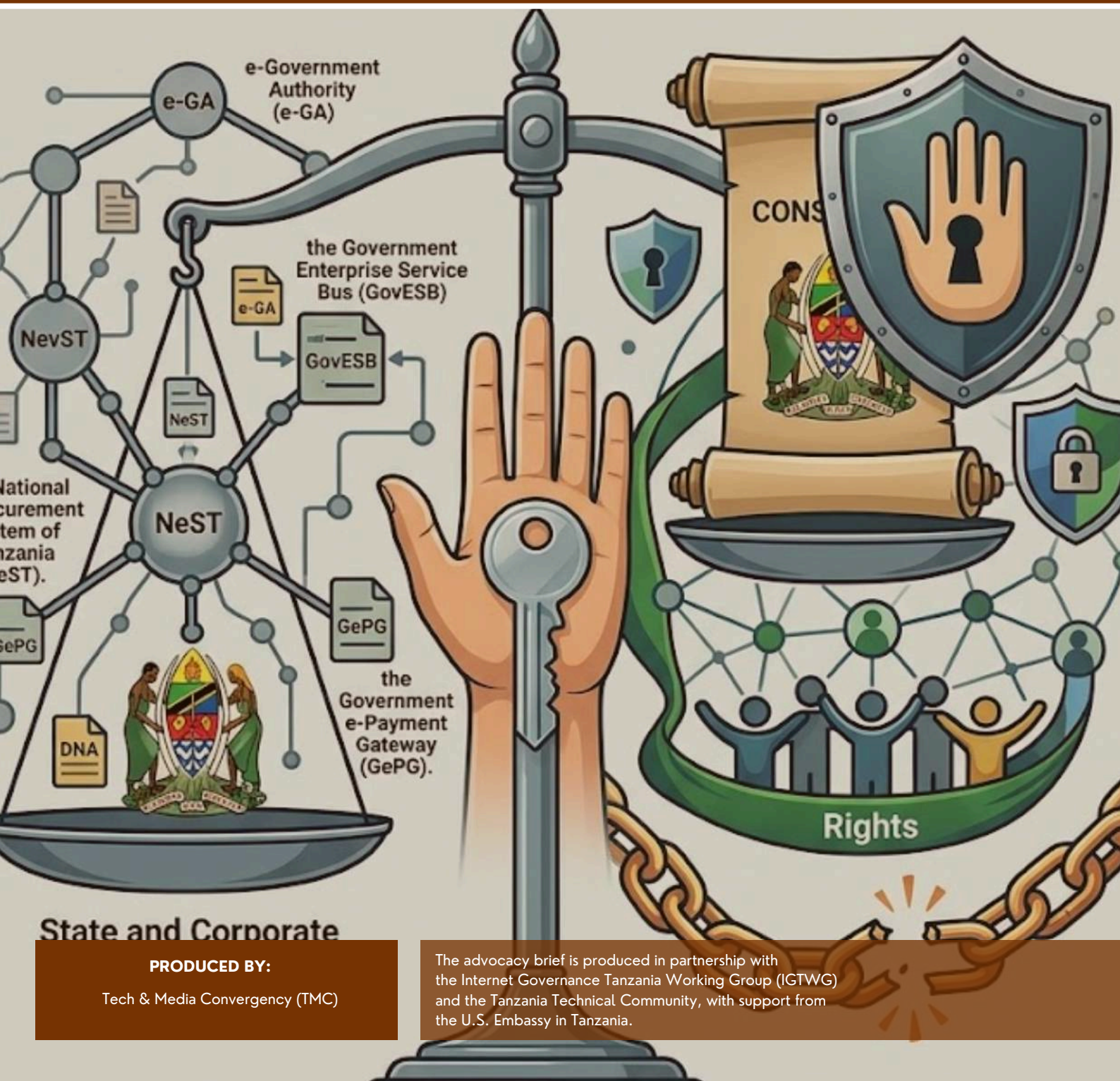


ADVOCACY BRIEF

Tanzania State of Internet Governance Series

Beyond Compliance: Building Data Minimization and Privacy into Tanzania's Digital Systems

ISSUE 11: OCTOBER 2026



PRODUCED BY:

Tech & Media Convergence (TMC)

The advocacy brief is produced in partnership with the Internet Governance Tanzania Working Group (IGTWG) and the Tanzania Technical Community, with support from the U.S. Embassy in Tanzania.



