade, Uganda's electoral process was observed to have shifted from a predominantly paper-based administrative model toward a hybrid system increasingly mediated by digital technologies. ***Biometric Voter Verification System (BVVS)*** was first introduced during the *2016* general elections and was subsequently expanded across successive electoral cycles[6]. In the lead-up to the 2026 general elections, the ***Electoral Commission (EC)*** was reported to have undertaken a nationwide update of the National Voters' Register and to have procured and received *109,142* ***Biometric Voter Verification Kits (BVVK)*** which were deployed for the 2025/2026 General Elections[7]. These initiatives were publicly framed by the EC as a measure aimed at improving the management and conduct of elections through authentication of voter identity.

In parallel, Uganda's foundational identity infrastructure administered by the ***National Identification and Registration Authority (NIRA)*** through the ***National Identification Number (NIN)*** system, became increasingly integrated into electoral administration[8]. As confirmed by the Electoral Commission (EC), the update of the National Voters Register relied significantly on data extracted from NIRA's national identity database, including the incorporation of citizens registered by NIRA and the use of NINs to assign polling stations and verify voter particulars. The EC further acknowledged operational dependence on biometric registration kits obtained from NIRA for voter registration and update exercises.

This institutional convergence between civil registration and electoral management represents a structural consolidation of Uganda's identity and voting data systems. While framed as an efficiency and verification measure, the integration of biometric civil identity data into voter roll compilation and polling station assignment carries significant implications for data protection and electoral integrity. It centralizes sensitive personal and biometric information within interoperable state databases, heightens the risks of function creep and surveillance, and reduces meaningful separation between citizenship documentation and political participation. In the electoral context, this architecture reshapes the governance of identity, enfranchisement, and data control, making voter eligibility, verification, and participation increasingly contingent on the integrity, security, and lawful processing of the national identity system itself.

At the same time, political actors, campaign organizations, and commercial intermediaries were increasingly documented to have adopted data-driven campaigning practices. These included the use of bulk SMS and voice calls, micro-targeted advertising on digital platforms, influencer-led messaging, and analytics-based voter segmentation. The growing reliance on such techniques intensified scrutiny over the sources of voter data, the legality of its collection and processing, the role of third-party data processors, and the adequacy of safeguards to prevent misuse, profiling, or unauthorized sharing of personal information.

These technological developments unfolded within the context of a relatively recent domestic data protection regime. Uganda's Data Protection and Privacy Act (2019)9, together with its implementing regulations10, constituted the primary legal framework governing the processing of personal data during the electoral cycle. The establishment of the Personal Data Protection Office (PDPO) was intended to provide oversight through registration, compliance monitoring, and enforcement. However, throughout the 2026 electoral period, concerns persisted regarding the PDPO's enforcement capacity, the absence of sector-specific guidance on election technologies, and the lack of clear, enforceable rules governing political parties, candidates, and campaign service providers. As digital tools assumed increasingly central roles in both electoral administration and political communication, these regulatory gaps were widely regarded as unresolved structural weaknesses in Uganda's electoral data governance framework.

6 The Electoral Commission of Uganda, *Press Statement on the Preparations for 2016 General Elections*, 27 January 2016, Electoral Commission of Uganda
7 "Statement by the Chairperson, Electoral Commission on the Progress of Implementation of Activities under the Roadmap for General Elections 2026," Electoral Commission, December 17, 2025
8 Electoral Commission of Uganda, *Press Statement on the Extension of the General Update of the National Voters Register* (10 February 2025)
9 Data Protection and Privacy Act, 2019 (Uganda)
10 Data Protection and Privacy Regulations, 2021 (Uganda)

1.2 Why data protection matters for democratic integrity, trust, and transparency

Elections were widely understood to function as a trust-based public good, dependent on citizens' confidence that their votes remained secret, were accurately counted, and would not be used to their detriment[11]. In this context, the collection, storage, and reuse of personal and biometric data within electoral processes were observed to implicate not only individual privacy rights but also the integrity and legitimacy of democratic governance. Where voters doubted the security of their biometric data, national identification numbers, telephone records, or inferred political preferences or feared that such information could be repurposed for surveillance, profiling, or partisan targeting, their willingness to participate risked being chilled, thereby undermining confidence in the electoral process and rendering outcomes more vulnerable to contestation.

As detailed in this report, robust data protection emerged not as a peripheral technical matter, but as a foundational condition for credible and inclusive elections. The report demonstrates that the ability of electoral authorities and associated actors to show lawful processing, clear purpose limitation, and effective safeguards over voter data directly shaped public trust in both the integrity of the electoral process and the legitimacy of its outcomes.

At the same time, the increasing concentration of sensitive identifiers including fingerprints, facial images, and National Identification Numbers within centralized and interoperable databases was identified as significantly raising the stakes of any data breach, unauthorized access, or unlawful sharing. While the deployment of biometric and digital technologies was credited with reducing certain electoral risks, such as duplicate registration and voter impersonation[12], it was also understood to introduce new systemic vulnerabilities. These risks were particularly pronounced in contexts where legal oversight mechanisms were weak, data minimization principles were inconsistently applied, secure storage standards were unclear, and retention or deletion policies were either absent or inadequately enforced.

Ensuring transparency around how electoral data were collected, processed, stored, and disposed of, and ensuring that both legal and technical safeguards were effectively implemented, was therefore widely regarded as essential to protecting voters' rights and sustaining public confidence in Uganda's 2026 electoral process.

1.3 How personal data shaped voter experience, security, and electoral credibility

In the period leading up to and during the 2026 electoral cycle, the practical effects of expanded data collection were observed at multiple stages of the election cycle. During updates to the voter register, biometric data capture and photographic enrolment were reported to have altered the mechanics of voter registration, introducing new administrative requirements while also enabling automated verification processes intended to reduce certain forms of fraud[13]. These changes reshaped interactions between voters and electoral officials and increased reliance on digital systems at the point of enrolment.

On polling day, biometric voter verification kits (BVVKs) were deployed nationwide to authenticate voter identity at polling stations. However, widespread reports of machine failures, delayed start times, connectivity challenges, insufficient training of operators, and malfunctioning or aging equipment significantly disrupted the verification process[14]. In several polling stations, the devices reportedly failed to load voter data, authenticate fingerprints, or function altogether, forcing election officials to revert to manual procedures. These operational breakdowns not only delayed voting and prolonged queues but also raised concerns about the integrity, auditability, and transparency of the verification process. The inability of some devices to reliably generate or preserve verifiable logs further complicated prospects for post-election review and dispute resolution. As documented in this report, the technical fragility and procedural handling of the BVVK system played a consequential role in shaping voter experience, public perceptions of procedural fairness, and broader confidence in the administration of the 2026 elections.

Beyond electoral administration, personal data were documented as central to political outreach and persuasion throughout the campaign period. Political actors increasingly relied on telephone databases, social-media-based custom audiences, and third-party analytics services to segment voters and deliver targeted messaging[15]. While such

11 European Commission, Study on the Impact of New Technologies on Free and Fair Elections: Literature Review (Annex I), Version 3.0 (19 Mar. 2021), at page 141

12 Electoral Commission of Uganda, Statement on Preparations for the General Elections 2016, 12 February 2016 (official press release)

13 Electoral Commission of Uganda, *Statement on Progress of Implementation Activities* (Nov 26, 2025)

14 Parliament of Uganda, Statement on BVVK failures and government response, *Parliament of Uganda News* (29 January 2026)

15 Bobi Wine, Facebook post, *"Here's the plot for tomorrow! We're challenging ourselves to make 50 phone calls each to voters,"* 13 March 2026 (on file with author)

practices were understood to enhance efficiency and reach, they also raised concerns about coercive or manipulative tactics in contexts where informed consent, transparency, and accountability were limited or absent. Previous election assessments and media reporting in Uganda and comparable jurisdictions had documented the use of automated calls[16], mass messaging, and targeted digital campaigns, underscoring how the same datasets that facilitate communication can also be deployed to micro-target voters, disseminate misleading information, or amplify polarizing narratives.

The credibility of electoral outcomes was therefore found to depend on both technical and governance dimensions of the digital ecosystem. Secure storage and transmission of electronic records, the availability of auditable device logs, independent scrutiny of technology vendors, and the existence of legal safeguards preventing unauthorized access or secondary use of electoral data were all identified as critical factors. Where weaknesses emerged in any of these areas, they were widely regarded as contributing to contested results, post-electoral litigation, and longer-term erosion of public trust in democratic institutions.

1.4 Data Protection Election Watch Initiative: Rationale, Design, and Systemic Significance

The ***Data Protection Election Watch initiative*** was established as a structured, evidence-based response to Uganda's rapid digitization of electoral processes, where biometric registration, digital verification, electronic results management, and data-driven campaigning expanded faster than oversight and accountability mechanisms. Recognizing that personal and biometric data had become central to voter eligibility, political mobilization, and electoral legitimacy, the initiative sought to systematically document how data was collected, processed, shared, secured, and retained across the entire electoral cycle.

The Watch combined monitoring, capacity-building, and advocacy. ***Unwanted Witness*** conducted a national data protection training for electoral stakeholders in July 2025[17], issued advisory letters to the Electoral Commission[18] and political parties[19] on registration and DPIA compliance, and deployed a structured monitoring tool to assess real-time handling of voter data. These efforts aimed not only to document non-compliance but to promote preventive governance.

The initiative was driven by heightened risks associated with mass biometric collection, centralized identity integration, bulk political messaging, and emerging AI-assisted campaigning in relation to the state's obligation under international human rights law[20]. In this context, data protection is inseparable from electoral integrity. By linking privacy compliance to democratic credibility, the Election Watch reframed voters as rights holders entitled to transparency, accountability, and remedy, and positioned data governance as a foundational safeguard for Uganda's digital elections.

16 Unwanted Witness, "MTN Uganda Has Shared Subscribers' Data with the Ruling Party (NRM)
17 Unwanted Witness, National Training on Safeguarding Electoral Integrity through Ethical Data Practices, Kampala, July 2025
18 Unwanted Witness, Advisory Letter to the Electoral Commission on Data Protection Compliance, 10 March 2025
19 Unwanted Witness, Advisory on Compliance with the Data Protection and Privacy Laws, letter to political parties, 10 March 2025
20 United Nations General Assembly, Universal Declaration of Human Rights, adopted 10 December 1948, Articles 12 and 21

2. Objectives of the Data Protection Election Watch Tool

The ***Data Protection Election Watch Tool*** was developed to operationalize data protection oversight within Uganda's 2026 electoral context by translating abstract legal obligations into observable, measurable indicators across the electoral cycle. The tool was designed to move beyond episodic incident reporting and enable systematic assessment of how personal data were governed in practice by key electoral stakeholders.

Specifically, the tool aimed to:

- **Assess stakeholder compliance with data protection laws**

  The Tool sought to evaluate the extent to which public authorities, political actors, and private entities involved in the electoral process complied with the requirements of the ***Data Protection and Privacy Act, 2019*** and the ***Data Protection and Privacy Regulations, 2021***. This included assessment of registration with the ***Personal Data Protection Office (PDPO),*** existence of privacy notices, appointment of data protection officers, implementation of technical and organizational safeguards, and adherence to lawful processing principles.

- **Evaluate Electoral Commission data handling across the electoral cycle**

  A core objective of the Watch was to examine how the Electoral Commission collected, processed, stored, shared, and retained voter data at each stage of the electoral process. This encompassed voter registration and register updates, biometric voter verification on polling day, electronic results transmission, publication of voter information through digital portals, and post-election data retention or disposal practices.

- **Monitor political parties and private contractors**

  The Tool was structured to capture the data protection practices of political parties and candidates, particularly in relation to digital campaigning, bulk messaging, profiling, and engagement of third-party service providers. It also sought to document the roles played by security agencies and private technology vendors in accessing, processing, or influencing personal data during elections, including their compliance with data protection obligations and contractual accountability mechanisms.

- **Promote transparency in data collection, storage, and sharing**

  By documenting whether stakeholders publicly disclosed privacy policies, data protection impact assessments (DPIAs), data-sharing arrangements, and safeguards, the Tool aimed to promote transparency as a prerequisite for electoral trust. Particular attention was paid to whether voters were meaningfully informed about how their data were used and whether avenues existed for redress or inquiry.

- **Identify systemic gaps and propose reform recommendations**

  Beyond individual instances of compliance or non-compliance, the Tool was designed to identify recurring structural weaknesses within Uganda's electoral data governance framework. These findings were intended to inform evidence-based recommendations for regulatory reform, institutional practice, and future election preparedness, with a focus on preventing the normalization of harmful data practices across electoral cycles.

3. Methodology

The methodology adopted for the ***Data Protection Election Watch*** was designed to generate triangulated, verifiable evidence on electoral data practices through a combination of field-based observation, stakeholder engagement, documentary analysis, and technical assessment. The approach reflected the understanding that data protection risks in elections are rarely visible through a single source and require multi-layered investigation.

3.1 Deployment of the Data Protection Election Watch Tool

The Watch Tool was deployed throughout the ***2026 electoral cycle***, covering pre-election, election-day, and post-election phases. It comprised structured indicators and checklists aligned to statutory data protection obligations, electoral procedures, and emerging digital risks. Observations were recorded systematically to allow comparison across institutions, regions, and stages of the electoral process.

3.2 Primary Data Collection

Primary data were collected using multiple methods to capture both formal practices and lived realities:

- **Structured surveys** administered to election observers, political actors, and relevant stakeholders to document awareness, compliance practices, and observed data protection risks.
- **Key informant interviews** with electoral officials, regulators, civil society representatives, journalists, and technology practitioners to contextualize observed practices and clarify institutional decision-making.
- **Direct observation** at voter registration centres, polling stations, tallying environments, and campaign activities to assess how data protection principles were implemented or departed from in practice, particularly in the use of biometric voter verification kits and digital tools.

3.3 Secondary Data Review

Secondary data analysis formed a critical component of the methodology. This included systematic review of:

- Applicable laws, regulations, and statutory instruments governing elections, data protection, communications, and cybersecurity;
- Institutional policies such as privacy notices, data protection policies, and internal guidelines;
- Publicly accessible voter registers, digital display portals, and electoral information systems;
- Media reports, court filings, and prior election assessment reports relevant to data protection and electoral integrity.

This documentary review enabled verification of stakeholder claims and identification of discrepancies between formal commitments and operational realities.

3.4 Limitations and Constraints

This investigation faced several limitations. Access to detailed technical documentation, vendor contracts, and back-end system architectures was restricted, limiting independent verification of certain security and data-flow claims. Institutional non-disclosure and national security exemptions constrained transparency around sensitive areas such as results transmission systems and inter-agency data sharing. In addition, uneven digital access and fear of reprisal reduced the willingness of some stakeholders to participate fully or speak candidly.

Despite these constraints, the use of multiple data sources and cross-validation methods strengthened the reliability of the findings. While definitive technical verification was not always possible, the methodology was sufficient to identify systemic patterns, governance gaps, and priority reform areas.

4. Background & Context

4.1 Evolution of Data and Technology in Uganda's Elections

4.1.1 Introduction of BVVKs and progressive digitization (2016–2021–2026).3.1

Uganda's electoral administration was reported to have pursued a trajectory of progressive digitization over the preceding decade, with biometric technologies evolving from limited pilot applications into a central operational component of the electoral process. Biometric Voter Verification commonly referred to in official documentation and local reporting as BVV, BVVK, or BVVS was first introduced during the 2016 general elections as part of broader efforts to modernize voter identification and reduce electoral fraud[21]. The initial rollout in 2016 was, however, widely described as uneven. Technical failures and prolonged verification delays were reported at a number of polling stations, prompting questions regarding system reliability, logistical preparedness, and the adequacy of contingency measures[22].

Again in 2021 general elections, biometric voter verification devices were re-deployed on a nationwide scale[23]. While their use had become more normalized, the electoral cycle was marked by persistent reports of technical malfunctions, limited transparency around system specifications and operations, and political contestation over the credibility and integrity of biometric outputs[24]. These experiences were widely understood to have reinforced public scepticism toward the technology, even as the Electoral Commission (EC) continued to characterize biometric systems as essential infrastructure for ensuring credible, fraud-resistant elections.

In the lead-up to the 2026 electoral cycle, the EC was reported to have further institutionalized biometric systems as part of a broader digital public infrastructure underpinning electoral administration[25]. Public communications by the Commission referenced demonstrations, testing, and preparatory activities for an updated Biometric Voter Verification System, as well as training programmes for legislators, electoral staff, and polling officials on its operation.[26]. The Commission's 2025–2026 roadmap and parliamentary briefings consistently positioned the BVVK as a central operational tool for voter authentication, voter register extraction, and polling-day processes. As a result, the technical design of the devices, the identity and role of vendors, and the management of data flows associated with biometric verification were increasingly regarded as critical factors in any assessment of electoral integrity and data protection compliance.

By the time of the 2026 general elections, the BVVK was no longer considered an experimental or auxiliary tool. It was widely recognized as a core component of Uganda's electoral architecture, with its configuration including the categories of data collected, storage modalities, transmission pathways, audit mechanisms, and retention practices understood to have material implications for both the integrity of the electoral process and the privacy rights of millions of Ugandan voters.

