THE DATA GOVERNANCE IN AFRICA RESEARCH FUND

Examining Sensitive Personal Data Protection and Data Sovereignty in Zambia

Author: **Emsie Erastus**
Contact: **emsieerastus[at]gmail[dot]com**

Research Support Team

Field Researcher:
Nyambe Jere

Peer Reviewer:
Esther Mwema

Layout Design
Chiedza Kehle

ABOUT THE AUTHOR

Emsie Erastus is a result-oriented Tech Rights Specialist with over 10 years' experience spanning journalism, policy and human rights. She is listed among the 100 Global Brilliant Women in AI Ethics (2024) and was nominated for the Women in Tech Global Africa 2025 Awards in the Tech Diplomacy category for her contributions to AI ethics, data protection and tech policy. Emsie holds an MSc in Media and Communications (with Distinction) from the London School of Economics and Political Science (LSE).

Disclaimer

This paper was produced as part of the Data Governance in Africa Research Fund, which is jointly supported by Mozilla Foundation and GIZ African Union under the Data Governance in Africa Initiative. The Initiative is financed by the European Union, Germany, Belgium, Estonia, Finland and France under the Digital for Development (D4D) Hub. The contents of this paper are the sole responsibility of the author and do not necessarily reflect the views of the funders.

ABSTRACT

In 2021, Zambia enacted its Data Protection Act, which stipulates that sensitive personal data, such as health records, biometrics, religious beliefs, and political opinions, must be stored within the borders of the country. The law further seeks to protect Zambia's data sovereignty in a world where data, including sensitive personal data,is often viewed as an economic resource. This raises questions about how data sovereignty can be guaranteed in an era of cross-border data flows and Western influence. Furthermore, how does Zambia's data protection law strike a balance between innovation, human rights, and data sovereignty when it comes to sensitive personal data?

Based on a survey of 33 organisations from Zambia, this research explores the opportunities and challenges associated with protecting sensitive personal data in Zambia. The study presents a critical assessment of cross-border data flows of sensitive personal data and critiques the model of data embassies, which advocate for the storage of sensitive personal data abroad.The study is informed by regional frameworks set out by the African Union (AU), including the AU Data Policy Framework (DPF), the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), and the African Charter on Human and Peoples' Rights (ACHPR). It further reviews the challenges and opportunities faced by Zambia's Data Protection Commission (DPC) in implementing the national Data Protection Act.

The study provides empirical data and policy contributions to local and international discourse on African data futures and how Zambia can serve as an example for other African nations seeking to protect and store sensitive personal data within their borders.

Table of Contents

INTRODUCTION

"As long as you speak my name, I shall live forever"

- African Proverb

Data has been described as "gold" or other valuable minerals and resources by organisations such as the World Economic Forum (2020). Most technologies today rely on this 'resource' to function; however, unlike natural resources, a lot of data extracted today comes from people. Thus, the concept of data protection is not simply a governance or technical issue; it is deeply human. To understand why this 'resource' needs to be protected, it is important to understand what data protection means and why it is a human rights matter.

In many African cultures, a name is sacred, representing belonging and identity. It embodies stories, beliefs, and connections between people, and defines personal identity. Protecting names and other related personal information is a means of respecting and maintaining privacy; thus, abuse or unauthorised exposure undermines social trust and violates personal dignity.

For example, in Oshiwambo[1], the concept of a mbushe, or namesake, goes far beyond just sharing a name. When a child is born, they are often given a name of a living or deceased relative, and it is believed that the newborn will carry on that person's legacy and characteristics (Ndakalako, 2023). Thus, a name carries weight, and it should not simply be viewed as a resource or data to profit from. It is in line with such cultural concepts that African nations, such as Zambia, have formulated and enacted data protection laws to safeguard sacred and sensitive personal information.

At a continental level, article 14(6)(a) of the Malabo Convention calls on State Parties to prohibit any data collection and processing of sensitive information revealing racial, ethnic, and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life, genetic information or, more generally, data on the state of health of the data subject.