ISSUE 11: OCTOBER 2026

About the Tanzania State of Internet Governance Series

The Tanzania State of Internet Governance Series is a comprehensive monthly initiative that examines the current landscape of Internet governance in Tanzania. It highlights key issues, challenges, and opportunities in digital governance, policy frameworks, cybersecurity, and digital rights. Through expert insights and data-driven analysis, the series aims to inform stakeholders, policymakers, and the public about critical trends shaping the country's digital future and digital economy. It promotes transparency, accountability, and inclusive decision-making in Internet governance. The series is part of the Tanzania Digital Collaboration Program, supported by the U.S. Embassy in Dar es Salaam, in collaboration with the Bureau of African Affairs at the U.S. Department of State.

About the Internet Governance Tanzania Working Group (IGTWG)

The Internet Governance Tanzania Working Group (IGTWG), led by civil society and coordinated by Tech & Media Convergence (TMC), comprises 25 organizations from Tanzania Mainland and Zanzibar. It promotes data governance, inclusivity, equitable internet access, and responsible usage while advocating for policy reforms to shape Tanzania's digital landscape.

About the Tanzania Technical Group

The Tanzania Technical Group draws from independent Tanzanian ICT experts, lawyers, policymakers, researchers, Social Media Activists, Communication Specialists, civil society organizations, and digital governance specialists to foster innovation, ensure sustainable development, and provide knowledge for informed policy briefs.

1. Introduction and Contextual Overview

The contemporary Tanzanian state is aggressively executing an epochal transition from paper-based bureaucracy to an omnipresent digital administrative apparatus. Coordinated by the e-Government Authority (e-GA), and facilitated by enterprise-scale platforms such as the Government Enterprise Service Bus (GovESB), the National e-Procurement System of Tanzania (NeST), and the Government e-Payment Gateway (GePG), this structural modernization has been heavily celebrated for unlocking administrative efficiency. However, this rapid digitization has quietly nurtured a profound, systemic pathology: the unexamined expansion of state and corporate appetites for citizen data, driven by technological determinism rather than necessity^[1].

Tanzania took a decisive step toward informational self-determination through the enactment of the Personal Data Protection Act (PDPA), No. 11 of 2022,^[2] operationalized by the Personal Data Protection (Personal Data Collection and Processing) Regulations of 2023^[3] establishing the Personal Data Protection Commission (PDPC).^[4] Despite this framework, a dangerous chasm persists between legislative proclamation and technical reality. As identified in the Tech & Media Convergency (TMC) Focus Group Discussion (FGD), the prevailing compliance culture has degenerated into procedural ritualism often a mere "tick-box" exercise while the underlying code remains aggressively extractive.^[5]

This policy brief addresses the core inquiries of the TMC Technical Group, tackling the doctrinal test of necessity, the architecture of coerced consent, the jurisprudence of systemic liability, the data lifecycle dilemma, and the co-regulatory mandate of the PDPC^[6]. Furthermore, it addresses critical contemporary issues including corporate data over-extraction, political dissonance regarding the National Identification Authority (NIDA) identity framework, and the panoptic threat of mandatory electronic payments under Government Notice (GN) No. 158C of 2026.^[7] Ultimately, this brief formulates actionable recommendations, notably urging the PDPC to issue explicit guidelines on data minimization and to enforce Privacy by Design and by Default (DPbDD) architectures to ensure the nation's digital transformation is realized without compromising fundamental privacy rights.

This structural tension is further compounded by a severe institutional imbalance between the speed of algorithmic rollout and the capacity for regulatory oversight. While state agencies and corporate actors rapidly deploy centralized, data-hungry systems under the banner of national modernization, the PDPC faces the uphill battle of establishing its enforcement authority against well-entrenched institutional habits. Without immediate structural interventions such as mandatory data protection impact assessments (DPIAs) prior to digital platform deployment and strict legal sanctions for silent scope creep, the architecture of digital governance risks transforming from a tool of public empowerment into an unchecked apparatus of digital surveillance. Consequently, bridging the gap between legislative intent and system design is not merely a technical imperative, but a foundational requirement to preserve civil liberties in Tanzania's digital age.