4.1.2 Rise of digital campaigning, and political profiling

Alongside the digital transformation of Uganda's electoral administration, there was a documented escalation in the use of digital campaigning tactics, which substantially altered how political actors engaged with the electorate[27]. Beginning with the 2016 general elections, social media platforms such as Facebook, WhatsApp, and X were observed to have assumed a central role in political communication. Candidates increasingly relied on viral content, memes, live-streamed messaging, and targeted advertising to mobilize supporters and shape public narratives[28].

---

21 *Biometric Voter Verification System (BVVS)*, Electoral Commission of Uganda (19 Jan. 2016) (launch announcement and description of system purpose).
22 Vava, R. C. (2015). Biometric Voter Registration: Lessons from Ugandan Polls. Zimbabwe Election Support Network.
23 East African Standby Force Election Observation Mission to Uganda, Final Report, 2021, at p. 13
24 Unwanted Witness, "Biometric Machines Exasperate Voters in Uganda's 2021 Elections," (25 Jan. 2021)
25 Electoral Commission of Uganda, Statement by the Chairperson on the Progress of Implementation of Activities Under the Roadmap for General Elections 2026 (Dec. 17, 2025)
26 Workers from the Uganda Electoral Commission demonstrate how the Biometric Voter Verification Machines (BVVM) will be used in the forthcoming presidential polls at their offices in Kampala, Reuters (Dec. 17, 2025)
27 Unwanted Witness, Data Exploitation in Digital Political Campaigns and Its Implication on Electoral Democracy,
28 Iva N. Rugambwa & Maike Messerschmidt, *Tagging, Tweeting, Posting: Social Media and Politics in Uganda* 9–10 (Sept. 2015)

By the 2021 election cycle, these practices had evolved into more complex and coordinated digital ecosystems. Opposition actors most prominently Bobi Wine were widely reported to have leveraged social media platforms for grassroots mobilization, rapid information dissemination, and counter-narratives to state-aligned traditional media outlets[29]. These strategies were assessed as partially offsetting structural disadvantages in access to broadcast media. In response, the state adopted a range of regulatory and technical countermeasures, including the imposition of social media taxes and the implementation of platform restrictions and nationwide internet shutdowns[30]. These interventions were widely understood to have had a disproportionate impact on opposition campaigns and independent civic engagement.

In the period leading up to the 2026 general elections, digital campaigning practices were reported to have intensified further, including coordinated peer-to-peer voter mobilization efforts, where supporters were encouraged to call and directly engage fellow voters through phone conversations, alongside bulk SMS messaging for voter outreach. Political parties were increasingly associated with the use of data analytics and digital marketing techniques for voter profiling. These practices involved the aggregation of personal data drawn from multiple sources, including voter registers, social media interactions, mobile communication records, and third-party datasets, to construct detailed voter profiles based on demographics, geographic location, inferred political preferences, and online behavior.

Such profiling was reported to have enabled hyper-targeted political messaging, including tailored advertisements delivered through social media platforms and direct messaging channels. This approach reshaped electoral strategies by facilitating micro-campaigning in strategically significant constituencies and perceived battleground districts. Some candidates deployed automated systems to disseminate personalized reminders, mobilization messages, and campaign propaganda at scale, drawing on global digital campaigning practices adapted to Uganda's context of high mobile phone penetration, estimated to be 79.1 percent of the total population[31].

Civil society organizations and election observers assessed these developments as having mixed implications. On one hand, digital campaigning was seen to have lowered entry barriers for younger candidates and voters, expanded avenues for political participation, and enabled rapid mobilization. On the other hand, it was also reported to have exacerbated existing inequalities, as rural populations and communities with limited internet access or lower digital literacy were comparatively marginalized[32]. These dynamics underscored the uneven distribution of political visibility and influence within Uganda's increasingly data-driven electoral environment.

4.1.3 Surveillance, Data Misuse, and Disinformation Risks

Uganda's 2026 elections took place against a decade marked by internet shutdowns, platform blocking, and expanding online regulation, which had already heightened public concern about surveillance, information control, and electoral manipulation[33]. The legacy of the ***2016*** and ***2021*** shutdowns meant that new technological layers introduced in ***2026*** including upgraded biometric voter verification systems and centralized data integration were viewed with suspicion and fears of potential abuse.

Although the ***Data Protection and Privacy Act, 2019*** was in force, its operationalization during the electoral cycle exposed significant weaknesses. Civil society raised concerns about the absence of clear regulatory guidance on how data protection standards applied to voter registers, biometric data, and civic oversight[34]. At the same time, enforcement actions targeting individual actors occurred amid unresolved compliance gaps among major institutional data holders, creating perceptions of uneven application of the law[35].

The electoral environment was further complicated by the rise of AI-generated disinformation, including deepfake audio and video, amplified through coordinated digital networks and bulk messaging systems. When combined with periods of restricted connectivity and limited transparency, these dynamics intensified risks of manipulation, profiling, and narrative control.

By the close of the 2026 electoral cycle, privacy and electoral integrity had become deeply intertwined. Operational opacity, large-scale voter data processing, AI-enabled disinformation, and information-control measures collectively underscored the urgent need for stronger oversight and accountable digital governance in Uganda's elections.

---

29 Collaboration on International ICT Policy for East and Southern Africa (CIPESA), *How Online Narratives Played Out on Twitter Before, During and After the 2021 Uganda Elections* (Kampala: CIPESA, May 2021)
30 Levi Boxell & Zachary Steinert-Threlkeld, *Taxing dissent: The impact of a social media tax in Uganda*, (Oct. 2022)
31 DataReportal – Global Digital Insights, *Digital 2026: Uganda* (Nov. 8, 2025)
32 CIPESA, *How Online Narratives Played Out on Twitter*.
33 Unwanted Witness, *No Signal, No Voice: How Internet Shutdowns Undermined Uganda's 2026 Elections* (January 2026)
34 Unwanted Witness, *"Why Data Privacy Is the Missing Piece of Electoral Integrity,"* 27 January 2026
35 *Position Statement by Unwanted Witness*, January 2026

4.2 Electronic Architecture of the 2026 General Elections

4.2.1 Overview of the Digital Ecosystem

The 2026 General Elections were conducted within a dense and interdependent electronic architecture that extended far beyond polling-day technology. Electoral administration, national identity infrastructure, telecommunications networks, private technology vendors, global digital platforms, and third-party data processors operated as interconnected layers of a single governance ecosystem.

This architecture did not merely support elections, it structured how identity was verified, how data circulated, how results were aggregated, and how political narratives were shaped. Understanding the design, ownership, interoperability, and control of these systems is therefore essential to assessing risks to privacy, electoral integrity, inclusion, and democratic accountability.

4.2.2 The Legal Mandate and Compulsory Deployment of the Biometric Voter Verification System (BVVK)

The *2026* election marked a significant regulatory shift. Under ***Statutory Instrument No. 98 of 2025***[36], biometric voter verification was elevated from a discretionary tool to a mandatory requirement at all *50,739* polling stations nationwide. No ballot paper could be issued without biometric verification.

The Electoral Commission (EC) procured *109,142* Biometric Voter Verification Kits (BVVKs), each polling station receiving both a primary and backup device[37]. The system incorporated capacitive fingerprint readers (replacing earlier optical scanners), infrared facial recognition fallback, independent battery power, and district-level preloaded offline data.

This compulsory nationwide deployment followed documented failures in 2016 and 2021 including machine malfunctions, delays, and in 2021[38], system collapse following election-day internet shutdowns. The 2026 rollout was therefore presented as a technological upgrade and credibility safeguard.

4.2.3 Technical Architecture and Vendor Dependency

By 2026, the Biometric Voter Verification Kit (BVVK) had evolved from a relatively simple identity-check device into a more sophisticated verification node embedded within a broader electoral data system, incorporating embedded processors, biometric sensors for fingerprint and facial recognition, localized extracts of the voter database, internal storage with operational logging capabilities, ballot inventory scanning functions, and integrated result-form photography and digital archiving features.

The EC relied on external technology vendors for procurement, configuration, and maintenance[39]. However, detailed technical specifications including encryption standards, software versioning, backend access controls, audit log immutability, and vendor-level administrative privileges were not publicly disclosed.

This opacity generated recurring concerns about vendor lock-in, dependence on proprietary systems, limited opportunities for independent technical auditing, and the concentration of administrative access within a narrow set of actors. From a data protection perspective, it also left unresolved critical questions regarding the scope of biometric data stored on the devices, applicable retention timelines, synchronization protocols with central systems, the conditions under which data could be extracted or subjected to forensic access, and the adequacy of chain-of-custody controls governing such processes.

Although the EC emphasized that voter identity data and ballot data were stored separately, the absence of published data protection impact assessments or independent audits limited external verification of these assurances.

36 The Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, SI No. 98 of 2025

37 Statement by the Chairperson, Electoral Commission on the Progress of Implementation of Activities Under the Roadmap for General Elections 2026 (Nov. 26, 2025)

38 Unwanted Witness, "Biometric Machines Exasperate Voters in Uganda's 2021 Elections"

39 Smartmatic International press release, "Uganda Deploys Biometric Technology to Improve General Election Transparency,"

4.2.4 NIN–Voter Register Integration

A defining structural feature of the *2026* electoral architecture was the operational integration of the *National Identification Number (NIN)* system into voter registration processes[40]. The Electoral Commission confirmed that updates to the voter register relied on data extracted from *National Identification and Registration Authority (NIRA)*, validation through the *National Identification Number (NIN)*, and the use of shared registration kits, with the *NIN* serving as a central identifier to verify citizenship status, assign polling stations, validate voter particulars, and update and cleanse the voters' roll.

This convergence represents a significant consolidation of civil registration and electoral administration, effectively transforming the *National Identification Number (NIN)* into a gateway credential for political participation. Although publicly framed as a mechanism to eliminate duplicate registrations and enhance the accuracy of the voters' roll, the integration introduced structural privacy and governance risks, including function creep through the repurposing of civil identity data for electoral use, cascading exclusion where inaccuracies in the national identity database directly affect voter eligibility, increased centralization that diminishes the separation between identity systems and civic participation, and heightened breach impact whereby a compromise of either system carries direct electoral consequences.

In a political context shaped by prior allegations of surveillance and contested elections, the linkage intensified fears of cross-dataset profiling including potential correlation with telecommunications metadata, taxation records, or geolocation information.

4.2.5 Digital Voter Register Portals and Systemic Voter Data Governance Risks

During the 2026 electoral cycle, the *Electoral Commission (EC)* expanded the use of digital voter register display portals to enable citizens to verify their registration and voter location details online[41]. These platforms were designed to enhance accessibility and administrative efficiency within an increasingly digitized electoral framework. In practice, however, they processed and exposed sensitive personal data including names, polling locations, registration numbers, and photographs at scale.

The subsequent emergence of the FANON application provides an instructive case study in how such vulnerabilities may translate into real-world data governance failures[42]. FANON appeared in late 2025 as a civic-tech voter-education and voter-locator platform that allowed users to search voter registration and polling-station details, reportedly enabled name-based searches of voter information with fewer access barriers than the official EC portal. Although its founders claimed that data was compiled from publicly displayed polling station registers, the scale and functionality of the platform coupled with the EC's decision to request police investigation into possible unauthorized digital access to its systems, raise credible concerns that centralized or semi-centralized digital sources may have been accessed, whether through scraping, insider leakage, insecure portals, or systemic weaknesses.

This episode highlights a deeper institutional risk: when large-scale voter data is digitized without robust authentication controls, audit logging, independent security testing, and strict access governance, the boundary between *"public display"* and *"bulk extraction"* becomes dangerously thin. Even if individual records are lawfully viewable for verification purposes, the automated aggregation of millions of entries transforms the character of the dataset into a powerful political profiling resource.

In the context of competitive elections, voter register data can be cross-referenced with commercially available datasets, social media profiles, geospatial mapping tools, or demographic analytics to construct inferred political affiliations, map perceived opposition strongholds, and design targeted political messaging. Such downstream risks are amplified where there is no publicly disclosed ***Data Protection Impact Assessment (DPIA)***, no independent security audit, and no transparent explanation of portal safeguards.

The FANON case further exposed weaknesses in regulatory coordination and data stewardship. The response prioritized communications enforcement and criminal investigation, while the ***Personal Data Protection Office (PDPO)*** the authority mandated to oversee lawful processing, investigate breaches, and regulate cross-border transfers, was not visibly central in the initial enforcement sequence. At the same time, concerns were raised regarding whether core institutional data holders themselves fully complied with registration and transparency obligations under the *Data Protection and Privacy Act*.

---

40 Electoral Commission, *Press Statement on the Extension of the General Update of the National Voters Register* (10 Feb. 2025)

41 Puzzle of the Electoral Commission voters' register, Daily Monitor (28 Nov 2025)

42 Electoral Commission, Statement by the Chairperson, Electoral Commission on the Progress of Implementation of Activities Under the Roadmap for General Elections 2026 (Dec. 31, 2025)

The expansion of digital voter portals and the *FANON* incident illustrate that Uganda's *2026* electoral digitalization occurred within a fragmented governance environment. Innovation outpaced oversight; enforcement appeared selective; and foundational safeguards, including authentication robustness, scraping prevention, hosting transparency, cross-border transfer controls, and independent auditing were not publicly demonstrated.

Accordingly, the issue is not simply the existence of digital voter portals, but the absence of verifiable, rights-centered data governance architecture surrounding them. Without demonstrable security controls, regulatory coherence, and transparent compliance with data protection standards, digital voter verification systems risk becoming vectors of large-scale data exposure rather than instruments of democratic trust.

4.2.6 Electronic Results Management and Tallying

Although the formal declaration of results remained anchored in manual tallying procedures, the *2026* elections were designed to rely significantly on digital tools for polling station result capture, scanning of declaration forms, electronic ballot inventory verification, and internal transmission of data to tally centres. However, widespread breakdowns of biometric machines reportedly linked in part to connectivity disruptions and broader technical failures, meant that several of these processes could not be executed as intended. In many instances, officials were forced to revert to improvised manual workarounds, undermining the consistency, traceability, and auditability that digitization was meant to enhance.

These operational disruptions not only exposed vulnerabilities in backend access controls, data reconciliation procedures, and audit-log governance, but also created uncertainty about whether intended safeguards were ever activated or verifiable. In a context already marked by fragile institutional trust, the combination of machine failures and the absence of detailed public documentation on system architecture and transmission protocols amplified post-election suspicion, dispute, and contestation over the credibility of the results.

4.2.7 Use of Online Platforms

Beyond formal electoral systems, global digital platforms profoundly shaped electoral competition during the *2026* cycle. Platforms such as Meta (Facebook, Instagram, and WhatsApp), TikTok, X, and YouTube operated simultaneously as campaign venues, fundraising channels, narrative amplification tools, and vectors for disinformation. Encrypted services, particularly WhatsApp, enabled the rapid circulation of coordinated political messaging with limited visibility or traceability, while algorithm-driven feeds prioritized emotionally charged and polarizing content, frequently displacing verified or contextual information. At the same time, platform-level governance decisions including content moderation policies, political advertising transparency rules, responses to state takedown or throttling requests, and enforcement of community standards, materially shaped Uganda's electoral information environment, often without meaningful local accountability, regulatory clarity, or judicial oversight.

4.2.8 Architecture as Power

The 2026 electronic electoral architecture functioned as an integrated and interdependent system in which biometric identity technologies, national identity infrastructure, electronic tallying mechanisms, digital communication platforms, and private data intermediaries operated in concert. Control over this architecture, including its design choices, auditability standards, data access permissions, interoperability arrangements, and regulatory oversight, was closely intertwined with the exercise of political power. Accordingly, this post-election investigation assesses not only the technical performance of these systems, but also how their configuration redistributed visibility, vulnerability, influence, and control across Ugandan society, shaping who could participate, who could be profiled, who could be excluded, and ultimately how electoral legitimacy was constructed and contested.

4.3 Lessons from Past Elections

An examination of Uganda's recent electoral history indicated that many of the risks observed during the 2026 General Elections were neither novel nor unforeseeable. Instead, they reflected unresolved structural and governance challenges that had manifested across successive electoral cycles, particularly in 2016 and 2021. These earlier experiences offered critical lessons regarding the deployment of electoral technologies, the governance of voter data, and the state's approach to digital political participation.

4.3.1 2016 Elections: Biometric Failures and Legal Vacuum

The 2016 General Elections marked Uganda's first nationwide deployment of biometric voter verification technologies[43]. These systems were introduced as part of an electoral modernization agenda, intended to curb multiple voting, improve the accuracy of the voter register, and strengthen public confidence in electoral outcomes. However, their rollout took

43 Electoral Commission of Uganda, Press Statement on Preparations for 2016 General Elections (27 Jan. 2016)

place at a time when Uganda had no data protection or privacy law governing the collection, use, storage, or sharing of personal data.