Furthermore, the extraction and storage of sensitive personal data has gone beyond the collection of names. In emerging tech, information related to biometrics, geolocation, and other digital identifiers is being monetised, which compels nations globally to protect their citizens' data more strictly.

[1] Language spoken in Northern Namibia and Southern Angola

The AU DPF further recommends that governance mechanisms and policies should enable the development of category and sector-specific data governance for children's data, health data, and other kinds of sensitive data or sector-specific data that warrant distinct treatment through processes that are in accordance with the principles in the DPF.

Zambia's Data Protection Act, No. 3 of 2021, represents adherence to the AU's frameworks, such as the Malabo Convention. Through the Act, a juridical framework is established, ensuring that sensitive personal data must be stored and processed within the country's borders. However, the localisation process faces challenges, since data often flows through global data centres and is often dictated by large foreign tech companies. Thus, this research paper examines this dynamic by asking: how can data sovereignty of sensitive personal data be guaranteed in an era of cross-border data flows and data embassies? How does Zambia's data protection approach balance innovation, human rights, and data sovereignty as far as sensitive personal data is concerned?

The study begins with a literature review, which examines some of the normative approaches of data protection in Africa, the connection between indigenous values of personhood and data governance. It then places the national approach of Zambia in the context of continental and global discussions on data sovereignty, critically examining the functions of the AU DPF, the Malabo Convention, and the Zambian Data Protection Act.

The study is not only timely but also crucial given continental developments. It challenges existing discourses that African countries should cede control over sensitive personal data to foreign actors, and instead offers its solutions with Africa in focus, focusing on local realities, respect for cultural values, and global human rights principles. As such, Zambia's experience can offer valuable lessons to other African nations that strive to protect sensitive information in a globalised digital environment.

LITERATURE REVIEW

The concept of data protection should be situated within the socio-cultural context of many African societies through an academic analysis of privacy and data governance. In such contexts, the protection of personal data is not only framed as an individual right, but also as relational and communitarian, tied to conceptions of personhood, social harmony, and duties owed within networks of family and community (Boshe, 2024; Nwoye, 2017).

This framing is echoed in scholarship that interrogates whether, and how, privacy in Africa should be understood beyond purely liberal-individualist accounts, including debates that caution against treating African societies as culturally static while still recognising the normative relevance of communitarian ethics (Makulilo, 2016). While it goes beyond the scope of this paper to explore everything of reference to Africa's stance on data protection, an example of this is the fact that much attention is given to the name of a person since it carries with it a sense of identity, belonging, and dignity (Udechukwu & Nnyigide, 2025). The disclosure or exposure of such an identifier without consent is viewed as a violation of social trust and individual respect (Kinyua, 2025). This normative framework is in line with human rights principles on data protection, which place strong emphasis on dignity and autonomy.

AU Data Policy Framework and the Malabo Convention

The African Union Data Policy Framework (AU DPF), adopted in 2022, and the Malabo Convention, adopted in 2014, are the most important continental tools of data governance by the African Union, but there is a big difference in terms of legal authority. The AU DFP is a policy framework that states a common vision and makes recommendations to Member States. It is not a binding treaty, thus depending on domestic absorption and implementation by national laws and regulatory bodies (AU DPF, 2022).

The AU DPF directly addresses the fact that confidence in the data ecosystem in Africa lies in the strong personal protection of data and numerous times reiterates that sensitive categories of data require increased protection. As one example, it acknowledges that sensitive data in most cases attract stricter cross-border regulation compared to non-personal data, and suggests category and sector-specific regulation in such areas as children's data and health data, without promoting silos or piecemeal compliance (AU DPF, 2022).

The AU DPF, however, was more focused on sensitive data using broad governance instruments, such as categorisation, data specificity, sectoral codes, and so-called trust models, instead of making firm minimum requirements in terms of permissible processing or conditions of such processing (AU DPF, 2022). As a result, in the context of scholarship about sensitive personal data (information), this difference is more consequential: according to the AU DPF, policy guidance is provided, but the national system is given significant freedom in its activities, which leads to the potential of uneven protection and deprives the country of cross-border confidence.