^[1] [DATA COLONIALISM: ARE BIG TECH COMPANIES BECOMING THE NEW SOVEREIGNS?](#)

^[2] [The Personal Data Protection Act \(PDPA\)](#), No. 11 of 2022.

^[3] [The Personal Data Collection and Processing Regulations](#), 2023.

^[4] [The Personal Data Protection Commission \(PDPC\)](#).

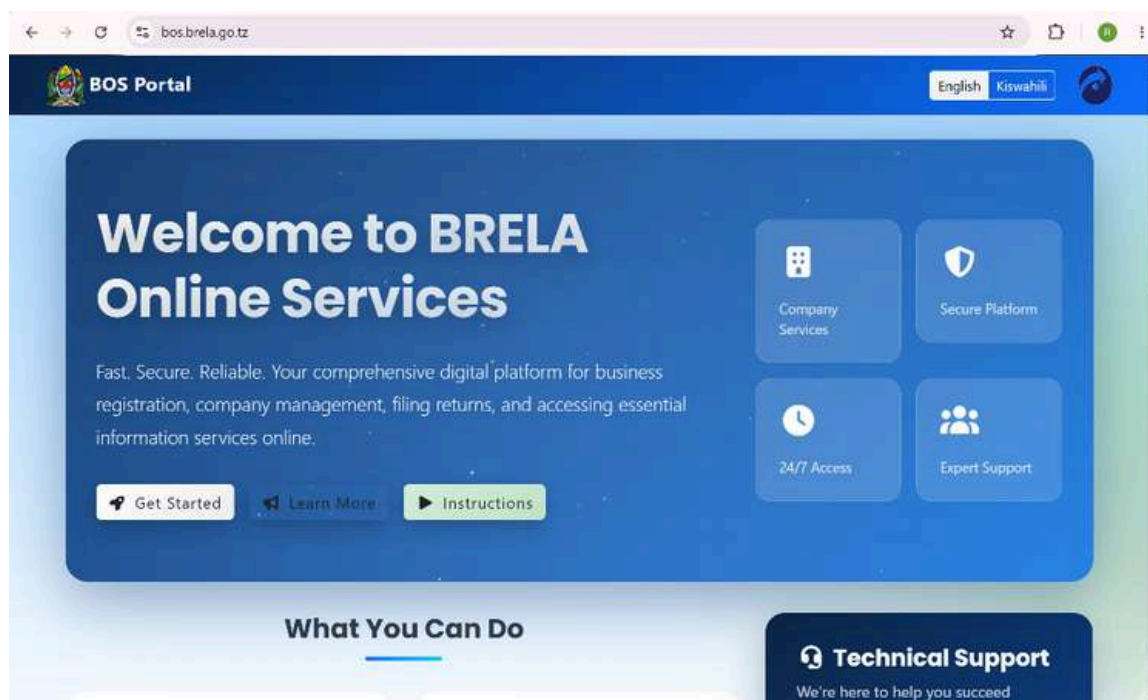
^[5] Georgios Kominis, et.al. [Systemic Imbalances in Integrity Management Systems: A Meso-Level Framework From Four Corruption Scandals](#).

^[6] Tech & Media Convergency (TMC) Focus Group Discussion (FGD) held on 11th September at TMC HQ.

^[7] See: [The Electronic Transactions \(Mandatory Electronic Payments for Specified Transactions\) Order, \(GN\) No. 158C of 2026](#).

2. Contextual Analysis and Justification

Across both public and private spheres, the interface between the Tanzanian citizen and institutional authority has been radically digitized. From registering a business entity via the Business Registrations and Licensing Agency (BRELA) to accessing sovereign registries and telecommunications networks, citizens must navigate an intricate labyrinth of centralized data repositories.