Post-election assessments and observer reports documented widespread operational challenges[44]. Biometric voter verification kits malfunctioned at numerous polling stations, with failures attributed to battery depletion, configuration errors, and difficulties in capturing or reading fingerprints particularly for elderly voters and manual laborers[45]. In many cases, polling officials reverted to manual identification procedures, creating inconsistencies in verification and weakening procedural integrity. These failures led to delays, voter frustration, and uneven application of safeguards, exposing deficiencies in planning, training, and technical support.

Beyond these operational issues, the 2016 elections revealed deep structural weaknesses in data governance. In the absence of a legal framework, there were no binding standards regulating how voter data, especially biometric identifiers was to be collected, secured, retained, shared, or eventually destroyed. Voters had no enforceable rights over their personal information, and institutions handling sensitive data operated without clear legal limits or accountability mechanisms.

Transparency was notably limited. There was little publicly available information about the technical architecture of the biometric systems, the identity and contractual obligations of technology vendors, where voter data was stored, or who had access to it. Without statutory duties of disclosure or independent oversight, the management of voter data remained largely opaque, with critical decisions concentrated in a small number of institutional and commercial actors.

This legal vacuum extended beyond the Electoral Commission to other stakeholders involved in the electoral ecosystem. Political parties, telecommunications companies, and third-party service providers were not subject to clear data protection obligations. As a result, the handling of personal data during the election period varied widely and was largely governed by informal practices rather than enforceable rules.

One of the most visible manifestations of this gap was the use of mass political robocalls and targeted voter messaging during the 2016 campaign, particularly by the incumbent National Resistance Movement (NRM) candidate[46]. Large numbers of voters reported receiving automated calls and messages directed at specific demographic or geographic segments. At the time, there was no public clarity on how political actors obtained the underlying contact data, nor were there legal requirements compelling disclosure of data sources, consent mechanisms, or data-sharing arrangements.

Questions were raised by civil society and the media about the apparent use of telecommunications subscriber data, including whether datasets held by major telecom operators such as MTN Uganda were accessed, shared, or repurposed for political campaigning. In the absence of data protection legislation, there were no statutory prohibitions clearly regulating secondary use of subscriber data, no consent standards for political messaging, and no independent authority empowered to investigate or sanction misuse. As a result, concerns about potential data exploitation remained unresolved and largely unexamined.

Importantly, these practices were not framed at the time as data protection violations. Instead, they were treated as campaign tactics, regulatory grey areas, or matters of political ethics. The lack of a rights-based data protection framework meant that voters had no legal avenue to challenge how their personal information was being used, nor could institutions be compelled to account for data flows between state bodies, private companies, and political actors.

The 2016 elections therefore represented an early warning. They demonstrated how the rapid digitization of electoral processes, biometric registration, electronic verification, and data-driven campaigning can dramatically expand the collection and circulation of personal data in the absence of legal safeguards. Operational failures exposed technical weaknesses, but the deeper risk lay in the normalization of large-scale data extraction and political profiling without consent, transparency, or accountability.

In hindsight, the events of 2016 underscore how Uganda entered the era of digital elections before establishing the legal and institutional foundations necessary to protect voter data. This legacy shaped subsequent electoral cycles, in which more advanced technologies were layered onto a system still grappling with unresolved questions about data ownership, control, and the balance of power between the state, private actors, and citizens.

44 Zimbabwe Election Support Network, Lessons from Uganda Biometric Voter Registration
45 African Union Election Observation Mission (AUEOM), Preliminary Findings on the 18 February 2016 General Elections in Uganda (20 February 2016, Kampala)
46 Unwanted Witness Uganda, Press Statement on MTN Uganda Sharing Subscribers' Data with Ruling NRM Party for Campaigns

4.3.2 2021 Elections: Legal Framework Without Enforcement

By the time of Uganda's 2021 General Elections, the country had formally entered the era of digital and technology-enabled elections. Unlike in 2016, this transition occurred against the backdrop of a newly enacted ***Data Protection and Privacy Act, 2019***[47], signaling an official recognition of privacy and data protection as fundamental rights and a matter of public policy and rights. However, this legal recognition remained largely theoretical. At the time of the elections, the enforcement architecture of the Act was not yet operational, with no fully established and functional data protection regulator capable of oversight, guidance, or enforcement.

This regulatory gap had significant consequences. Although data protection obligations existed on paper, there was no institutional authority actively enforcing compliance, issuing binding guidance, conducting audits, or responding to violations. In practice, this meant that the rapid expansion of data-intensive electoral technologies and digital campaigning unfolded in an environment of legal formality without regulatory restraint.

In parallel, Uganda undertook deliberate legislative reforms to entrench the use of technology in the management of elections. Through the Electoral Commission (Amendment) Act, 2020, Parliament amended ***Section 12 of the Electoral Commission Act (Cap 140)*** to explicitly authorize technological adoption by the Electoral Commission[48]. Newly introduced ***subsections (1a) and (1d)*** empowered the Commission to adopt technology in election management, establish electronic display systems at tallying centres, and prescribe by statutory instrument, the manner in which such technology would be used.

Further amendments to the ***Presidential Elections Act, 2005*** introduced electronic transmission of results by returning officers, including return forms, tally sheets, and declarations of results, while requiring copies to be shared with political parties and candidates alongside physical delivery of hard copies[49]. Collectively, these reforms marked a decisive legal shift toward digitized electoral administration.

These amendments were widely interpreted as a response to the Supreme Court's fourth recommendation in ***Mbabazi v. Museveni***, which called for legislation to regulate the use of technology in elections. However, while the reforms succeeded in authorizing technology, they fell short of regulating its data protection implications and safeguarding people's rights. The laws focused on functionality and efficiency, how technology could be used rather than on how voter data generated, transmitted, or processed through these systems would be protected, governed, or constrained.

Against this backdrop, the 2021 elections were conducted under the banner of *"scientific elections,"* a model justified on public health grounds but which drastically curtailed physical campaigning[50]. Political competition shifted decisively into digital and broadcast spaces. Social media platforms, bulk SMS messaging, televised addresses, and online influencer networks became central to electoral mobilization. Political actors increasingly relied on data-driven strategies, including targeted messaging based on geography, language, demographics, and inferred political affiliation.

At the same time, the election period was marked by severe information controls, including platform blocking and a near-total internet shutdown. These measures limited independent observation, media reporting, civic engagement, and real-time verification, while disproportionately affecting opposition actors and civil society organizations dependent on digital tools.

The combined effect of these developments exposed a profound regulatory imbalance. On one hand, electoral law had been amended to legitimize the extensive use of digital technologies in both election administration and political campaigning. On the other, the absence of an operational data protection regulator meant there was no effective oversight of how voter data was sourced, processed, shared, or repurposed. Consent mechanisms were largely absent in practice, transparency obligations remained unenforced, and voters had little ability to understand, let alone challenge how their personal data was being used in political contexts.

In effect, the 2021 elections normalized a system in which technology was legally embedded in electoral processes, while data protection remained institutionally unenforced. The result was not merely a gap in compliance, but a structural condition in which data-driven political power expanded faster than the safeguards meant to protect citizens from its misuse. This imbalance laid critical groundwork for the tensions that would later emerge as data protection law began to be enforced without first having been embedded through consistent regulatory practice.

47 Republic of Uganda. *Data Protection and Privacy Act, 2019.* Act No. 9 of 2019
48 Advocates for Law and Policy – East Africa, Electoral Law Reforms in Uganda: 2021 Elections (23 July 2020)
49 ALP East Africa, *Electoral Law Reforms in Uganda as Country Prepares for 2021 Elections*
50 Centre for Basic Research, Preparations for Uganda's 2021 Scientific Elections

4.3.3 Recurring Governance Gaps

As observed in 2016 and 2021 electoral cycles, and persisting into the lead-up to the 2026 elections, a set of recurring governance gaps became increasingly evident. These gaps did not remain static; rather, they evolved alongside Uganda's gradual adoption of data protection law, revealing a pattern in which legal recognition advanced faster than institutional enforcement and democratic safeguards.

A central and persistent gap concerned meaningful consent. In both 2016 and 2021, biometric identifiers, voter contact details, and digital traces were routinely collected and processed as matters of administrative necessity or political expediency. Voters were rarely informed about how their data would be used beyond immediate electoral purposes, how long it would be retained, or whether it would be shared with third parties. Even after the enactment of the ***Data Protection and Privacy Act in 2019***, consent remained largely nominal in practice, particularly in electoral contexts where participation was functionally compulsory and alternatives were limited.

Transparency deficits similarly endured across electoral cycles. Critical components of the electoral technology ecosystem including procurement processes, vendor contracts, system architectures, data hosting arrangements, and inter-agency data flows, remained largely shielded from public scrutiny. In 2016, this opacity reflected the absence of any legal disclosure obligations. By 2021, while legal obligations formally existed, they were not operationalized through binding guidance or active oversight. As Uganda moved towards the 2026 elections, this lack of transparency took on greater significance: technologies had become more embedded, data flows more complex, yet public visibility into how electoral data systems functioned remained limited.

Cybersecurity vulnerabilities were not merely theoretical concerns within Uganda's 2026 electoral cycle; they materialized in ways that exposed structural weaknesses in the protection of the National Voters' Register. As already illustrated through the FANON incident discussed earlier in this report, the appearance of a third-party platform capable of enabling large-scale, name-based searches of voter data, followed by the Electoral Commission's decision to request police investigation into suspected unauthorized access to its systems, signaled credible concerns that centralized or semi-centralized digital repositories may have been compromised[51]. The scale and functionality of the exposed data rendered explanations of purely manual compilation implausible, pointing instead to possible scraping, insecure portal configurations, insider leakage, or other systemic vulnerabilities within the Commission's digital architecture. Despite the heightened sensitivity of biometric and voter-identification datasets, there was limited public evidence of prior independent cybersecurity audits, penetration testing, or clearly articulated breach notification protocols. The regulatory response further revealed fragmented oversight, with enforcement measures focusing on criminal investigation and communications takedown, while the statutory data protection regulator was not visibly central to the initial response. These developments underscored an electoral data environment in which unauthorized access risks were plausible, institutional preparedness was opaque, and accountability mechanisms remained uneven, thereby amplifying public uncertainty regarding the security, control, and lawful stewardship of voter data.

Enforcement emerged as the most consequential cross-cutting weakness. Although the **Data Protection and Privacy Act, 2019** came into force prior to the 2021 elections, its enforcement mechanisms were not yet operational. The **Data Protection and Privacy Regulations** were only gazetted in ***March 2021***[52], and the **Personal Data Protection Office (PDPO)** was officially operationalized in August 2021 after the elections had already taken place[53]. As a result, the 2021 elections occurred in a transitional phase where data protection obligations existed in law but not in practice.

This gap had lasting implications. The absence of regulatory guidance from the ***PDPO*** meant that key actors public authorities, political parties, and private service providers operated without clear, authoritative interpretations of how data protection principles applied to electoral processes. Compliance was fragmented and largely discretionary, shaped more by institutional power and political context than by enforceable standards.

As Uganda entered the 2026 electoral cycle, these longstanding governance gaps remained largely unresolved. Although the ***Personal Data Protection Office (PDPO)*** was operational, no comprehensive electoral data protection guidelines had been issued to clarify how the Data Protection and Privacy Act applied to voter registers, biometric systems, or digital campaigning practices. Moreover, despite being one of the largest custodians of sensitive personal and biometric data in the country, the Electoral Commission remained unregistered with the ***PDPO*** and without a publicly accessible privacy policy throughout the pre-election and election period, even after being formally advised to comply by Unwanted Witness in ***March 2025***.

---

51 Uganda Electoral Commission, *Statement by the EC Chairperson – General Election Updates* (31 Dec. 2025)
52 See *Data protection laws in Uganda*, DLA Piper
53 RSM Uganda, *The Data Protection and Privacy Act, 2019* (27 Jan 2022) (noting establishment and mandate of the Personal Data Protection Office under the Act)

It was only after the ***January 2026*** general elections that the Commission proceeded to register with the ***PDPO*** on ***21 January 2026***, thereby attaining active status[54]. While this post-election registration marked a formal step toward compliance, its timing underscores a critical institutional lapse: core data protection obligations were not embedded at the point when electoral data processing was at its most intensive and consequential. The cumulative effect of these gaps is a data protection regime that exists in law but remains unevenly institutionalized in practice. Consent mechanisms remain weak, transparency partial, cybersecurity assurances opaque, and enforcement inconsistent. In electoral contexts, where data-intensive technologies intersect with political competition and state power, such weaknesses risk transforming data protection law from a proactive democratic safeguard into a reactive instrument, applied after harm has occurred rather than systematically preventing it.

For democracy, the implications are significant. Elections increasingly depend on digital systems and data-driven practices, yet voters remain largely excluded from meaningful control over how their personal information is used. Without consistent enforcement, clear guidance, and institutional compliance particularly by electoral authorities themselves, data protection cannot function as a trust-building mechanism. Instead, it risks deepening asymmetries of power between the state, political actors, private companies, and citizens, with long-term consequences for electoral legitimacy and democratic accountability.

4.3.4 Implications for the 2026 elections

The trajectories of the 2016 and 2021 elections reveal a consistent pattern in which technological adoption repeatedly outpaced governance, oversight, and rights protection. What began in 2016 as biometric experimentation in a legal vacuum evolved by 2021 into a formally regulated but institutionally unenforced data protection environment. By the time Uganda entered the 2026 electoral cycle, these unresolved gaps had not narrowed; instead, they had hardened into structural features of the electoral system.

The 2016 elections exposed the risks of deploying biometric and data-intensive technologies without any legal safeguards, normalizing large-scale data extraction without consent, transparency, or accountability. The 2021 elections, conducted after the enactment of the ***Data Protection and Privacy Act*** but before the operationalization of its enforcement machinery, demonstrated how legal recognition without regulatory capacity could legitimize expanded data use while leaving voters unprotected in practice. Electoral laws were amended to authorize technology, electronic displays, and electronic transmission of results, yet the governance of the data flowing through these systems remained largely unaddressed.

As Uganda moved towards the 2026 elections, the cumulative effect of these earlier failures became more pronounced. Electoral processes were characterized by deeper biometric integration, expanded interlinkages between voter databases and other state systems, and the emergence of more sophisticated data-driven political strategies, including algorithmic amplification and AI-assisted political messaging. However, the foundational questions raised in earlier cycles who controls voter data, under what legal basis, with what safeguards, and subject to whose oversight, remained unresolved.

Crucially, the post-2021 period marked a turning point in how data protection law was applied. With the ***Data Protection and Privacy Regulations*** gazetted in ***March 2021*** and the ***Personal Data Protection Office*** operationalized in ***August 2021***, enforcement capacity formally existed as the country approached the 2026 elections. Yet instead of being embedded through consistent guidance, institutional compliance, and preventative regulation, data protection law began to surface primarily through selective criminal enforcement.

This shift had significant implications. Rather than being used to compel compliance by major data-holding institutions most notably the ***Electoral Commission***, which remained unregistered with the PDPO and without a publicly accessible privacy policy even after formal advisories, data protection law was increasingly invoked against individual civic actors and human rights defenders. In effect, the law designed to protect citizens' privacy was repurposed as a mechanism to police scrutiny of electoral data, while institutions controlling vast repositories of sensitive personal and biometric information continued to operate outside the core compliance requirements of the same statute.

The prosecution of human rights defenders under ***Section 35 of the Data Protection and Privacy Act*** illustrated this inversion[55]. Actions that had historically formed part of electoral transparency, verification, and public-interest oversight were reframed through a criminal lens, even as the institutional custodians of voter data benefitted from their own non-compliance. This dynamic produced a profound rule-of-law asymmetry: the Electoral Commission, despite failing to meet basic statutory obligations such as registration and publication of a privacy policy, could invoke the Act as a shield, while those scrutinizing electoral integrity were exposed to its punitive edge.

54 PDPO, *PDPO-202601-9760: ELECTORAL COMMISSION – Registered Data Controller* (21 January 2026)
55 Amnesty International, *Uganda 2025: Summary of human rights concerns* (Report, AFR59/0598/2026)

In this context, the 2026 elections did not merely inherit unresolved data protection challenges from previous cycles; they exposed the consequences of failing to address them. Data protection law, insufficiently embedded through guidance and compliance, became vulnerable to instrumentalization. Rather than functioning as a trust-building framework that constrained power and protected voter autonomy, it risked operating as a selective tool of control, chilling oversight and deterring legitimate human rights work.

The post-election record therefore suggests that many of the data protection, privacy, and power-related concerns observed in the ***2026*** elections were not anomalies of a single cycle. They were the foreseeable outcome of lessons from ***2016*** and ***2021*** that had been acknowledged in law but not absorbed into institutional practice. Without recalibrating enforcement toward systemic compliance, transparency, and accountability particularly by electoral authorities themselves, data protection risks entrenching, rather than correcting, the structural imbalances that undermine electoral legitimacy and democratic accountability in Uganda.