Conversely, the Malabo Convention (2014) gives direct and specific legal principles for the protection of personal information and even sensitive personal information, and is designed to serve as a harmonising legal framework to domestic laws. It provides the definition of sensitive data and lists certain principles of its processing in Article 14, such as a strong prohibition foundation and a narrow range of exceptions (Malabo Convention, 2014). Article 1 (Definitions) explicitly defines "Sensitive data" as a subset of personal data (covering, among other things, political opinions, religious or philosophical beliefs, trade union membership, sex life, race, health, social measures, legal proceedings, and penal or administrative sanctions).

The Convention also stipulates enforceable data-subject rights, such as the right to information, the right of access, the right of objection, and the right of rectification or erasure, and the fundamental obligations of controllers to implement, which is the rights-based approach based on dignity and autonomy (Malabo Convention, 2014). Most importantly, as a treaty, the Malabo Convention is binding only to those Member States that ratify it. This juristic status demonstrates the reason why Malabo is at liberty to establish sensitive-data rules in a way that the AU DPF is incapable of, and thus amplifies the criticism of the latter.

Accordingly, this paper supports Zambia's sovereign right to control sensitive personal data within its jurisdiction, including through localisation or in-country handling requirements where the Zambia Data Protection Act, 2021, and related national measures so provide (Republic of Zambia Data Protection Act, 2021).

The paper argues that sensitive personal data (information) should be subject to stricter control measures. This position is to an extent also consistent with the AU DPF's recognition of sovereignty and data control as legitimate governance objectives, particularly where such control is necessary to protect rights, security, and the public interest (AU DPF, 2022).

Data Protection Law Evolution in Zambia

The African continent has taken many steps toward implementing laws of data protection responsive to digital changes, including as far as sensitive personal data is concerned. Though congruent with international concepts, these frameworks are locally enforced.

The Data Protection Act of Zambia is one of the milestones in this path. It gives a clear definition of sensitive personal data, namely:

...personal data that in its nature may be misused to subdue the fundamental rights and freedoms of the data subject and such data may consist of the race, marital status, ethnic origin, genetic data, biometric data, child abuse data, political opinions, religious beliefs, trade union membership, as well as physical or mental health condition of a data subject.

(Republic of Zambia Data Protection Act, 2021, Section 2)

This definition categorically recognises certain types of data that require higher levels of protection since they may pose risks in case of misuse. The Act forbids any arbitrary treatment of such data, but allows it under specific conditions:

A data controller shall not handle sensitive personal data unless it is necessary to do so on medical, health, social services or judicial grounds, or it is done in the public interest.

(Republic of Zambia Data Protection Act, 2021, Section 14)

This limitation ensures that data processing is reasonable and reduces the risks to vulnerable communities. The key provision of the sovereign claim made by Zambia in terms of sensitive data?! is the localisation provision:

Any personal data shall be saved and processed on servers or data centres within the Republic, although it can be transferred outside of Zambia with the approval of the data subject and the Data Protection Commissioner. Personal sensitive information can only be stored in Zambia.

(Republic of Zambia Data Protection Act, 2021, Section 70)

This provision gains juridical dominance over sensitive data storage and seeks to protect citizens against foreign influence. In addition, the Act grants data subjects several fundamental rights, such as the right to be informed, the right to access, rectify, or erase their data, the right to consent or object to processing, and the right to legal redress of violations (Republic of Zambia, 2021, Sections 15, 69) and thus enhancing individual autonomy.

Office of the Data Protection Commission

In 2023, the Data Protection Commission (DPC) was established by Zambia's Data Protection Act of 2021 and is the regulator responsible for ensuring the protection and processing of personal data in Zambia. The Office reports to the Minister of Technology and Science, and is mandated to register data controllers and processors, license auditors, investigate complaints, and enforce the law. It is headed by Commissioner Likando Luywa, who was appointed as the nation's first Data Protection Commissioner in 2023.