While Section 5 of the PDPA 2022 mandates that data processing must be lawful, fair, transparent, and limited to what is adequate, relevant, and strictly necessary, developers and procurement officers lack enforceable technical benchmarks.^[8] Data controllers frequently believe that paying registration fees to the PDPC, appointing a nominal Data Protection Officer (DPO),^[9] and displaying opaque "Terms and Conditions" notices constitutes full compliance. Meanwhile, as highlighted in the FGD, institutions collect vast amounts of personal information including mother's maiden names, expansive familial relationships, and biometric markers not because it is strictly necessary, but simply because digital storage is economically negligible and modern code makes collection frictionless.^[10]

True informational privacy cannot be achieved by retrofitting legal disclaimers onto fundamentally invasive software after deployment. As posited in the doctrine of Privacy by Design, privacy must begin before the system ever asks for the data.^[11]

3. The Policy Problem: The "Collect First, Justify Later" Syndrome

Tanzania's digital expansion is currently constrained by systemic design failures that actively subvert the right to privacy enshrined in Article 16 of the Constitution of the United Republic of Tanzania.^[12]

3.1 The Inversion of Necessity and the Doctrinal Test

The primary vulnerability is the inversion of necessity. System architects routinely approach database design by asking, "What data can we technically capture?" rather than, "What minimal data is strictly indispensable to achieve this specific public purpose?". This creates massive, vulnerable data lakes ripe for function creep.

As debated in the FGD, establishing a Doctrinal Test of Necessity is paramount. The PDPC must translate the broad principles of Section 5 of the PDPA into an enforceable "Necessity and Proportionality Test" that halts unnecessary

^[8] Section 5 of the Personal Data Protection Act 2022.

^[9] PDPC: [Data Protection Officer](#).

^[10] Insights from the Tech & Media Convergency (TMC) Focus Group Discussion (FGD) held on 11th September at TMC HQ.

^[11] Also see: [Privacy By Design: The Seven Foundational Principles](#). By Dr. Ann Cavoukian.

^[12] Article 16 of the Constitution of the United Republic of Tanzania.

collection before code deployment.^[13] Tanzanian policymakers can draw vital jurisprudential guidance from the Canadian Federal Court case *Eastmond v. Canadian Pacific Railway (2004 FC 852)*,^[14] which established a stringent four-part test determining if data collection is legally justifiable:

1. Is the measure demonstrably necessary to meet a specific need?
2. Is it likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?^[15] Subjecting public portals to this test would drastically reduce the extractive scope of Tanzanian digital systems.

3.2 Coerced Consent and the Architecture of Defaults in Monopolistic Systems

The second failure involves the architecture of defaults and coerced consent. When a citizen interacts with essential public registration portals (e.g., tax, business licensing, land registries) where no market alternatives exist, the doctrine of "freely given consent" collapses. When citizens have no alternative channel to exercise a civic right, mandatory fields cease to be an agreement and become coerced administrative extraction.

During the FGD, participants noted the severe complexities of internet accessibility and public sector data processing, citing a past instance of a five-day internet shutdown that disrupted proactive practices and access to critical services. In monopolistic environments, technical standards must be imposed to ensure that privacy-protective settings are activated by default, and that optional data fields are visually, legally, and functionally distinct from mandatory fields to dismantle the legal fiction of consent.

3.3 The Lifecycle Dilemma: Taming Indefinite Data Retention

A frequently ignored component of data minimization is storage limitation.^[16] Given that the economic cost of cloud storage tends toward zero, state data lakes and commercial servers universally lack automated mechanisms to enforce the right to erasure.

The FGD highlighted the urgent necessity of addressing this lifecycle dilemma, particularly concerning the sensitive tracking and record management of minors and children with offenses in coordination with the police.^[17] Retaining such highly sensitive personal statements and records indefinitely without cryptographic shredding, redaction, or anonymization once their primary administrative purpose has lapsed constitutes a severe violation of the PDPA.^[18] Systems must be compelled to automate data deletion routines to protect vulnerable demographics from permanent digital stigmatization.

4. The Jurisprudence of Systemic Liability and ICT Procurement

Addressing the jurisprudence of systemic liability requires shifting the burden of compliance to the point of software procurement. State and private ICT procurement evaluate systems almost exclusively on financial cost and functional uptime, systematically ignoring mandatory *Data Protection Impact Assessments (DPIAs)* and contractual exit rights. The National e-Procurement System of Tanzania (NeST), operated by the Public Procurement Regulatory Authority (PPRA), mandates the end-to-end digital submission of sensitive corporate and financial data.^[19] While NeST has improved efficiency and reduced paper-based carbon emissions, its procurement frameworks must be reformed. Where should legal liability sit when an ICT vendor delivers a digital architecture that violates data minimization? As proposed in the FGD, PPRA policies must be reformed to mandate DPIAs involving technical developers from the outset as an absolute statutory condition for contract awards.