5. Legal and Regulatory Framework

Election management directly involves several human rights norms under the *International Covenant on Civil and Political Rights (ICCPR),* which apply both online and offline, and guide whether on what conditions technology should be used and regulated. Specifically, the right to privacy is guaranteed under Article 17 of the ICCPR, is fundamental in a democratic society and increasingly important in a data driven world. The right to privacy incorporates the principles of data protection.

Uganda's 2026 General Elections were conducted within a complex but uneven legal and regulatory environment governing data protection, electoral administration, political activity, and digital technologies. While significant statutory developments have occurred over the past decade particularly with the adoption of the data protection law and the formal use of election technologies during elections, there lack of comprehensive regulatory coherence, consistent enforcement, or safeguards tailored to the realities of digital and data-driven elections.

5.1 Data Protection and Privacy Act, 2019 and Regulations, 2021

The *Data Protection and Privacy Act, 2019 (Chapter 97)* establishes Uganda's primary statutory framework governing the collection, processing, storage, disclosure, and cross-border transfer of personal data. Under Section 1, the Act applies to all persons, institutions, and public bodies collecting or processing personal data within Uganda, as well as to entities outside Uganda processing data relating to Ugandan citizens. Section 3 sets out the core principles of data protection, requiring that personal data be processed fairly and lawfully; collected for specific, explicit and legitimate purposes; limited to what is adequate and not excessive (minimality); retained only for authorized periods; kept accurate and up to date; secured against foreseeable risks; and handled transparently with accountability to the data subject.

Part III of the Act regulates lawful collection and processing, including the requirement of prior consent under Section 7, subject to limited statutory exceptions such as performance of a public duty, national security, or law enforcement purposes. Section 9 imposes restrictions on the processing of special personal data, including financial information and political opinions, while Section 19 governs cross-border data transfers by requiring either adequate protection in the receiving jurisdiction or the data subject's consent. Part IV further mandates the adoption of appropriate technical and organizational security measures (Section 20) and obliges data controllers to notify the Authority of data security breaches (Section 23). The Act also creates criminal offences for unlawful obtaining, disclosure, destruction, alteration, or sale of personal data (sections 35-37), reinforcing its enforcement architecture.

The Data Protection and Privacy Regulations, 2021 operationalize these statutory obligations. They elaborate the institutional role of the Personal Data Protection Office (PDPO), establish the Data Protection Register, and require mandatory registration of data collectors, processors, and controllers (Regulations 15–19). They further require disclosure of processing purposes, categories of personal data, data retention periods, security measures, and cross-border transfer details at the point of registration. Regulation 12 introduces the requirement for Data Protection Impact Assessments where processing poses high risks to the rights and freedoms of individuals, while Regulation 30 details conditions for processing personal data outside Uganda, including adequacy and consent requirements. Regulation 31 requires adherence to generally accepted information security practices and procedures, reinforcing the security obligations under Section 20 of the Act.

In the electoral context, the Act and Regulations clearly apply to voter registers, biometric identifiers, identification numbers, and associated digital records, all of which fall within the statutory definition of *"personal data."* However, the practical application of these provisions to electoral transparency mechanisms, voter verification systems, political campaigning technologies, and election observation remains uneven. While Sections 7(2) and 17(3) permit certain processing activities in the performance of public duties or for law enforcement purposes, the absence of detailed sector-specific electoral guidance has created interpretive ambiguity. Consequently, the framework operates as a comprehensive rights-protective regime in law, but in practice has generated uncertainty regarding how data protection obligations intersect with constitutional mandates of electoral transparency, public participation, and democratic accountability.

5.2 Electoral Commission Act (Cap 140): Governance and Oversight

The Electoral Commission Act, Cap 140[56] establishes the Electoral Commission as a corporate body (Section 2) and defines its constitutional mandate, powers, and functions in relation to the conduct of elections. Under Part III, Section 18, *the Commission is expressly mandated to "compile, maintain and update, on a continuing basis, a national voters register,"* including constituency and polling station rolls. Sections 23–25 further regulate custody of the register, public inspec-

56 Electoral Commission Act, **Cap. 140** (Uganda) (as amended)

tion, display of rolls, and objection procedures, embedding principles of transparency and public scrutiny within an analogue administrative framework.

While the Act grants the Commission broad operational authority including powers to ensure secure electoral conditions *(Section 12(1)(f))*, accredit observers *(Section 16)*, resolve complaints *(Section 15),* and exercise special adaptive powers during elections (Section 50), it does not contain detailed provisions governing digital data management, cybersecurity safeguards, system audits, or technological accountability. Section 23(2) allows the voters register to be kept *"in such form as may be prescribed by the commission by statutory instrument,"* thereby permitting technological formats, but without prescribing substantive standards for data governance, integrity verification, encryption, access control, breach notification, or independent technical oversight.

Moreover, although Section 13 affirms the independence of the Commission and *Section 49* provides immunity for actions taken in good faith, the Act does not impose explicit statutory obligations regarding publication of privacy policies, mandatory cybersecurity audits, algorithmic transparency, or data protection impact assessments in relation to digital electoral systems. Nor does it establish an external supervisory mechanism specifically tasked with reviewing the technological infrastructure underpinning voter registration, biometric systems, or electronic results management.

As a result, while the Act robustly empowers the Commission to control and manage the national voters register and broader electoral process, it was primarily designed within a pre-digital administrative paradigm. The absence of express digital governance standards has created a regulatory gap: the Commission exercises comprehensive authority over voter data and electoral technologies, yet operates without clearly codified statutory requirements concerning digital security auditing, system transparency, or structured technological oversight. In an increasingly digitized electoral environment, this gap has significant implications for accountability, public trust, and the integrity of data-driven election administration.

5.3 Biometric Voter Verification, Regulations, 2025

The Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, 2025[57] constitute the most direct statutory instrument governing the compulsory deployment of biometric technology in Uganda's elections. Made under *Section 12(2), (4) and (5) of the Electoral Commission Act,* the Regulations mandate the use of the Biometric Voter Verification System (BVVS) at all polling stations for presidential, parliamentary, and local council elections *(Regulations 2 and 4). Regulation 4(1)* requires that no ballot paper be issued until a voter's identity has been verified through the biometric system, thereby elevating biometric verification from a discretionary tool to a binding procedural requirement.

Regulation 5 prescribes detailed operational steps for presiding officers, including scanning national identification cards or voter location slips, fingerprint verification through the biometric voter verification kit, fallback facial recognition where fingerprint verification fails, and referral of voters identified at different polling stations. Regulation 6 further extends the use of the biometric kit beyond identity verification to electronic ballot inventory management, including scanning unique ballot codes before and after polling and capturing image copies of signed declaration of results forms for storage on the device. Regulation 7 creates offences for failure to use the system as prescribed or for unlawful interference, imposing fines or imprisonment and barring convicted persons from future engagement with the Commission.

While the Regulations clearly standardize the functional and procedural use of biometric verification technology, they remain largely silent on substantive data protection safeguards. They do not specify biometric data retention periods, deletion protocols, encryption standards, access control hierarchies, independent security audits, or mechanisms for transparency and external oversight of the data generated and stored on the kits. Nor do they articulate safeguards governing post-election storage, transfer, or synchronization of biometric logs and image records captured under *Regulation 6.* Consequently, although the Regulations entrench biometric verification as a mandatory element of electoral administration, they normalize the routine processing of sensitive biometric data without embedding explicit privacy-by-design, data-minimization, or accountability-by-design principles within the regulatory framework governing electoral technologies.

5.4 Structural Gaps in Uganda's Electoral Data Protection Framework

Notwithstanding the existence of the *Data Protection and Privacy Act and its Regulations, the Electoral Commission Act,* and the *2025 Biometric Verification Regulations,* the current framework leaves several critical governance gaps insufficiently addressed. These omissions are particularly consequential in a data-intensive electoral environment.

57 Electoral Commission, *Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, 2025* (Uganda)

5.4.1 Absence of Electoral Data Governance Framework

Uganda's current legal and regulatory architecture does not provide a comprehensive, sector-specific framework clarifying how data protection principles apply across the full electoral cycle, nor does it impose structured obligations to document and map electoral data flows. While the Data Protection and Privacy Act establishes general principles of lawful processing, purpose limitation, transparency, and accountability, there is no dedicated electoral guidance translating these principles into operational standards for voter registration, register inspection, biometric verification, political campaigning, results transmission, observer access, and post-election data retention. As a result, key actors including the *Electoral Commission, political parties, civil society organizations, contractors, and technology vendors* operate without harmonized, election-specific compliance benchmarks. Compounding this gap is the absence of a mandatory requirement for the Electoral Commission to develop and publicly maintain a comprehensive data inventory detailing the categories of voter data collected, the systems in which they are stored, access control hierarchies, lawful bases for processing, data-sharing arrangements, retention schedules, and cross-border transfers. Without structured data mapping across biometric verification kits, digital voter display portals, results management systems, and inter-agency integrations, accountability remains fragmented and data flows opaque. The combined absence of electoral-specific guidance and systematic data inventory obligations weakens transparency, obscures institutional responsibility, and limits the capacity of regulators, courts, observers, and voters to meaningfully scrutinize how electoral data are governed in practice.

5.4.2 Lack of Mandatory Data Protection Impact Assessments (DPIAs) Disclosure

Although the *Data Protection and Privacy Regulations, 2021 contemplate Data Protection Impact Assessments (DPIAs)* for high-risk processing, the framework's effectiveness is undermined by the absence of a publicly established list of processing operations that automatically trigger the *DPIA* requirement, as mandated under *Regulation 12(3)*. The law expressly requires the regulator to establish and make public such a list, thereby providing clarity and predictability to data controllers and processors. In the absence of this regulatory instrument, there is no explicit, publicly binding designation that core electoral technologies including biometric voter verification systems, digital voter portals, large-scale voter databases, and results transmission platforms, constitute high-risk processing subject to mandatory *DPIAs*. Given the scale, sensitivity, and democratic implications of biometric and political data processing during elections, the failure to operationalize and publish this list creates regulatory opacity, weakens preventive oversight, and leaves *DPIA* compliance dependent on discretionary interpretation rather than structured legal obligation.

5.4.3 Interoperability without Data-Sharing Framework

The operational integration of the *National Identification and Registration Authority (NIRA)* and the *Electoral Commission (EC)* in the 2025/2026 electoral cycle has exposed a structural gap in Uganda's election data protection framework: the absence of a clearly codified, publicly accessible inter-agency data-sharing and governance regime. As reflected in the documented cooperation between NIRA and the EC where the National Identification Number (NIN) system was embedded into voter verification, polling station assignment, and voter roll updates, and where NIRA registration kits were deployed within electoral processes, the foundational civil identity database and the electoral register effectively operated as a unified data ecosystem[58]. Yet this deep interoperability is not matched by a dedicated statutory instrument or binding protocol detailing purpose limitation boundaries, data minimization standards, audit rights, retention schedules, breach notification responsibilities, cybersecurity obligations, or independent oversight mechanisms specific to cross-institutional electoral data processing. In the absence of such a framework, the transformation of a civil identifier into a mandatory gateway for political participation raises heightened risks of function creep, cascading data inaccuracies, centralized vulnerability, and diffuse accountability. The legal framework authorizes both institutions to perform their respective mandates, but it does not comprehensively regulate the governance architecture created when those mandates converge leaving a critical gap at the intersection of identity management, electoral administration, and constitutional rights.

58 Electoral Commission (Uganda), *Press Statement on the Extension of the General Update of the National Voters Register* (10 Feb. 2025)

6. Findings And Analysis

6.1 Overall Summary of Findings

The *Data Protection Election Watch Tool* reveals that Uganda conducted its 2026 General Elections with a formal data protection framework in place but without a functioning compliance culture embedded across electoral institutions and political actors. While the Data Protection and Privacy Act, 2019 (DPPA) and its *Regulations* provide a comprehensive statutory architecture governing lawful processing, storage limitation, registration, and data subject rights, the investigation demonstrates that this framework was not operationalized during the most data-intensive electoral cycle in the country's history.

The findings do not indicate the absence of law. Rather, they expose a gap between legislative adoption and institutional implementation. In practice, registration requirements were unmet, DPIAs were not publicly demonstrated, privacy notices were largely inaccessible, and campaign-era data practices expanded beyond clearly articulated lawful bases.

This disconnect is particularly significant given the increasing digitization of Uganda's electoral infrastructure, including biometric voter verification systems and the integration of the *National Identification Number (NIN)* system into voter registration processes. In a digital election, data governance is not peripheral, it is foundational.

6.2 Strengths Observed

One positive institutional development was the multi-stakeholder training convened on *30 July 2025* by *Unwanted Witness,* aimed at strengthening awareness of compliance obligations among political parties, Electoral Commission officials, and civil society actors. The workshop addressed core requirements including *PDPO registration, DPIA obligations, lawful basis articulation, and the principle of storage limitation*[59].

In addition, formal advisory letters were issued to both the Electoral Commission and major political parties urging compliance with registration and transparency requirements.

However, these preventative interventions did not translate into measurable compliance outcomes. Awareness was not accompanied by institutional follow-through. The failure was therefore not informational, it was structural.

6.3 Challenges and Systemic Non-Compliance

The findings confirms that operational compliance across core electoral stakeholders during *Uganda's 2026* General Elections was structurally weak, uneven, and in several instances entirely absent. These failures were not isolated administrative oversights. They reflect deeper governance gaps affecting institutional accountability, campaign practices, regulatory clarity, and the protection of voter rights within an increasingly digitized electoral system.

The weaknesses identified are particularly grave given the scale and sensitivity of the data involved. The 2026 elections relied on the processing of millions of biometric, demographic, and identity-linked voter records. Biometric data such as fingerprints and facial images are irreversible identifiers. Political affiliation, voting intention, and inferred political opinion constitute sensitive personal data under data protection law. In this context, compliance failures carry amplified and long-term consequences.

6.4 Key Findings

- **Universal Political Party Non-Registration:** No political party registered with the ***Personal Data Protection Office (PDPO),*** despite prior multi-stakeholder training and formal written advisories. This represents a baseline statutory breach and removed political parties from structured regulatory oversight during the most data-intensive phase of electoral competition.

- **Delayed Electoral Commission Registration:** The Electoral Commission did not register with the ***PDPO*** during the active electoral cycle and only completed registration on ***21 January 2026*** after elections had concluded[60]. Registration is a foundational compliance obligation; its absence during live processing periods weakened transparency and supervisory capacity.

59 Unwanted Witness, National Training on Electoral Data Protection Compliance, Kampala, July 2025
60 Personal Data Protection Office (PDPO), *Register of Data Controllers and Processors: Electoral Commission*, registration status Active, registered 21 January 2026

- **Absence of Public DPIAs:** No publicly accessible ***Data Protection Impact Assessments (DPIAs)*** were demonstrated for high-risk processing activities, including biometric voter verification systems and the integration of ***National Identification Number (NIN)*** data. In a large-scale biometric environment, the absence of ***DPIAs*** signals insufficient risk anticipation and mitigation planning.

- **Opaque Identity–Electoral Integration:** The convergence of the ***National Identification Registration Authority (NIRA)'s*** civil identity system[61] with voter registration processes occurred without publicly documented data-sharing agreements, retention schedules, interoperability safeguards, or independent audit disclosures. This centralization of identity and electoral data heightens surveillance risk and magnifies the consequences of breach or misuse.

- **Failure to Operationalize Storage Limitation:** The statutory requirement that personal data must not be retained ***"longer than necessary"*** under ***Section 10 of the DPPA*** was not transparently operationalized. Political campaign data collected between ***November 2025*** and ***January 2026*** lacked defined deletion timelines or published retention policies. This creates a real and unresolved risk of indefinite retention of politically sensitive personal data.

- **Widespread Informal Campaign Data Practices:** Bulk SMS messaging, WhatsApp group additions, decentralized phone-call outreach, and informal voter segmentation occurred without documented lawful bases, consent frameworks, opt-out mechanisms, or clearly identifiable data controllers. The scale of these activities suggests systemic normalization rather than isolated deviation.

- **Violation of Data Subject Rights:** There was no visible operationalization of core data subject rights, including rights of access, rectification, objection, erasure, or complaint. Voters were not clearly informed of how to challenge unlawful processing or request deletion of their data during the campaign period.

- **Transparency and Auditability Gaps:** No independent audits of electoral data systems were publicly disclosed. The absence of audit trails, transparency reports, or public compliance attestations weakened institutional accountability and limited external scrutiny.

- **Cross-Border Exposure Risks:** The ***FANON*** incident revealed the potential hosting and routing of voter data through offshore infrastructure without transparent authorization, adequacy assessments, or regulatory safeguards. Cross-border processing of electoral data introduces jurisdictional uncertainty and sovereignty concerns.

- **Regulatory Ambiguity:** No comprehensive electoral data guidance was issued by the ***PDPO*** prior to enforcement incidents, leaving campaign-era data practices legally uncertain and allowing informal norms to proliferate without corrective direction.

- **Enforcement Asymmetry:** Institutional non-compliance persisted alongside criminal investigations targeting individual actors. This asymmetry raises proportionality concerns and risks undermining perceptions of equal application of the law.

