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

OFFICIAL STATEMENT

International Data Privacy Week 2026

"Personal Data: Guard it like it is your own"

28 January 2026

Kampala, Uganda | Africa

Unwanted Witness marks International Data Privacy Week 2026 at a moment when questions of personal data, political power, and democratic governance have become inseparable across Uganda and the African continent. As societies become more digitally mediated, personal data increasingly shapes how citizens are identified, receive information, governed, and, in electoral contexts, persuaded or excluded.

This year's theme selected by Personal Data Protection Office, Uganda, **"Personal Data: Guard it like it is your own,"** is both timely and urgent. It speaks to a fundamental principle: personal data is not merely a technical resource or administrative input, it is an extension of human dignity, autonomy, and democratic participation.

Why data privacy matters in Uganda now

Uganda's digital transformation has accelerated rapidly in recent years, spanning national identification systems, biometric voter registration and verification, digital voter registers, electronic results transmission, and data-driven political campaigning. These developments have expanded the scale, sensitivity, and reach of personal data processing by state institutions, political actors, and private intermediaries.

At the same time, enforcement of data protection obligations has remained uneven. While Uganda has a Data Protection and Privacy Act and an operational regulator, compliance gaps, limited sector-specific guidance, and selective enforcement have weakened public confidence. For citizens, this has translated into growing uncertainty about who controls their data, how it is used, and whether it can be misused without consequence.

Data privacy matters now because elections, public services, and political participation are increasingly mediated by digital systems that collect and concentrate sensitive personal and biometric information. Where safeguards are weak, privacy violations risk becoming systemic rather than incidental.

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

Elections, digital campaigning, biometrics, and surveillance

Uganda's 2026 general elections underscored how deeply data has become embedded in the electoral process. Biometric voter verification systems, national identification linkages, digital voter display portals, and electronic transmission tools all relied on the processing of sensitive personal data at unprecedented scale. These technologies were introduced to improve efficiency and credibility, yet they also introduced new vulnerabilities related to data security, transparency, retention, and oversight.

Beyond electoral administration, political campaigning increasingly relied on bulk SMS, automated and Person-to-person calls, social-media targeting, WhatsApp groups, and third-party data analytics. Many citizens reported receiving unsolicited political messages or being added to political groups without consent, raising serious questions about the sources of phone numbers, the lawfulness of data processing, and accountability for misuse.

These practices unfolded against a backdrop of longstanding concerns about surveillance, platform restrictions, and internet shutdowns during election periods. Together, they illustrate how personal data can be repurposed from participation to profiling, from civic engagement to control if not governed by clear, consistently enforced safeguards.

Lessons from the 2026 elections

The 2026 electoral cycle offers critical lessons. First, the existence of data protection law alone is insufficient. Without proactive guidance, institutional compliance, and consistent enforcement, legal protections remain fragile. Second, selective application of data protection where powerful data-holding institutions operate outside core obligations while civic actors face punitive enforcement, undermines both the rule of law and public trust.

Third, biometric and data-driven systems heighten risk when transparency is limited. Voters must be able to understand how their data is collected, used, stored, shared, and ultimately disposed of. In the absence of this clarity, fears of surveillance, profiling, and misuse can chill participation and weaken electoral legitimacy.

Finally, elections demonstrate that data protection is not a peripheral technical issue; it is a democratic safeguard. Where personal data is mishandled, democratic processes themselves are placed at risk.

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

A regional and African perspective

These challenges are not unique to Uganda. Across Africa, states are rapidly adopting biometric identification systems, digital voter technologies, and data-driven governance tools, often faster than regulatory frameworks can mature. Many countries face similar tensions: expanding digital infrastructure alongside weak enforcement, opaque procurement of election technologies, growing reliance on private vendors, and limited public scrutiny.

Africa's democratic future depends in part on whether data protection frameworks evolve as instruments of empowerment rather than control. Data protection must serve to constrain power, protect civic space, and uphold human dignity, not to silence scrutiny y or legitimize unchecked data accumulation.

Calls to action

As we commemorate International Data Privacy Week 2026, Unwanted Witness calls for the following actions:

- **To Government and Electoral Authorities:** Lead by example through full compliance with data protection laws, including registration, publication of privacy notices, conduct of data protection impact assessments, and transparent governance of electoral technologies.
- **To the Personal Data Protection Office and Regulators:** Issue clear, election-specific guidance on biometric systems, political campaigning, and third-party data processing, and apply enforcement consistently across all actors, public and private.
- **To Political Parties and Candidates:** Respect consent, transparency, and purpose limitation in all forms of digital campaigning. Personal data must not be treated as an unlimited campaign resource.
- **To African Policymakers and Institutions:** Invest in regulatory capacity, regional cooperation, and shared standards to ensure that digital elections strengthen, rather than undermine, democratic governance.

Conclusion

International Data Privacy Week 2026 is a reminder that personal data is inseparable from personal freedom. Guarding personal data "like it is your own" requires more than awareness, it requires accountability, restraint, and

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

respect for the rights of citizens.

Unwanted Witness reaffirms its commitment to advancing data protection as a cornerstone of democratic integrity in Uganda and across Africa. We stand ready to work with governments, regulators, civil society, and regional partners to ensure that the digital future of elections is rights-respecting, transparent, and worthy of public trust.