Furthermore, FGD participants identified autonomous cyber attacks as a critical issue requiring immediate reflection and engagement. Unminimized data repositories are highly lucrative targets for systemic cyber attacks. Procurement standards must demand that vendors implement appropriate technical guidelines and testing to mitigate these autonomous threats, holding vendors jointly liable for delivering inherently insecure code.^[20]

^[13] Insights from the Tech & Media Convergency (TMC) Focus Group Discussion (FGD) held on 11th September at TMC HQ.

^[14] *Eastmond v. Canadian Pacific Railway (2004 FC 852)*.

^[15] Priolaw: *Employee Screen-Monitoring Software May Breach*.

^[16] *Data protection laws in Tanzania*.

^[17] CYRILLA, *The Personal Data Protection Act 2023*.

^[18] *Tanzania Data Protection Laws Overview*.

^[19] *The Foundation For E-Procurement in Tanzania - Final – Copie*.

^[20] Insights from the FGD.

5. Mismatches in Political Pronouncements: The NIDA Identity Crisis

The effective implementation of DPbDD requires a coherent understanding of statutory definitions across all branches of government. A significant epistemic crisis arose when the Minister for Home Affairs, Patrobas Katambi, publicly declared that the National Identification Authority (NIDA) identity card does not constitute "personal data".^[21] The Minister argued that because the card is heavily used in daily life from registering SIM cards to land sales it is a "public document" and that basic particulars like age and residence are public knowledge, stating colloquially, "ni public na ndio maana mnasheherekea birthday" (it is public, which is why you celebrate birthdays).^[22]

This political rhetoric stands in dangerous contradiction to Section 3 of the PDPA 2022, which unequivocally defines "personal data" as information about an identifiable person, explicitly enumerating identification numbers, ages, and addresses. Furthermore, the PDPA classifies biometric data (fingerprints) as highly protected "sensitive personal data".^[23] The second and third-order implications of this political dissonance are severe. When executive authorities incorrectly declare national IDs to be "public," private data controllers are implicitly encouraged to abandon data security protocols, normalizing the reckless photocopying and unencrypted storage of NIDA cards. As noted during the FGD, current Tanzanian banking procedures strictly rely on fingerprint verification as the ultimate proof of existence for critical financial accounts. If the foundational document of this financial verification process is treated as public information, the integrity of the entire banking and Anti-Money Laundering (AML) sector is structurally compromised.

6. The Panoptic Threat of Mandatory Electronic Payments (GN No. 158C)

A critical focal point for contemporary data protection policy in Tanzania is the intersection of sovereign financial digitization and citizen privacy, specifically triggered by the Electronic Transactions (Mandatory Electronic Payments for Specified Transactions) Order, 2026, under Government Notice No. 158C.^[24] Coming into operation on July 1, 2026, with a transitional window ending December 31, 2026, the Order mandates that payments for a highly expansive list of specified daily transactions ranging from bus transit and ferry tolls to accommodation and retail shopping must be made exclusively through electronic means, heavily utilizing the Government electronic Payment Gateway (GePG).

While aimed at tax traceability and financial inclusion, GN 158C eradicates transactional anonymity. Every payment falling within the expansive Schedule now sits permanently on a digital ledger, attributable to an identifiable payer.^[25] The implementation of mandatory electronic payments acts as a catalyst for unprecedented mass data accumulation, leaving vast amounts of behavioral data "hanging" and vulnerable to severe misuse.

This mandate operates atop the highly rigid Electronic and Postal Communications (SIM Card Registration) Regulations, 2020 (GN No. 112 of 2020), which requires biometric registration of all SIM cards linked to NIDA.^[26] Because the 2020 Regulations strictly criminalize registering a SIM card on behalf of another individual (Regulation 4(4)), a citizen is forced into an inescapable chain of identity linkage.^[27] They must use their biometrics to get a SIM, and that specific SIM to make the mandatory GN 158C payments. This highly integrated chain vastly increases the severity of function creep, allowing state entities and Mobile Network Operators (MNOs) to build comprehensive behavioral, geographical, and economic profiles of citizens without specific warrants, thereby risking violations of Article 16 of the Constitution.