6.5 Consequence Linkage

These compliance failures occurred within a large-scale biometric and identity-linked electoral system affecting millions of voters. In such an environment, the absence of uniform registration, documented DPIAs, transparent retention schedules, enforceable consent mechanisms, and consistent regulatory oversight does not merely reflect procedural gaps. It creates enabling conditions under which:

- Voter data may be retained indefinitely without justification.
- Political profiling may occur without transparency or accountability.
- Identity system inaccuracies may cascade into electoral exclusion.
- Data may be exposed to unauthorized access or cross-border control.
- Political actors may leverage information asymmetrically in competitive contexts.

61 Electoral Commission, *Press Statement on the Extension of the General Update of the National Voters Register*, 10 February 2025

The cumulative effect is a governance environment in which the legal framework exists, but practical safeguards are weakened.

Collectively, these weaknesses demonstrate that Uganda's first fully digitized electoral cycle operated without a consistently applied, transparently supervised, and uniformly enforced data governance regime. The gap was not legislative absence, it was institutional implementation failure.

In high-volume biometric elections, data governance is not peripheral to electoral integrity; it is integral to it. Where compliance is fragmented, oversight inconsistent, and retention undefined, democratic confidence becomes structurally vulnerable.

6.6 Campaign Period Case Study: Phone-Based Mobilisation and Decentralised Data Processing

The campaign period between ***November 2025*** and ***January 2026*** illustrates how significant data protection risks can arise not only from advanced electoral technologies but also from decentralized, human-driven mobilization strategies. The *National Unity Platform's (NUP)* directive encouraging supporters to call at least 50 contacts each[62], while framed as peer-to-peer civic engagement, effectively operationalized large-scale personal data processing outside formal compliance structures. In practice, the numerical target incentivized supporters to extend beyond their immediate personal contacts and source telephone numbers from *WhatsApp groups, forwarded lists, community registers, business directories, and online platforms*, transforming informal social communication into structured political outreach.

Under ***Section 3 of the Data Protection and Privacy Act (DPPA)***, personal data must be processed *fairly, lawfully, and for specific, explicit,* and *legitimate purposes.* Where phone numbers originally shared for social, commercial, or community purposes were repurposed for political campaigning without clear lawful basis, this raises concerns under *Section 7 of the Act,* which requires explicit, informed, and purpose-specific consent unless another lawful ground applies. Mere possession of a phone number does not constitute valid consent for political messaging.

Further, political opinions constitute "*special personal data*" ***under Section 9 of the DPPA***, warranting heightened protection. Where volunteers recorded, inferred, or informally categorized individuals' political preferences during calls even without maintaining formal databases, such activity may amount to the processing of sensitive data. At scale, this creates what may be described as shadow political datasets: decentralized, undocumented profiling systems operating outside declared data inventories or regulatory scrutiny. Legally, campaign volunteers engaged in structured outreach at the direction or encouragement of a political party may qualify as data processors under the Act, with the party itself potentially bearing responsibility as a data controller for processing carried out on its behalf. The absence of *formal data handling guidelines, structured oversight, or documented Data Protection Impact Assessments (DPIAs)* raises the governance question of whether political parties sufficiently embedded controller accountability into volunteer-driven mobilization.

Beyond legal compliance, the voter-level harms are non-trivial. Repeated unsolicited political calls may create coercive pressure, particularly in tightly networked communities where political affiliation carries social or economic consequences. Individuals may experience a chilling effect, moderating their political expression or disengaging from participation due to perceptions of monitoring or profiling. Vulnerable groups such as public employees, small business operators, or recipients of state services, may feel disproportionately exposed where outreach blurs into implicit pressure. Thus, what appears as low-tech mobilization can generate high-risk data processing when scaled across constituencies.

The episode also reflects a broader implementation deficit within Uganda's electoral data governance architecture. There was no publicly documented sector-specific guidance clarifying how political parties should manage volunteer-driven data processing; no evidence of systematic DPIAs addressing mass phone-based mobilization; and limited indication of proactive regulatory engagement tailored to campaign-period risks. In more mature regulatory environments, political parties are typically required to maintain declared campaign data policies, map campaign databases, and ensure that volunteer activity falls within structured controller accountability frameworks. In the absence of such embedded safeguards, decentralized campaign practices risk normalizing informal data ecosystems that operate beyond visibility and audit.

This case therefore reinforces a central analytical finding of the report: electoral data risks are not confined to biometric systems or digital platforms; they also emerge from organizational and cultural practices that convert social networks into instruments of political data extraction. When informal mobilization becomes systematized without compliance architecture, it contributes to the entrenchment of asymmetrical data power and shifts electoral competition toward increasingly expansive, and insufficiently governed, data-driven engagement.

62 "NUP Party Launches Phone Call Campaign," NTV Uganda, 17 March 2026.

6.7 Emerging Structural Risks

Beyond immediate compliance failures, three structural risks threaten long-term electoral data governance.

6.7.1 Regulatory Displacement

In high-profile incidents such as the ***FANON*** application case, enforcement responses were primarily led by security and communications authorities rather than the ***Personal Data Protection Office (PDPO)***[63], the statutory body mandated under the ***Data Protection and Privacy Act*** to supervise lawful processing, investigate breaches, and provide corrective guidance.

While criminal law may apply in instances of unlawful data access or disclosure, sidelining the data protection regulator shifts the focus from compliance and remediation to control and containment. This reframing weakens the rights-based foundation of the ***DPPA***, which is designed to promote accountability, proportionality, and preventive oversight rather than purely punitive enforcement.

When enforcement is treated principally as a security matter rather than a regulatory compliance issue:

- Corrective and preventive guidance diminishes.
- Transparency in decision-making decreases.
- Proportionality in enforcement risks erosion.
- Institutional authority of the PDPO is weakened.
- Data controllers receive fewer signals on how to achieve lawful compliance.

Over time, this dynamic creates fragmentation in electoral data governance, where multiple agencies act without clear coordination or unified standards. Such fragmentation undermines legal certainty, weakens supervisory consistency, and risks eroding public confidence in the neutrality and coherence of data protection enforcement during elections.

6.7.2 Selective Enforcement Patterns

The prosecution of civil society actors[64] under ***Section 35 of the Data Protection and Privacy Act*** occurred in a context where the Electoral Commission and all registered political parties had not complied with baseline statutory obligations, including mandatory registration with the ***Personal Data Protection Office (PDPO)*** under ***Section 29 of the Act.***

This juxtaposition exposes a structural imbalance in enforcement. The Data Protection and Privacy Act establishes both compliance duties and criminal penalties. It requires registration, transparency, accountability, and observance of data protection principles under *Section 3,* while simultaneously criminalizing unlawful obtaining or disclosure of data under *Section 35*. When punitive provisions are activated in the absence of uniform enforcement of compliance obligations, the equilibrium intended by the Act is disrupted.

Such asymmetry risks undermining:

- Equal application of the law
- Regulatory neutrality
- Proportionality in enforcement
- Institutional accountability
- Public confidence in enforcement integrity

Where major institutional data holders remain outside visible compliance structures while individuals face criminal sanction, enforcement begins to appear selective rather than systemic. This perception alone can weaken trust in the neutrality of the regulatory regime. More substantively, it risks deterring legitimate scrutiny, discouraging civic oversight, and narrowing democratic accountability mechanisms in an already sensitive electoral context.

A data protection regime that is perceived as unevenly applied may shift from being a rights-protective framework to

63 Position Statement by Unwanted Witness
64 Amnesty International, *Uganda: Human Rights Lawyer Arbitrarily Detained - Dr. Sarah Bireete*

becoming a deterrent instrument not through the text of the law, but through the pattern of its implementation.

6.7.3 Identity–Electoral Convergence

The integration of NIN data into electoral processes created a centralized identity-electoral architecture. While administratively efficient, this convergence increases:

- Surveillance potential
- Breach impact severity
- Cascading exclusion risks

Errors in civil identity systems may translate directly into political disenfranchisement. Biometric data, once compromised, cannot be reissued or replaced. The long-term governance implications are therefore irreversible.

7. Comparative Analysis

This section situates Uganda's 2026 electronic elections within both a longitudinal national trajectory and a broader regional and international comparative framework. By examining Uganda's experience across three electoral cycles, contrasting it with peer African democracies, and benchmarking it against continental and global standards, the analysis seeks to clarify whether observed data protection and governance challenges were exceptional, convergent, or structurally entrenched.

7.1 Uganda Compared with Kenya.

A comparative assessment between Uganda and Kenya demonstrates that divergent outcomes in electoral data governance are not products of technological inevitability, but of institutional design, judicial culture, and regulatory choices. Both countries have adopted biometric voter registration, electronic voter verification, and digital results transmission. Both have enacted modern data protection legislation ***(Kenya in 2019; Uganda in 2019).*** Yet the trajectory of oversight and accountability surrounding these systems has differed markedly.

In Kenya, repeated electoral disputes particularly following the **2013** and 2017 presidential elections, triggered sustained judicial intervention into electoral technology[65]. The Supreme Court's 2017 decision nullifying the presidential election elevated transparency, auditability, and server integrity into constitutional requirements rather than administrative preferences. Courts demanded disclosure of system logs, transmission records, server locations, and vendor arrangements. This jurisprudence normalized the expectation that electoral technology must be independently verifiable and legally scrutinizable. As a result, technology in Kenya became embedded within a culture of court-enforced transparency, even where political contestation persisted.

Parallel to judicial oversight, Kenya's data protection framework has progressively moved toward sector-specific operationalization. The ***Office of the Data Protection Commissioner (ODPC)*** issued formal Guidance Notes for Electoral Purposes, explicitly clarifying lawful bases, consent requirements, publication standards, data subject rights, DPIA obligations, and privacy-by-design safeguards for electoral actors[66]. Notably, the Guidance expressly recognizes that biometric processing in elections constitutes high-risk processing requiring Data Protection Impact Assessments and enhanced safeguards. This regulatory articulation reduces ambiguity and establishes ex ante compliance expectations before enforcement becomes necessary.

Institutionally, ***Kenya's Independent Electoral and Boundaries Commission (IEBC)*** publicly undertook development of a data inventory and conducted a Data Protection Impact Assessment in preparation for future electoral cycles, acknowledging its custodianship of over 22 million voter records and multiple categories of sensitive personal data[67]. Public statements by IEBC leadership have emphasized mandatory responsibility to protect personal information and cautioned against inappropriate sharing of personally identifiable information (PII) with political parties, particularly in the context of AI-driven profiling risks. This signals progressive internalization of a data protection culture within electoral administration[68].

Additionally, Kenya has seen growing regulatory attention to political party membership databases, bulk SMS governance, telecommunications compliance, and opt-out rights[69]. Public discourse increasingly frames elections as a "high-risk data environment," requiring heightened safeguards across the electoral ecosystem. While compliance gaps remain and political messaging abuses persist, the normative baseline has shifted: electoral data protection is treated as a central governance question rather than a peripheral compliance matter.

Uganda presents a contrasting institutional pattern. Although the ***Data Protection and Privacy Act (2019)*** provides a comprehensive statutory framework, sector-specific electoral guidance was not publicly issued prior to the 2026 election cycle. Mandatory registration, DPIAs for biometric systems, inter-agency data-sharing transparency, and retention schedules were not visibly embedded before high-volume data processing commenced. Judicial scrutiny of electoral technologies has been more limited in scope, and systemic disclosure of backend architectures, audit logs, or server governance has not been normalized as a constitutional expectation.

65 Supreme Court of Kenya, *Raila Amolo Odinga & Stephen Kalonzo Musyoka v Independent Electoral and Boundaries Commission & Others* (Presidential Election Petition 1 of 2017)
66 Office of the Data Protection Commissioner (ODPC), *Guidance Notes for Electoral Purposes*
67 IEBC News, *Commission develops data inventory and conducts data protection impact assessment*, 17 February 2025
68 Independent Electoral and Boundaries Commission, *"IEBC and ODPC Engage to Strengthen Electoral Data Governance Ahead of the 2027 General Election,"* IEBC News
69 Rose Mosero, *In Kenya's 2022 Elections, Technology and Data Protection Must Go Hand-in-Hand*, Carnegie Endowment for International Peace, 8 August 2022

The divergence is therefore not technological but institutional. Kenya's electoral data governance has evolved through iterative judicial correction, regulatory clarification, and public documentation of safeguards. Oversight mechanisms including courts, the ODPC, and parliamentary debate have incrementally constrained opacity. Uganda, by contrast, entered its first fully digitized electoral cycle with fragmented regulatory articulation, limited ex ante transparency obligations, and enforcement patterns that appeared reactive rather than structurally preventative.

In comparative perspective, Uganda's challenge is not that it adopted biometric and digital systems; Kenya did the same. The distinction lies in the balance between institutional power and regulatory accountability. Kenya's experience demonstrates that electoral technology can coexist with data protection oversight when courts demand disclosure, regulators issue targeted guidance, and electoral bodies publicly document compliance measures. Uganda's 2026 experience illustrates the risks that arise when digitization advances more rapidly than embedded supervisory culture, judicial transparency norms, and proactive regulatory articulation.

The comparative lesson is therefore structural: credible digital elections depend not only on hardware, software, or statutory text, but on whether oversight institutions courts, regulators, and electoral commissions, actively operationalize data protection as democratic infrastructure rather than as an afterthought to technological adoption.

7.2 Benchmarking Against GDPR-Aligned and International Electoral Data Protection Standards

When benchmarked against GDPR-aligned frameworks and emerging international standards on data and elections, Uganda's 2026 electoral data governance architecture reveals substantive compliance gaps not only at the technical level, but at the level of legal clarity, institutional safeguards, and rights implementation. Contemporary democratic practice, reflected in the ***EU General Data Protection Regulation (GDPR),*** Convention 108+ standards on political campaigning, treats elections as inherently high-risk data environments requiring heightened safeguards across the entire electoral ecosystem[70].

7.2.1 Clear Identification of Data Controllers and Processors

Under ***GDPR-aligned*** standards and comparative frameworks such as ***Turkey's KVKK practice,*** election management bodies, political parties, candidates, and third-party analytics providers are explicitly classified as data controllers, with defined obligations[71]. International guidance stresses that political campaign organizations, data brokers, social media platforms, and voter analytics companies may act as joint controllers where they determine purposes and means of processing. In Uganda's 2026 context, the absence of clearly articulated public documentation identifying data controllers and processors across the electoral data chain limited traceability and shielded accountability, particularly in relation to political profiling, bulk messaging, and vendor-level backend access.

7.2.2 Lawful Basis and Processing Conditions of Personal Data for Political activities

GDPR-aligned systems require a specific lawful basis for each processing activity, especially where personal data reveal or infer political opinions, a special category requiring enhanced safeguards[72]. Convention 108+ explicitly recognizes political opinion data and inferred voter profiling as sensitive processing requiring proportionality, purpose limitation, and appropriate safeguards[73].

In Uganda's 2026 elections, there was limited public articulation of the lawful bases relied upon for:

- Bulk SMS and WhatsApp mobilization,
- Analytics-driven voter segmentation,
- Cross-referencing NIN data with voter registration data, and
- Potential inference of political affiliation through digital engagement patterns.

Under GDPR standards, consent must be specific, informed, freely given, and revocable. Silence or pre-ticked assumptions are insufficient. There was no publicly verifiable evidence that structured consent frameworks governed large-scale political messaging or profiling operations during the campaign period.

---

70 Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (Consultative Committee of Convention 108, T-PD-BUR(2021)
71 Berfin Erdoğan, *Protection of Personal Data in Election Activities*, CottGroup (April 4, 2024)
72 The UK Information Commissioner's Office (ICO) guidance on *Special Category Data* from the UK GDPR lawful-basis guide
73 Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*

7.2.3 Mandatory DPIAs for High-Risk Processing

GDPR requires Data Protection Impact Assessments (DPIAs) for high-risk processing, particularly large-scale biometric data use, profiling, and automated decision-making[74]. Convention 108+ similarly emphasizes proportionality and risk-based safeguards in political campaigning.

Uganda's electoral system involved biometric voter verification, integration of the National Identification Number (NIN), and centralized digital databases all qualifying as high-risk processing. However, no publicly disclosed DPIAs as require by ***Regulation 12 of the Data Protection and Privacy Regulations 2021***, independent security audits, or risk mitigation reports were issued prior to the 2026 election cycle. Under GDPR-aligned standards, such absence constitutes a structural compliance gap.

7.2.4 Restrictions on Profiling and Micro-Targeting

Under ***GDPR and Convention 108+***, profiling that produces legal or similarly significant effects requires safeguards, transparency, and, in many cases, explicit consent. Political micro-targeting is specifically identified as posing risks of voter suppression, discrimination, and manipulation[75].

The 2026 Ugandan electoral environment featured expanded use of informal voter targeting through bulk communication and decentralized data mobilization networks. Without structured oversight of profiling practices or documented compliance audits, these activities operated in a regulatory grey zone inconsistent with GDPR-aligned expectations of necessity, proportionality, and fairness.

7.2.5 Data Security, Breach Notification, and Institutional Coordination

GDPR-aligned regimes require robust technical and organizational measures, breach notification obligations, and coordination between election authorities, cybersecurity agencies, and data protection authorities. Privacy International underscores that digital elections require whole-of-system cybersecurity risk assessment and inter-agency coordination[76].

While Uganda possesses a statutory data protection framework, publicly visible coordination between the ***PDPO, Electoral Commission, NIRA,*** and communications regulators during the 2026 cycle was limited. The absence of transparent breach-readiness protocols and public audit disclosures contrasts with international expectations for election-critical infrastructure.

7.2.6 Independent Oversight and Effective Remedies

GDPR-aligned systems emphasize the operational independence of supervisory authorities, consistent enforcement, and accessible remedies. International guidance highlights the importance of complaint mechanisms and regulatory neutrality[77].

Uganda's enforcement landscape during the electoral period appeared uneven, with limited demonstrable pre-election supervisory guidance for political actors and inconsistent visibility of corrective compliance measures for major institutional data controllers.

7.2.7 Normative Assessment

The comparative deficit identified is therefore not merely procedural or technical; it is normative and structural. GDPR-aligned democratic data governance rests on five foundational principles: *lawfulness, necessity, proportionality, transparency, and accountability.*

74 European Commission. *When is a Data Protection Impact Assessment (DPIA) required?*
75 Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), *Personal Data Processing by and for Political Campaigns: The Application of the Council of Europe's Modernised Convention 108*, T-PD(2020)02 (Strasbourg: Council of Europe, 11 June 2020)
76 Privacy International, *Technology, Data and Elections: A card game*, 7 November 2025
77 GDPR - The enforcement mechanism" chapter from Texts and Materials in Data Protection and Digital Human Rights

Uganda's 2026 electoral cycle demonstrated:

- Weak ex ante regulatory articulation,
- Limited DPIA transparency,
- Ambiguity in lawful bases for political profiling,
- Insufficiently documented cross-system safeguards, and
- Fragmented supervisory visibility.

While Uganda possesses a modern statutory framework on paper, its operationalization during the 2026 elections did not consistently align with internationally recognized safeguards governing biometric processing, political opinion data, profiling, and electoral infrastructure security.

In digitally mediated elections, compliance with these standards is not aspirational benchmarking; it is a democratic resilience requirement. The absence of demonstrable alignment with GDPR-equivalent safeguards places electoral data governance at risk of drifting from a rights-protective model toward an administratively permissive one with long-term implications for institutional trust, political equality, and electoral legitimacy.

8. Recommendations

The findings of this investigation demonstrate that ***Uganda's 2026 General Elections*** were conducted within a formally established but operationally under-embedded data protection regime. The following recommendations are structured to move from diagnosis to implementation. Each recommendation identifies both the action required and the mechanism through which it can realistically be achieved before the next electoral cycle.

8.1 Electoral Commission

8.1.1 Publish a Comprehensive Electoral Data Governance Framework

The ***Electoral Commission (EC)*** should, pursuant to its statutory powers under the ***Electoral Commission Act,*** develop and formally publish a sector-specific Electoral Data Governance Framework to operationalize the ***Data Protection and Privacy Act (DPPA)*** across the entire electoral cycle including the pre-election, polling-day, and post-election phases. Although the Act does not explicitly mandate such a framework, sufficient legal authority exists within its provisions, including ***Section 12(1)(p)*** which grants the Commission residual powers necessary for the proper discharge of its functions, ***Sections 12(1)(e)-(f)*** which require the Commission to ensure the integrity, fairness, and security of the electoral process, ***Section 18*** which mandates the compilation and continuous maintenance of the national voters register, and ***Section 23(2)*** which empowers the Commission to prescribe the form in which the voters register is maintained. Additional administrative authority arises from ***Section 8(8)*** permitting the Commission to regulate its own procedures and Section 51 allowing the making of regulations for the effective performance of electoral functions. Collectively, these provisions provide a sufficient statutory basis for the Commission to establish a comprehensive electoral data governance framework that ensures lawful, secure, and accountable processing of electoral data throughout the electoral process.

The Framework should provide a clear, publicly accessible articulation of how voter data is collected, processed, stored, shared, and disposed of. At a minimum, it should include:

a. A comprehensive mapping of all categories of voter data processed, including biometric identifiers, ***National Identification Numbers (NINs)***, contact details, polling station assignments, result-form images, device-level logs, and any associated metadata;

b. A clear identification of the lawful basis for each category of processing, aligned with the provisions of the ***DPPA***;

c. Defined and publicly disclosed data retention periods, including automatic deletion triggers where applicable;

d. Transparent documentation of all data-sharing arrangements, including those involving the ***National Identification and Registration Authority (NIRA)***, technology vendors, telecommunications operators, observer groups, and any third-party processors; and

e. Disclosure of any cross-border data hosting or transfer arrangements, together with the legal safeguards and adequacy mechanisms relied upon.

8.1.2 Conduct and Publish Electoral Data Protection Impact Assessments (DPIAs)

The ***Electoral Commission*** should conduct and publish ***Data Protection Impact Assessments (DPIAs)*** for all high-risk electoral data processing activities prior to the next general election cycle. At a minimum, DPIAs must be undertaken for the ***Biometric Voter Verification Kits (BVVKs),*** the integration of the ***National Identification Number (NIN)*** system with the voter register, digital voter display and verification portals, and all electronic results capture and transmission systems.

Each DPIA should assess necessity and proportionality, identify risks to voter rights and freedoms, evaluate cybersecurity vulnerabilities, define mitigation measures, and clarify data retention timelines. The completed assessments should be submitted to the ***Personal Data Protection Office (PDPO***) for review, and a non-sensitive public summary should be published to enhance transparency and public trust.

8.1.3 Institutionalize Independent Technical and Cybersecurity Audits

The ***Electoral Commission*** should institutionalize mandatory, independent technical and cybersecurity audits of all election-critical digital systems prior to each general election. These audits should be conducted by qualified third-party experts and completed sufficiently in advance of polling day to allow remediation of identified vulnerabilities. At a minimum, the audit framework should include:

a. Comprehensive penetration testing of voter registration and display portals to identify vulnerabilities to scraping, unauthorized access, and data extraction;
b. Independent technical review of ***Biometric Voter Verification Kit (BVVK)*** software, firmware integrity, and update controls;
c. Assessment of vendor-level backend access privileges, including administrator rights, remote access capabilities, and audit log governance;
d. Verification of encryption standards, data-at-rest and data-in-transit protections, and access control mechanisms across all interconnected systems.

Audit findings should be submitted to the ***Personal Data Protection Office*** and summarized publicly in a redacted assurance statement that balances transparency with legitimate security considerations.

8.1.4 Codify Interoperability Safeguards with NIRA

The ***Electoral Commission (EC)*** and the ***National Identification and Registration Authority (NIRA)*** should formalize their data-sharing relationship through a publicly accessible ***Memorandum of Understanding (MoU)*** that clearly defines the legal, technical, and accountability boundaries governing the integration of the ***National Identification Number (NIN)*** system into electoral processes. The MoU should expressly articulate purpose limitation constraints to prevent secondary or unrelated use of identity data; define access control hierarchies and audit rights; allocate institutional responsibility in the event of data breaches; and establish mandatory breach notification and remediation protocols.

Given the scale and sensitivity of identity-linked electoral data, such an instrument should be developed with oversight from the ***Personal Data Protection Office (PDPO)*** and tabled before the relevant parliamentary committees to enhance transparency, legal certainty, and public trust.

8.1.5 Establish Clear Retention and Deletion Protocols

The ***Electoral Commission (EC)*** should formally adopt and publish binding retention and deletion schedules governing all electoral data processed during the electoral cycle. This should include clearly defined timelines for the retention of biometric verification logs, the archival or destruction of result-form images captured through electronic systems, and the deletion of voter roll extracts stored on biometric voter verification devices.

These schedules should be grounded in the principle of storage limitation under the ***Data Protection and Privacy Act*** and operationalized through technical safeguards, including automated deletion triggers where feasible. Publicly accessible retention policies would enhance transparency, reduce the risk of indefinite storage of sensitive voter data, and strengthen institutional accountability.

8.1.6 Create a Public Electoral Data Transparency Portal

The ***Electoral Commission (EC)*** should establish and maintain a publicly accessible ***Electoral Data Transparency Portal*** as a permanent institutional feature of its digital governance framework.

The portal should proactively publish key accountability documents, including:

a. the list of technology vendors and service providers engaged in electoral systems;
b. summaries of data-sharing arrangements with public institutions and third parties;
c. non-sensitive summaries of ***Data Protection Impact Assessments (DPIAs)*** conducted for high-risk systems;
d. annual electoral data compliance and audit reports; and
e. confirmed data breach notifications, including remedial measures taken.

Publication of this information should occur on a rolling basis and, at minimum, within 30 days of finalization of each document. By institutionalizing structured transparency, the Commission would reduce speculation, strengthen public trust, and demonstrate measurable compliance with the ***Data Protection and Privacy Act***.

8.2 Personal Data Protection Office (PDPO)

8.2.1 Issue Binding Electoral Data Protection Guidelines (No Later Than 12 Months Before the Next General Election)

Pursuant to its mandate under ***Section 5(1)(a), (b), (c)*** and ***(g),*** and ***Section 5(2) of the Data Protection and Privacy Act, 2019***, the ***Personal Data Protection Office (PDPO)*** should, at least twelve months prior to the next general election, issue comprehensive ***Electoral Data Protection Guidelines*** clarifying the application of the ***Data Protection and Privacy Act*** to electoral processes. These Guidelines should explicitly define lawful bases for political profiling and voter analytics; establish consent standards for campaign-related data processing; regulate bulk SMS, automated calling, and digital messaging practices; prescribe limits and safeguards for data sharing between public institutions, including the ***Electoral Commission*** and ***NIRA***; and set clear conditions for cross-border hosting or processing of electoral data. The objective of these Guidelines should be to eliminate interpretive ambiguity, embed preventative compliance prior to live electoral activity, and ensure consistent, proportionate enforcement during the campaign period.

8.2.2 Publish the Mandatory High-Risk Processing List (Regulation 12(3))

Pursuant to ***Regulation 12(3)*** of ***the Data Protection and Privacy Regulations, 2021***, the ***Personal Data Protection Office (PDPO)*** should urgently establish and make public the mandatory list of processing operations that require a ***Data Protection Impact Assessment (DPIA)***. In the electoral context, this list should explicitly designate biometric voter verification systems, national voter databases, political profiling and micro-targeting practices, and AI-enabled political content processing as high-risk operations automatically subject to ***DPIA*** requirements. The publication of this list would eliminate interpretive ambiguity, strengthen preventative compliance, and provide clear regulatory direction to electoral institutions, political parties, and technology vendors prior to the next election cycle.

8.2.3 Adopt a Proactive Compliance Model Rather than Reactive Criminal Enforcement

The ***Personal Data Protection Office (PDPO)*** should transition from a predominantly reactive enforcement posture toward a structured, preventative compliance model in the period preceding each general election. Rather than relying primarily on post-incident criminal investigations, the ***PDPO*** should institutionalize pre-election compliance audits of the ***Electoral Commission*** and all registered political parties to assess adherence to registration, lawful processing, retention, and transparency obligations. Where gaps are identified, the Office should issue formal compliance notices with defined corrective timelines prior to polling day. To strengthen transparency and public confidence, the ***PDPO*** should also publish anonymized compliance scorecards summarizing levels of institutional preparedness and corrective actions taken.

This approach would reposition data protection from a punitive instrument applied after alleged violations to a preventative governance mechanism designed to reduce risk, enhance institutional accountability, and safeguard electoral integrity before harm occurs.

8.2.4 Create a Dedicated Electoral Data Oversight Unit

Given the scale, sensitivity, and systemic importance of electoral data processing, the ***Personal Data Protection Office (PDPO)*** should establish a temporary but operationally empowered ***Electoral Data Oversight Unit*** during each general election cycle. This unit should be mandated to monitor political campaign data practices, coordinate rapid response to data breaches affecting electoral systems, receive and process citizen complaints relating to electoral data misuse, and issue time-sensitive advisory clarifications to electoral stakeholders. The unit should operate for a defined pre-election and post-election period, with clearly allocated technical personnel and budgetary support, and should publish a post-election oversight report summarizing key compliance findings and systemic risks.

8.2.5 Develop Clear Guidance on AI and Deepfake Political Content

The ***Personal Data Protection Office (PDPO)*** should develop and issue formal regulatory guidance clarifying the application of the ***Data Protection and Privacy Act*** to AI-generated and synthetic political content. The guidance should specify the circumstances under which synthetic media including deepfakes, voice cloning, and AI-generat-

ed images or videos constitutes personal data processing, particularly where identifiable individuals are depicted or impersonated. It should further establish transparency obligations requiring political actors to clearly disclose the use of AI-generated campaign materials, define accountability standards for parties and third-party vendors deploying generative tools, and outline enforcement consequences where synthetic content results in unlawful profiling, impersonation, or manipulation. Such guidance should be issued sufficiently in advance of the next electoral cycle to ensure legal certainty and preventative compliance.

8.3 Political Parties

8.3.1 Mandatory Registration and Appointment of Data Protection Officers (DPOs)

All political parties intending to participate in a general election should be required to register with the ***Personal Data Protection Office (PDPO)*** no later than twelve months prior to polling day. Proof of active registration should constitute a precondition for acceptance of candidate nominations by the ***Electoral Commission***, in the same manner that statutory compliance is required for other regulated entities. In addition, political parties engaged in large-scale voter data processing, including digital campaigning, profiling, or bulk messaging, should formally designate a ***Data Protection Officer (DPO)*** responsible for overseeing compliance with the ***Data Protection and Privacy Act***, maintaining internal records of processing activities, and serving as a liaison with the ***PDPO***.

8.3.2 Publish Campaign Data Privacy Notices

Political parties should be required to publish clear and accessible campaign data privacy notices prior to engaging in voter outreach or digital campaigning activities. Such notices should, in compliance with the principles of lawful and transparent processing under ***Section 3(1)(b) and (f) of the Data Protection and Privacy Act (DPPA)***, disclose the categories and sources of personal data used (including voter registers, telecommunications datasets, and social media platforms), the existence and nature of any profiling or analytics practices, applicable data retention periods, and the mechanisms available for voters to opt out of political communications. Further, pursuant to ***Section 13 (information to be given to the data subject prior to collection)***, voters must be informed in advance of the purpose of processing, data recipients, retention period, and their rights of access and rectification.

Such disclosure is essential to ensure informed voter participation, reduce perceptions of manipulation, and align political campaign practices with the ***DPPA's*** requirements on lawful processing, purpose limitation, and transparency.

8.3.3 Establish Lawful Consent and Opt-Out Systems for Messaging

Political parties and campaign actors must ensure that all bulk SMS, automated calls, and WhatsApp-based outreach are grounded in a clearly articulated lawful basis In line with ***Section 7 (lawful basis for processing, including consent)*** of the ***Data Protection and Privacy Act (DPPA).*** Each communication should transparently identify the data controller responsible for the message, specify the legal basis for processing the recipient's personal data, and provide a simple, functional opt-out mechanism. Telecommunications-compliant opt-out codes should be embedded in all bulk political messaging, and parties must maintain documented consent or lawful processing logs capable of demonstrating compliance upon regulatory request. Failure to implement verifiable opt-out systems should constitute a breach of electoral data governance standards.

8.3.5 Prohibit Unauthorized Voter Data Aggregation

Political parties should formally adopt and enforce internal data governance policies prohibiting the unauthorized aggregation, acquisition, or combination of voter data. This should expressly include a ban on scraping digital voter portals, purchasing unverified telecommunications datasets, or merging datasets for profiling purposes without a clearly documented lawful basis under the Data Protection and Privacy Act. These policies should be accompanied by mandatory compliance training for campaign staff and data handlers, and should assign internal accountability to a designated data protection focal person responsible for oversight and documentation.

8.3.6 Conduct Party-Level DPIAs for Digital Campaigning

Political parties that deploy profiling techniques, data analytics tools, voter segmentation systems, or artificial intelligence technologies in the course of digital campaigning should be required to conduct ***Data Protection Impact Assessments (DPIAs)*** prior to engaging in such processing. The ***DPIA*** should identify the categories of personal data processed, the lawful basis relied upon, potential risks to voters' rights and freedoms, measures adopted to mit-

igate manipulation or discriminatory profiling, and defined retention and deletion timelines. Parties should retain documented risk mitigation plans and make summaries available to the ***Personal Data Protection Office (PDPO)*** upon request. To ensure proportionality, the ***PDPO*** may develop simplified ***DPIA*** templates tailored to campaign contexts, particularly for smaller political parties.