7. Comparative Jurisprudence

As Tanzania seeks to secure its digital economy and national identity ecosystems, it is vital to examine regional regulatory peers. A prime example is the Office of the Data Protection Commissioner (ODPC) in Kenya, accessible via their official portal at <https://www.odpc.go.ke/>.^[28] Established to enforce Kenya's Data Protection Act, 2019, the ODPC provides actionable, regulatory case studies on how to transition from nominal compliance to active enforcement and privacy-by-design.^[29] Tanzania's PDPC can draw several critical lessons from the ODPC's robust regulatory toolkit.

^[21] JamiiForums. [Waziri Patrobas Katambi: Kitambulisho cha NIDA sio taarifa binafsi.](#)

^[22] Ibid.

^[23] [Tanzania Personal Data Protection Act.](#)

^[24] The Electronic Transactions (Mandatory Electronic Payments for Specified Transactions) Order, 2026, under Government Notice No. 158C.

^[25] BowmansLaw "[Tanzania: Electronic payments mandated for specified transactions](#)".

^[26] [The Electronic and Postal Communications \(SIM Card Registration\) Regulations, 2020](#) (Government Notice No. 112 published on February 7, 2020).

^[27] FB Attorneys, [Registering a SIM card for a friend.](#)

^[28] Securiti.ai, [Kenya Data Protection Act 2019 \(DPA\) Compliance Guide.](#)

^[29] Ibid.

7.1 Mandatory DPIAs and Enforcement Penalties

A core element of the ODPC's strategy is the rigid enforcement of Data Protection Impact Assessments (DPIAs). The Kenyan ODPC has explicitly outlined that any high-risk processing activity such as the large-scale processing of sensitive data or the deployment of new technologies must undergo a rigorous DPIA that assesses data necessity and proportionality.^[30] The ODPC has made it clear that the mere absence of DPIA documentation is in itself a compliance failure, and it has issued substantial financial penalties running into millions of shillings against Kenyan businesses for unauthorized data extraction and failing to mitigate risks.^[31] This active enforcement demonstrates that regulatory bodies must penalize the architecture of extraction and poor planning, not just react to eventual data breaches.

7.2 Proactive Sector-Specific Guidance Notes

Rather than relying solely on broad legislative texts, the Kenyan ODPC proactively published comprehensive, sector-specific guidance notes to aid organizational compliance across healthcare, finance, education, and technology.^[32] For instance, their technology sector guidance emphasizes the absolute necessity of privacy by design and default, secure software development, and data minimization from the very outset of system creation^[33]. Their guidance on DPIAs further operationalizes the principles of purpose limitation and storage limitation, ensuring data is deleted or anonymized once its primary purpose is served.^[34] By providing these granular guidelines, the ODPC has successfully bridged the gap between legal theory and technical implementation a model that Tanzania's PDPC must urgently replicate.

8. Cryptographic Solutions: Privacy-Preserving Architecture

To definitively dismantle the "Collect First, Justify Later" paradigm and address the architecture of defaults in monopolistic systems, Tanzania must transition its focus to technical compliance embedded directly in code.

One of the most promising architectural solutions is the integration of Zero-Knowledge Proofs (ZKPs), Differential Privacy, and Verifiable Credentials. Under a Zero-Knowledge Proof Know-Your-Customer (ZK-KYC) mechanism, a user can mathematically prove to a verifier that a specific statement is true (e.g., "I am over 18" or "I hold a valid digital identity") without revealing the underlying data used to generate the proof.^[35]

By leveraging standards such as the W3C Verifiable Credentials Data Model, Tanzanian institutions could issue digital credentials that allow citizens to selectively disclose only the strictly necessary attributes required for a transaction. This approach inherently satisfies the PDPA's data minimization mandate and neutralizes the threat of secondary data harvesting. Additionally, for macro-level state analytics via the GePG, the government must implement Differential Privacy adding mathematical noise to datasets to ensure that macroeconomic trends can be extracted without re-identifying specific individuals.^[36]

9. Strategic Policy Interventions and the Co-Regulatory Mandate of the PDPC

The Personal Data Protection Commission (PDPC) possesses immense statutory authority, but overcoming institutional inertia requires targeted, co-regulatory strategies that bridge the gap between legal mandates and software engineering.^[37] To answer the FGD's inquiries regarding the PDPC's co-regulatory mandate, TMC recommends the following urgent policy interventions:

9.1 PDPC Guidelines on Data Minimization (FGD Primary Recommendation)

As explicitly recommended during the FGD, data minimization must be formally established as a priority requirement for institutional compliance. The PDPC must urgently draft, publish, and enforce explicit "Guidelines on Data Minimization and Privacy by Design." These guidelines should mandate institutional policies ensuring clear security and minimization standards across all government and private entities, putting an end to arbitrary data hoarding.