8.4 Parliament

8.4.1 Amend the Electoral Commission Act to Embed Digital Data Governance Safeguards

Parliament should amend the ***Electoral Commission Act, Cap 140*** to expressly incorporate digital data governance obligations within the Commission's statutory mandate. As the Act currently regulates voter registration, ballot design, and polling procedures but remains silent on biometric data governance and cybersecurity safeguards, targeted amendments are required to align the Act with Uganda's ***Data Protection and Privacy Act (DPPA).***

The amendments should include the following:

a. Amendment to Section 12 (Additional Powers of the Commission):

Insert a new subsection requiring the Commission to:

- Conduct ***Data Protection Impact Assessments (DPIAs)*** for high-risk electoral technologies, including biometric voter verification systems and results transmission infrastructure.
- Commission independent cybersecurity audits prior to each general election.
- Implement technical and organizational measures to safeguard voter data against unauthorized access or breach.

b. Amendment to Section 18 (National Voters Register):

Insert provisions requiring:

- Lawful basis documentation for all voter data processing.
- Statutory retention limits for biometric verification logs.
- Clear deletion triggers for device-level voter extracts.
- Mandatory breach notification to the ***Personal Data Protection Office (PDPO)*** within a defined timeframe (e.g., 72 hours).

c. New Section Under Part III – Electoral Data Governance:

Introduce a new section requiring the Commission to:

- Publish an ***Electoral Data Governance Framework***.
- Disclose summaries of DPIAs for high-risk systems.
- Maintain transparency regarding vendor data-processing arrangements.
- Ensure purpose limitation in data-sharing with NIRA and other public bodies.

d. Amendment to Section 51 (Regulations):

Expand regulation-making powers to explicitly authorize statutory instruments governing:

- Electoral technology security standards.
- Biometric data handling.
- AI and automated decision-making in electoral systems.

8.4.2 Strengthen Oversight Through Parliamentary Committees

Parliament, through its ***Standing Committees on ICT, Legal Affairs***, and ***Human Rights***, should institutionalize structured oversight of electoral data governance as part of its regular supervisory mandate. This should include requiring the ***Electoral Commission (EC)*** and the ***Personal Data Protection Office (PDPO)*** to submit annual electoral data governance reports, conducting mandatory pre-election compliance hearings to assess preparedness of high-risk digital systems, and publishing committee findings and recommendations prior to each general election cycle.

To ensure continuity, these oversight engagements should be scheduled within the parliamentary calendar at least twelve months before polling day, with follow-up reviews conducted six months thereafter. Formalizing this oversight cycle will embed transparency, reduce regulatory fragmentation, and reinforce Parliament's constitutional role in safeguarding electoral integrity.

8.4.3 Fund Institutional Capacity Building

Parliament should ensure that dedicated and ring-fenced budgetary allocations are provided to strengthen institutional capacity for electoral data governance. This should include targeted funding to enhance the technical expertise of the ***Personal Data Protection Office (PDPO)***, particularly in areas of biometric systems oversight, cybersecurity assessment, artificial intelligence monitoring, and forensic audit capability. Allocations should also support periodic independent cybersecurity testing of electoral infrastructure and the development of standardized data protection training programs for Electoral Commission staff, political parties, and relevant regulators.

To operationalize this reform, the ***Ministry of Finance***, in consultation with the ***Electoral Commission***, ***Ministry of ICT and National Guidance*** and the ***PDPO***, should integrate electoral data governance capacity into the Medium-Term Expenditure Framework at least two financial years before the next general election. Where appropriate, development partner support may supplement domestic funding, provided that institutional independence and domestic oversight remain intact.

9. Conclusion

Uganda's 2026 General Elections marked a decisive shift toward a highly digitized electoral ecosystem, where biometric verification, integrated identity systems, digital platforms, and data-driven campaigning fundamentally reshaped political participation. This transformation underscored that privacy is not peripheral but central to democratic integrity, safeguarding voter autonomy, ballot secrecy, and public trust. However, the investigation reveals a critical gap between technological expansion and institutional readiness: while a legal data protection framework exists, its implementation remains uneven, oversight largely reactive, and safeguards insufficiently embedded. The elections exposed structural risks arising from weak governance, inconsistent compliance, and growing asymmetries of digital power that can influence participation, profiling, and political outcomes. Addressing these challenges requires a shift from ad hoc enforcement to proactive, system-wide governance anchored in transparency, lawful processing, accountability, and continuous monitoring. In this context, *Unwanted* ***Witness's Data Protection Election Watch*** demonstrated the essential role of civil society in translating legal principles into practical oversight and reinforcing the link between digital rights and electoral integrity. Looking ahead, Uganda's democratic resilience will depend on whether data governance evolves alongside technological innovation, ensuring that digital systems empower citizens rather than concentrate unchecked power; embedding privacy, institutional oversight, and rights protection into the core of electoral processes is therefore not optional, but a democratic imperative.

10. Annex

10.1 Annex A (Data Table): Institutional Compliance and Electoral Data Governance Indicators

This section presents a structured synthesis of findings generated through the ***Data Protection Election Watch Tool***, translating qualitative observations into a consolidated institutional compliance matrix. The table below captures key indicators assessed across principal electoral stakeholders during Uganda's 2026 General Elections, as documented in "***Uneven Enforcement of Data Protection Laws Puts Data Subjects Rights at Risk in Uganda's 2026 Polls***". The table reflects observed compliance status during the live electoral cycle (pre-election through immediate post-election period), not post-hoc corrective actions unless explicitly indicated.

(i) Institutional Data Protection Compliance Matrix (2026 Electoral Cycle)

Stakeholder	PDPO Registration Status (During Election Period)	DPIA Conducted & Published	Privacy Notice/Public Data Policy	Data Inventory & Mapping	Retention & Deletion Policy	Digital Campaign Compliance	Overall Risk Assessment
Electoral Commission (EC)	Not registered during core electoral period (registered post-election: 21 Jan 2026)	Not publicly demonstrated for BVVK, NIN integration, portals	No publicly accessible comprehensive privacy framework	No publicly disclosed structured data inventory	No transparent retention/deletion schedule for biometric logs or portal data	Not applicable (administrative role)	**High institutional governance risk**
National Identification and Registration Authority (NIRA)	Operational data controller (separate mandate)	No publicly disclosed DPIA for EC data interoperability	Limited public disclosure regarding EC integration	No published joint EC–NIRA data mapping framework	Retention policies not clarified for electoral interoperability	Not applicable	**High interoperability & function creep risk**
Political Parties (Collectively)	None registered during campaign period	None demonstrated for profiling, bulk SMS, analytics	No standardized campaign privacy notices	No documented campaign data inventories	No published retention timelines for campaign databases	Bulk SMS, call mobilization, profiling without structured consent	**Systemic non-compliance & decentralized processing risk**
Private Campaign Vendors / Data Intermediaries	Not demonstrated	Not demonstrated	Opaque	Opaque	Not disclosed	Active in digital targeting and messaging	**High profiling and shadow-dataset risk**
Personal Data Protection Office (PDPO)	Operational	No published high-risk processing list under Reg. 12(3)	Limited sector-specific electoral guidance	No public electoral-specific compliance framework	No election-period oversight unit	Reactive enforcement model	**Under-embedded supervisory oversight**
Digital Platforms (Meta, X, TikTok, YouTube, WhatsApp)	Outside domestic registration regime (cross-border actors)	Not disclosed in electoral context	Platform-level privacy policies (generic, not electoral-specific)	Proprietary and opaque	Platform governed	Algorithmic amplification, AI-enabled content risks	**High cross-border governance complexity**

(ii) Indicator-Based Compliance Assessment

The following table reflects aggregated findings across key monitoring indicators deployed under the Watch Tool.

Indicator	EC	Political Parties	NIRA–EC Integration	Vendors	PDPO Oversight	Observed Pattern
Transparency of Data Use	Limited	Minimal	Opaque	Opaque	Limited	Structural opacity
Lawful Basis Clarity	Public duty asserted	Not articulated	Not publicly codified	Not articulated	Not clarified through guidance	Ambiguity
Data Minimization	Not demonstrated publicly	Not demonstrated	Not publicly documented	Not demonstrated	Not audited	Expansion without mapping
Consent Mechanisms	Not applicable (public function)	Weak/implicit	Not publicly addressed	Not documented	No campaign-specific guidance	Consent illusion in campaigns
Data Sharing Disclosure	Limited	None	No codified sharing framework	Opaque	Not proactively reviewed	Interoperability gap
Retention & Deletion	Not disclosed	Not disclosed	Not disclosed	Not disclosed	Not enforced pre-election	Storage limitation ambiguity
Cybersecurity & Audit	No published independent audit	Not demonstrated	Not demonstrated	Not transparent	No public audit trigger list	Technical opacity
DPIA Implementation	Not demonstrated	Not demonstrated	Not demonstrated	Not demonstrated	High-risk list unpublished	Preventive safeguard gap
Enforcement Consistency	EC non-compliance observed	None registered	Not scrutinized	Not scrutinized	Criminal enforcement used in selective contexts	Enforcement asymmetry

(iii) Electoral Data Lifecycle Risk Mapping

Electoral Phase	Primary Data Types Processed	Governance Strength	Principal Risks Identified
Voter Registration	Biometric data, NIN, demographic identifiers	Weakly embedded	Centralization, interoperability risk, lack of DPIA
Campaign Period	Phone numbers, profiling data, digital traces	Informal & decentralized	Shadow datasets, consent breakdown, micro-targeting
Polling Day	Fingerprints, verification logs, ballot scans	Procedural but opaque	Device failure, audit log integrity concerns
Results Management	Scanned declarations, tally data	Limited transparency	Backend opacity, auditability gaps
Post-Election Retention	Biometric logs, voter extracts	Undefined	Indefinite retention risk, unclear deletion triggers

i. Analytical Synthesis

The data table findings demonstrate that Uganda's 2026 elections operated within a legally established but operationally fragmented data protection regime. Compliance was not uniformly institutionalized across stakeholders, and preventive safeguards such as DPIAs, data mapping, retention schedules, and independent audits were not publicly embedded prior to or during high-risk electoral processing activities.

The pattern observed was not absence of law, but uneven operationalization:

- Core public authorities processed large-scale biometric data without publicly demonstrated DPIAs.

- Political parties conducted data-driven campaigning without structured lawful-basis articulation.
- Interoperability between identity and electoral systems lacked a codified governance framework.
- Oversight mechanisms were reactive rather than preventive.

Across the electoral data lifecycle, transparency deficits and documentation gaps amplified institutional risk exposure, particularly in areas involving biometric verification, digital voter portals, decentralized campaign mobilization, and cross-platform political communication.

The consolidated data table therefore supports the report's central finding: Uganda's 2026 electronic elections were governed by a formal rights-protective framework that was insufficiently embedded into institutional practice at the point where electoral data processing was most intensive and consequential

10.2 Annex B: Legal and Regulatory Framework

Legal Instrument	Scope & Mandate	Key Provisions Relevant to Elections	Strengths	Structural Gaps / Limitations	Responsible Authority
Data Protection and Privacy Act, 2019 (Chapter 97)	Governs collection, processing, storage, disclosure, and cross-border transfer of personal data in Uganda. Applies to public and private entities.	***Section 3*** – Data protection principles (lawfulness, fairness, purpose limitation, minimization, accuracy, retention limits, security, accountability). ***Section 7*** – Consent requirement (with limited public duty exceptions). ***Section 9*** – Protection of special personal data (including political opinions). ***Section 19*** – Cross-border transfer safeguards. ***Section 20*** – Security safeguards. ***Section 23*** – Breach notification. ***Sections 35–37*** – Criminal offences for unlawful processing.	Comprehensive rights-based framework. Recognizes biometric and political data as protected categories. Establishes enforceable obligations and penalties.	No electoral-specific guidance clarifying application to voter registers, biometric systems, or campaign profiling. Public duty exception (***Section 7(2))*** lacks detailed limits in electoral context. Enforcement uneven in practice. No mandatory published list of high-risk electoral processing under ***Regulation 12(3).***	Personal Data Protection Office (PDPO)

Data Protection and Privacy Regulations, 2021	Operationalizes the DPPA; establishes compliance mechanisms and regulator powers.	***Regulations 15–19*** – Mandatory registration of data controllers/processors. ***Regulation 12 – DPIA*** requirement for high-risk processing. ***Regulation 30*** – Cross-border processing conditions. ***Regulation 31*** – Information security standards. Establishes Data Protection Register.	Creates procedural compliance architecture. Requires disclosure of processing purposes, retention, and safeguards. Introduces DPIA mechanism.	No published high-risk processing list explicitly covering biometric electoral systems. No binding electoral data governance guidelines. Limited proactive compliance audits during electoral cycle.	PDPO
Electoral Commission Act (Cap 140)	Establishes Electoral Commission (EC); governs voter registration, electoral administration, and oversight.	***Section 2*** – Establishes EC as corporate body. ***Section 18*** – Mandate to compile and maintain national voters' register. ***Sections 23–25*** – Public inspection of register. ***Section 12*** – Operational powers. ***Section 16*** – Accreditation of observers. ***Section 50*** – Special adaptive powers.	Provides legal authority for voter register management. Embeds transparency through public inspection mechanisms. Grants operational autonomy to EC.	Designed in analogue paradigm; lacks explicit cybersecurity, encryption, audit, or data governance standards. No statutory requirement for privacy policies or DPIAs for electoral systems. No independent technical oversight mechanism for digital infrastructure. No codified inter-agency data-sharing safeguards with NIRA.	Electoral Commission
Electoral Commission (Amendment) Act, 2020	Authorizes adoption of technology in election management.	***Section 12*** amendments – Enables electronic systems, digital displays, and technological prescriptions via statutory instrument.	Legally legitimizes technology in elections. Responds to Supreme Court recommendation on tech regulation.	Focuses on functionality rather than data protection safeguards. No embedded privacy-by-design obligations.	Electoral Commission

Presidential Elections (Amendment) Act, 2020	Authorizes electronic transmission of results.	Permits electronic transmission of return forms and tally sheets; requires copies to candidates.	Formalizes electronic result transmission. Enhances procedural efficiency.	No explicit data integrity verification standards. No transparency requirements on back-end systems. No mandatory security audit obligations.	Electoral Commission
Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, 2025	Governs mandatory use of biometric voter verification systems (BVVS/BVVK).	***Regulations 2 & 4*** – Mandatory biometric verification before ballot issuance. ***Regulation 5*** – Operational biometric verification procedures. ***Regulation 6*** – Digital ballot inventory and results form capture. ***Regulation 7*** – Offences for misuse or non-use.	Standardizes biometric verification procedures nationwide. Enhances uniformity in polling-day identity checks. Creates offences for tampering or non-compliance.	Silent on biometric data retention timelines. No deletion protocols. No encryption or cybersecurity standards specified. No independent audit requirement. No transparency on device-level data governance. No explicit privacy-by-design obligations.	Electoral Commission
NIRA–EC Operational Integration (Administrative Practice)	Operational convergence of National Identification Number (NIN) system and voter register.	NIN used for voter verification, polling station assignment, and register updates. Shared registration kits and database reliance.	Enhances identity verification efficiency. Reduces duplicate r		

10.3 Annex C: Data Protection Election Watch Tool Framework

i. Overview

The ***Data Protection Election Watch Tool*** is a structured compliance and risk-assessment instrument developed by Unwanted Witness to monitor how personal and biometric data were collected, processed, secured, shared, retained, and, where applicable, deleted throughout Uganda's 2025–2026 electoral cycle.

The Tool operationalizes obligations under:

- The Data Protection and Privacy Act, 2019
- The Data Protection and Privacy Regulations, 2021
- The Electoral Commission Act (Cap 140)
- The Electoral Commission (Adoption and Manner of Use of Biometric Voter Verification System) Regulations, 2025

It translates statutory principles into measurable indicators across the entire electoral data lifecycle.

ii. Objectives of the Tool

The Data Protection Election Watch Tool was designed to:

a. Assess compliance of electoral stakeholders with statutory data protection obligations.
b. Identify high-risk processing operations involving biometric and political data.
c. Monitor transparency, consent mechanisms, and lawful basis declarations.
d. Evaluate institutional accountability structures (registration, DPO appointment, DPIAs).
e. Detect systemic governance gaps across voter registration, campaigning, verification, and results management.
f. Generate evidence-based recommendations for reform and regulatory action.

iii. **Scope of Monitoring**

The Tool covers the full electoral data lifecycle:

Electoral Phase	Data Protection Focus
Voter Registration & Update	Biometric capture, NIN integration, lawful basis
Voter Register Display	Public exposure, scraping risks, access controls
Campaign Period	Data sourcing, profiling, bulk messaging, AI use
Polling Day	Biometric verification, device logging, fallback procedures
Results Transmission	Digital capture, storage integrity, transmission safeguards
Post-Election	Retention limits, deletion triggers, archival practices

Stakeholders Assessed
The Tool evaluates compliance across the following actors:
- Electoral Commission (EC)
- National Identification and Registration Authority (NIRA)
- Personal Data Protection Office (PDPO)
- Political Parties and Candidates
- Campaign Volunteers and Data Processors
- Telecommunications Operators
- Technology Vendors
- Digital Platforms (where relevant to political advertising and profiling)

iv. **Structure of the Monitoring Framework**

The Tool is organized into **12 Core Monitoring Pillars**, each mapped to statutory obligations and observable indicators.

a. **Transparency of Data Collection**
Legal Basis: Sections 3, 7 DPPA; Regulations 15–19
Indicators:

- Publicly accessible privacy notices
- Disclosure of data categories collected
- Explanation of processing purposes
- Identification of data controllers and processors
- Accessibility of information to voters

Risk Rating: Low / Moderate / High / Critical

b. **Lawful Basis and Consent Mechanisms**
Legal Basis: Section 7 DPPA
Indicators:

- Explicit consent documentation
- Alternative lawful basis justification
- Evidence of informed and purpose-specific consent

- Withdrawal mechanisms

Special scrutiny applied where political opinion data or profiling occurs.

c. **Sensitive Personal Data Safeguards**
Legal Basis: Section 9 DPPA
Indicators:

- Processing of biometric identifiers
- Processing of political opinions
- Enhanced safeguards for special personal data
- Restricted access protocols

d. **Data Minimization and Purpose Limitation**
Legal Basis: Section 3 DPPA
Indicators:

- Collection limited to necessary data
- No secondary use without lawful basis
- Prevention of function creep
- Clear linkage between purpose and processing activity

e. **Registration and Institutional Accountability**
Legal Basis: Regulations 15–19
Indicators:

- PDPO registration status
- Appointment of Data Protection Officer
- Internal data governance policies
- Record of processing activities
- Evidence of training

f. **Data Protection Impact Assessments (DPIAs)**
Legal Basis: Regulation 12
Indicators:

- Identification of high-risk processing
- Conduct of DPIAs prior to deployment
- Publication or disclosure of DPIA summaries
- Periodic review mechanisms

High-risk systems monitored include:

- Biometric voter verification systems
- NIN–voter database integration
- Digital voter portals
- Political profiling and AI-assisted analytics

g. **Data Security and Cybersecurity Controls**

Legal Basis: Section 20 DPPA; Regulation 31
Indicators:

- Encryption standards
- Device-level safeguards (BVVKs)
- Rate limiting and scraping prevention
- Audit logging
- Independent security audits
- Breach notification preparedness

h. **Data Sharing and Interoperability**
Legal Basis: Sections 3, 19 DPPA
Indicators:

- Formal data-sharing agreements
- Inter-agency protocols (EC–NIRA)
- Cross-border transfer disclosures
- Adequacy assessments

i. **Storage Limitation and Retention Policies**
Legal Basis: Section 3 DPPA
Indicators:

- Defined retention periods
- Post-election deletion triggers
- Archival policies
- Biometric log disposal mechanisms

j. **Digital Campaigning and Political Profiling**
Legal Basis: Sections 7, 9, 35 DPPA
Indicators:

- Source of voter contact data
- Consent for bulk SMS and automated calls
- Micro-targeting transparency
- Volunteer data processing oversight
- AI-generated content safeguards
- Shadow dataset risks

Political parties assessed as potential data controllers for volunteer-driven processing.

k. **Data Breach Preparedness and Incident Response**
Legal Basis: Section 23 DPPA
Indicators:

- Breach reporting protocols
- PDPO notification evidence

- Containment procedures
- Public communication transparency

l. **Enforcement, Oversight, and Proportionality**
Legal Basis: Part VI DPPA
Indicators:

- Consistency of enforcement actions
- Institutional vs. individual accountability
- Publication of regulatory guidance
- Preventative vs. punitive orientation

v. Scoring Methodology

Each indicator is assessed using a qualitative compliance scale:

Score	Description
0	No evidence of compliance
1	Minimal / informal compliance
2	Partial compliance
3	Substantial compliance
4	Full demonstrable compliance

Scores are aggregated within pillars and translated into:

- Strong Compliance
- Moderate Compliance
- Weak Compliance
- Systemic Non-Compliance

vi. Evidence Collection Methods

The Tool integrates:

- Field Observation Reports
- Stakeholder Questionnaires
- Legal and Regulatory Review
- Public Record Analysis
- Incident Documentation
- Advisory Correspondence Tracking
- Technical Risk Assessments
- Training Participation Records

vii. Preventative and Capacity-Building Components

Beyond monitoring, the Tool was embedded within a broader compliance-strengthening initiative that included:

- National data protection training workshop (30 July 2025)
- Advisory letters to the Electoral Commission (March 2025)
- Advisory letters to all January 2026 participating political parties
- Development of structured compliance questionnaires

– Public-interest documentation of institutional registration status

This integrated approach positioned the Tool not merely as an auditing instrument, but as a governance intervention aimed at improving institutional compliance before and during electoral processing.

viii. **Systemic Risk Lens**

The Tool is grounded in the recognition that:

– Digital elections amplify power asymmetries.

– Biometric systems raise irreversible risk profiles.

– Decentralized campaigning creates shadow data ecosystems.

– Selective enforcement undermines democratic legitimacy.

Accordingly, the Tool evaluates not only legal compliance, but democratic impact.

ix. **Analytical Function**

The Data Protection Election Watch Tool serves three analytical functions:

- **Diagnostic:** Identifying compliance and governance gaps
- **Evidentiary:** Generating documentation for regulatory and parliamentary reform
- **Normative:** Reframing data protection as a structural pillar of electoral integrity

10.4 Annex D: Stakeholder Mapping Table

Stakeholder Category	Specific Stakeholder	Role in 2026 Electoral Cycle	Data Protection Relevance / Risk Profile
Constitutional Electoral Authority	Electoral Commission (EC)	Conducted elections; managed voter register; deployed BVVKs; operated digital voter portals; oversaw results capture and tallying	Primary data controller of voter and biometric data; responsible for lawful processing, retention, transparency, and cybersecurity safeguards
Data Protection Regulator	Personal Data Protection Office (PDPO)	Oversight of data protection compliance; registration of data controllers/processors; enforcement actions	Responsible for regulatory guidance, DPIA oversight, enforcement proportionality, and publication of high-risk processing list
Civil Identity Authority	National Identification and Registration Authority (NIRA)	Managed NIN database; provided identity validation; shared registration kits; integrated civil identity data with voter register	Co-controller/critical data-sharing partner; risks of interoperability, function creep, centralization, and cross-dataset profiling
Political Parties	NRM, NUP, FDC, UPC, JEEMA, PPP and others	Candidate nomination; campaign mobilization; digital messaging; voter outreach	Processed voter contact data; risk of profiling, bulk messaging without consent, decentralized volunteer processing
Candidates & Campaign Teams	Presidential, Parliamentary & Local Council Candidates	Direct voter engagement; use of bulk SMS, calls, targeted ads	Potential data controllers/processors; high risk of informal data ecosystems and consent violations
Technology Vendors	BVVK suppliers; software integrators; system maintenance providers	Supplied biometric kits; configured systems; maintained backend infrastructure	Access to sensitive biometric data; vendor lock-in risks; cross-border hosting and data transfer concerns
Telecommunications Companies	Mobile Network Operators (e.g., MTN Uganda, Airtel Uganda)	Enabled bulk SMS, calls, campaign messaging; managed subscriber data	Custodians of subscriber data; risk of secondary use, political targeting, and metadata exposure

Global Digital Platforms	Meta (Facebook, Instagram, WhatsApp), TikTok, X, YouTube	Hosted political content; enabled targeted advertising; amplified narratives	Algorithmic amplification; AI-generated disinformation; opaque political ad governance
Private Data Intermediaries	Digital marketing firms; analytics providers	Voter segmentation; profiling; micro-targeting; data aggregation	Shadow datasets; profiling of political opinions (special personal data); cross-border transfers
Security Agencies	Police; security intelligence services	Enforcement actions; investigations into alleged data misuse	Access to electoral datasets; potential surveillance risks; enforcement proportionality concerns
Judiciary	Courts; Supreme Court	Adjudicated electoral petitions; interpreted electoral and data protection laws	Oversight of legality; interpretation of ***Section 35*** enforcement and electoral technology disputes
Civil Society Organizations	Unwanted Witness; election observers; digital rights groups	Monitoring; advocacy; legal advisory letters; training workshops; deployment of Watch Tool	Promoted accountability; subject to enforcement risks; strengthened voter data literacy
Election Observers	Domestic and international observer missions	Observed polling and verification processes	Dependent on access to data; affected by transparency and shutdown measures
Voters (Data Subjects)	Registered citizens	Provided biometric data; participated in verification and voting	Rights holders; exposed to profiling, function creep, and data breach risks
Parliament / Policymakers	Parliament of Uganda	Enacted amendments authorizing technology use	Responsible for embedding digital safeguards and oversight mechanisms in electoral law
Media & Journalists	Traditional and digital media outlets	Reported on electoral process and data incidents	Relied on access to information; impacted by shutdowns and enforcement climate
Artificial Intelligence Content Producers	AI tool developers; content creators	Generated synthetic audio, video, and political messaging	Deepfake and disinformation risks using biometric likenesses

Structural Observation

The 2026 electoral ecosystem functioned as an interconnected governance network rather than a linear chain of actors. Control over voter data was distributed across constitutional authorities, civil identity systems, telecommunications infrastructure, global digital platforms, private vendors, and decentralized political actors. However, accountability obligations were unevenly embedded across these stakeholders, contributing to fragmented oversight and asymmetrical enforcement dynamics.

10.1 Annex E: Advisory to Electoral Commission on Compliance with the Data Protection and Privacy Laws of Uganda

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Block 381, Plot No 26, Nsibambi Village
P.O. Box 71314 Clock Tower K"la
Tel: +256 414 697635
Email: info@unwantedwitness..org
Website: www.unwantedwitness.org

Date: 10th March, 2025

ELECTORAL COMMISSION
Security Registry
11 MAR 2025
RECEIVED
P. O. Box 22678, Kampala

Hon. Justice Byabakama Mugenyi Simon
Chairperson, Electoral Commission of Uganda
Plot 1-3/5 Seventh Street Industrial Area
P.O. Box 22678, Kampala, Uganda.

Dear Hon. Justice Byabakama,

Subject: Advisory on Compliance with the Data Protection and Privacy Regulations, 2021

Unwanted Witness is a civil society organization dedicated to advancing **digital rights, privacy, and data protection** in Uganda. Our mission is to promote transparency, accountability, and good governance in the digital era by advocating for policies and practices that safeguard the fundamental rights of citizens.

Following a search through the Personal Data Protection Office (PDPO) public register, we have observed that the Electoral Commission of Uganda is not registered as a data collector, processor, or controller, as required under **Section 29 (2) of the Data Protection and Privacy Act, 2019** and **Regulation 15 of the Data Protection and Privacy Regulations, 2021**. As the body mandated under **Article 61 (1) (a) of the 1995 Constitution of Uganda (as amended)** to ensure free and fair elections, it is imperative that the Commission adheres to **data protection laws** to uphold the integrity of Uganda's electoral processes a head of the 2026 general elections.

To reinforce public trust and ensure a free and fair election, we urge the Electoral Commission under your able leadership to register with the Personal Data Protection Office without further delay. Compliance with this legal requirement will not only fulfill a statutory obligation but also:

1. **Demonstrate Transparency and Accountability** - By registering with the PDPO, the Electoral Commission will publicly affirm its commitment to the lawful handling of personal data, assuring Ugandans that their electoral data is collected, processed, and stored in compliance with established standards.

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Block 381, Plot No 26, Nsibambi Village
P.O. Box 71314 Clock Tower K'la
Tel: +256 414 697635
Email: info@unwantedwitness..org
Website: www.unwantedwitness.org

Date: 10th/ January/2025

Ref No.: *UW/PP-NRM/25/01/042*

NATIONAL RESISTANCE MOVEMENT
Plot 10 Kyadondo Road
10 JAN 2025
P. O. Box 7778 Kampala
SECRETARIAT

Hon. Richard Todwong

The Secretary-General
National Resistance Movement
Plot 10 Kyadondo Rd. Box 7778

Kampala-Uganda

Dear Hon. Todwong,

Re: Advisory on Compliance with Data Protection and Privacy Laws in Preparation for the 2026 General Elections

I hope this letter finds you well. On behalf of **Unwanted Witness**, a civic organization advocating for the protection of privacy and data rights, I would like to extend our gratitude to the National Resistance Movement (NRM) for the crucial role it plays in Uganda's political landscape. We recognize the Party's commitment to democratic processes and the safeguarding of citizens' rights, especially in relation to the forthcoming 2026 General Elections.

As we move toward this significant electoral event, we would like to take this opportunity to advise the NRM on the importance of adhering to the provisions of Uganda's Constitution, the Data Protection and Privacy Act, 2019, and the Data Protection and Privacy Regulations, 2021. These legal frameworks are designed to ensure the responsible collection, processing, and management of personal data, particularly in the context of electoral processes.

Key Provisions for Compliance:

1. ***Article 27 of the 1995 Constitution of Uganda*** guarantees the fundamental right to privacy, including the right not to have personal information disclosed without consent. As a political entity, the NRM is required to respect this right, especially when collecting and processing personal data in electoral activities. This includes voter registration, profiling, and other related processes.
2. ***Regulation 12 of the Data Protection and Privacy Regulations, 2021*** mandates that entities involved in personal data collection to conducting a **Data Protection**

10.7 Annex G: Advisory to National Unity Platform (NUP) on Compliance with the Data Protection and Privacy Laws of Uganda

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Block 381, Plot No 26, Nsibambi Village
P.O. Box 71314 Clock Tower K'la
Tel: +256 414 697635
Email: info@unwantedwitness.org
Website: www.unwantedwitness.org

Date: 10th/ January/2025

Ref No.: *UW/PP-NUP/25/01/043*

Mr. David Lewis Rubongoya

The Secretary-General
National Unity Platform (NUP)
Plot 831/1023 Bombo Road

Makerere-Kavule

NATIONAL UNITY PLATFORM
RECEIVED

Dear David Lewis Rubongoya,

Re: Advisory on Compliance with Data Protection and Privacy Laws in Preparation for the 2026 General Elections

I hope this letter finds you well. On behalf of **Unwanted Witness**, a civic organization advocating for the protection of privacy and data rights, I would like to extend our gratitude to the National Unity Platform (NUP) for the crucial role it plays in Uganda's political landscape. We recognize the Party's commitment to democratic processes and the safeguarding of citizens' rights, especially in relation to the forthcoming 2026 General Elections.

As we move toward this significant electoral event, we would like to take this opportunity to advise the NUP on the importance of adhering to the provisions of Uganda's Constitution, the Data Protection and Privacy Act, 2019, and the Data Protection and Privacy Regulations, 2021. These legal frameworks are designed to ensure the responsible collection, processing, and management of personal data, particularly in the context of electoral processes.

Key Provisions for Compliance:

1. ***Article 27 of the 1995 Constitution of Uganda*** guarantees the fundamental right to privacy, including the right not to have personal information disclosed without consent. As a political entity, the NUP is required to respect this right, especially when collecting and processing personal data in electoral activities. This includes voter registration, profiling, and other related processes.
2. ***Regulation 12 of the Data Protection and Privacy Regulations, 2021*** mandates that entities involved in personal data collection to conducting a **Data Protection**

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Block 381, Plot No. 26, Nsibambi Village
P.O. Box 71314 Clock Tower K'la

Tel: +256 414 697635
Email: info@unwantedwitness.org
Website: www.unwantedwitness.org

Date: 5th January, 2026

Personal DATA Protection OFFICE
05 JAN 2026
RECEIVED
KAMPALA - UGANDA

Ref: UW/DPO/26/01/140

Mr. Baker Birikujja
Director,
Personal Data Protection Office
7th Floor, Padre Pio House, Plot 32 Lumumba Avenue,
Kampala, Uganda

RE: REQUEST FOR REGULATORY GUIDANCE AND LEADERSHIP ON DATA PROTECTION IN ELECTORAL CONTEXTS

Dear Mr. Birikujja,

Unwanted Witness writes to you in the public interest to formally request regulatory guidance and leadership from the Personal Data Protection Office (PDPO) concerning the application of the Data Protection and Privacy Act, 2019 to electoral processes.

We respectfully draw your attention to the enclosed **Position Statement by Unwanted Witness on Public Concerns Arising from the Application of Data Protection Laws in Uganda's Electoral Context**, published on 3 January 2026 and attached hereto for ease of reference. The statement sets out systemic and policy concerns relating to legal certainty, proportionality, institutional accountability, and the protection of civic space. We do not restate its contents here, but instead seek to engage your Office on concrete regulatory actions that fall squarely within its mandate.

As the statutory regulator charged with oversight, guidance, and enforcement of the data protection framework, the PDPO occupies a pivotal role in ensuring that the Act is applied consistently, proportionately, and in a manner that strengthens public trust, particularly during electoral periods where transparency and rights protection must be carefully balanced.

In this regard, Unwanted Witness respectfully requests the PDPO to consider the following **specific regulatory actions**:

1. **Issuance of Written Regulatory Guidance or a Public Advisory**

   We request that the PDPO issue clear, written guidance clarifying the application of the Data Protection and Privacy Act to electoral data. In particular, such guidance should:

Uneven Enforcement of Data Protection Laws Puts Data Subjects' Rights at Risk in Uganda's 2026 Polls

The Unwanted Witness
Bulange, Nsibambi Village P.O.BOX 23184 Kampala – Uganda
Mob: +697635 414-256 Email: info@unwantedwitness.org