^[30] Ibid.

^[31] Securezaidi, [How to Conduct a DPIA Under the Kenya Data Protection Act](#).

^[32] ODPC Kenya, [ODPC Releases Sector-Specific Guidance Notes for Compliance](#).

^[33] Ibid.

^[34] [DPIA ODPC Guidelines KE DPIA Guidelines From KE ODPC](#).

^[35] ResearchGate ["Binding Verified Digital Identity Credentials to Large Language"](#).

^[36] DPF, [Differential Privacy for Databases](#).

^[37] Magist, [Tanzania PDPA requirements for apps in Tanzania, 2026](#).

9.2 Mandating the Doctrinal Test of Necessity

The PDPC must translate Section 5 of the PDPA into an enforceable "Necessity and Proportionality Test," modeled on the Eastmond criteria. Before any state portal or private platform is deployed, the data controller must algorithmically and legally prove that every requested data field is genuinely necessary for the specific transaction.

9.3 Overhauling ICT Procurement and Systemic Liability

The jurisprudence of systemic liability must be shifted to the point of public procurement. The PPRA must reform standard bidding documents within NeST to mandate Data Protection Impact Assessments (DPIAs) as an absolute statutory condition for contract awards, ensuring that technical developers integrate privacy at the architecture level. Vendors who deliver non-compliant code lacking automated deletion routines should bear joint liability for subsequent data breaches.

9.4 Accountability Check for Private Sector DPOs

As raised in the FGD, the PDPC must conduct an immediate "Accountability Check" to determine the actual number and technical capacity of Data Protection Officers currently working in the private sector. Current compliance is largely nominal; verifying the existence of technically proficient DPOs is critical to ensuring operational transparency and accountability in ongoing data protection efforts.

9.5 Institutional Communication and Sandboxes

The FGD highlighted that institutional structures in the digital age are horizontal rather than vertical, necessitating improved inter-institutional communication for security coordination. The PDPC should establish regulatory sandboxes where organizations can test privacy-preserving architectures in a safe environment. Improved communication channels between institutions will also enhance defenses against the systemic, autonomous cyber attacks threatening Tanzania's data infrastructure.

9.6 Reconciling Political Directives and Mitigating GN 158C

High-level state officials must undergo data privacy literacy programs to prevent the mischaracterization of foundational systems like NIDA, harmonizing political rhetoric with the PDPA. Concurrently, to mitigate the surveillance risks of GN 158C, the Ministry of Finance and e-GA must implement robust pseudonymization and differential privacy protocols within the GePG network to shield citizens' low-value transactional metadata from unauthorized behavioral tracking.

10. Conclusion

The United Republic of Tanzania stands at a critical juncture. The aggressive digitization of civic, financial, and administrative life has unlocked remarkable efficiencies but has dangerously normalized a culture of systemic data extraction. While the enactment of the Personal Data Protection Act of 2022 represents a commendable milestone, true informational self-determination requires a fundamental paradigm shift from post-deployment procedural compliance to Data Protection by Design and by Default.

By enforcing rigorous necessity tests, integrating zero-knowledge cryptographic proofs, overhauling public procurement standards, establishing horizontal institutional coordination, and issuing explicit PDPC guidelines on data minimization, Tanzania can dismantle the "Collect First, Justify Later" syndrome. Only by embedding privacy directly into the digital bedrock can the state ensure its rapid technological advancement empowers citizens rather than subjects them to a pervasive digital panopticon.

Contact Information

Tech & Media Convergency (TMC)

Mikocheni B Plot no 35,
Block A, Post Code - 14112
House no MKC/MCB/5
Rose Garden Rd,
Dar es Salaam, Tanzania

E: info@mediaconvergency.co.tz
M: +255 764 477 927



@mediaconvergency

 linktr.ee/mediaconvergency