Amongst its mandates, the DPC is tasked with raising awareness, advising governments, and representing Zambia in regional and international data protection forums. Entities that process personal data must register with the Commission and adhere to principles such as lawful processing, data minimisation, accuracy, security, and respect for data subject rights (Republic of Zambia, 2021). According to the Act, data processors must undergo regular audits by licensed data auditors to ensure adherence.

Even with significant legal developments, data protection authorities in Africa still face systemic problems, such as a lack of technical capacity, financial resources, lack of facilities, and the challenges of Big Tech domination. The DPC recognises these challenges and is undertaking capacity-building measures and stakeholder engagement plans with the view of ameliorating the gaps (CIPESA, 2021; Internews, 2023).

Protecting Sensitive Personal Data and Strengthening Data Infrastructure in Zambia

In 2024, Zambia launched its National ICT Policy. As part of this plan, the government, through the Ministry of Technology and Science, has earmarked ZMW 2.4 billion (USD 130 million) for the upgrade of ICT infrastructure, which includes the construction of 10 regional data centres for ZMW 500 million (USD 27 million) between 2022 and 2027 (Ministry of Technology and Science, 2024). The National ICT Policy is aimed at helping Zambia develop its digital sector both socially and economically in alignment with the country's Vision 2030 agenda. The policy seeks to increase access to the internet, improve digital skills, and create strategies that are competitive for the Southern African nation (Ministry of Local Government and Rural Development, 2024).

However, over the past three years, the country has faced several problems that has hindered the implementation of the National ICT Policy. While recovering from the impacts of Covid-19, severe droughts have disrupted the national electricity supply, making it hard to keep ICT systems running smoothly (Freedom House, 2024). In addition to this, the DPC has not received sufficient funding from the Government, which has delayed important regulatory work and enforcement (Zambia Information and Communication Technology Authority (ZICTA), 2024). These issues have slowed down the implementation of the Data Protection Act, which is overseen by the DPC, leaving gaps in protecting people's privacy as Zambia becomes more digital (Digital Development, 2024).

Zambia's National ICT Policy acknowledges that the rapid pace of technological advancements has brought about new challenges related to information security and data privacy (Ministry of Technology and Science, 2023).

To address this, the ICT Policy seeks to ensure a safe and secure ICT environment by enhancing data privacy and protection. The Zambian Government plans on building 10 data centres in all 10 provinces over a span of five years. Through such plans, the nation hopes to spread data storage throughout the country and provide services to all provinces (National Electronic Government Plan, 2023). Nevertheless, these plans depend on regular electricity. While caused by drought, power outages that have plagued the country over the past three years decrease the availability and quality of online services (Freedom House, 2024). Furthermore, resources continue to be a major challenge. Which stalls the DPC from fully carrying out its mandate of protecting personal data and managing digital rights effectively (ZICTA, 2024).

Without enough funds, Zambia is unable to develop its ICT industry, let alone build data centres. This can restrict the public's confidence in the DPC and digital services' management (Digital Development, 2024). Despite all of these challenges, government departments recognise that training people and collaborative approaches are key to improving data management (Ministry of Local Government and Rural Development, 2024).

Data Embassies and Their Implications for Data Sovereignty

The notion of a data embassy, where data is kept in foreign countries, but is still considered an extension of national territory, has drawn the interest of stakeholders and governments as a solution to cross-border data flow challenges (Lemos, 2025).

Data embassies are an emerging concept in data management. It was first introduced by Estonia to secure critical government information by means of secure, offshore-based data centres with de facto diplomatic immunities similar to traditional embassies (Rashica, 2025). The example of Estonia is to own data embassies in Luxembourg, where important government datasets related to the population, land, and business registries are stored, which improves resilience to cyberattacks, natural disasters, and military threats (Lars, 2025). Other states, such as Monaco and India, have been reviewing or have tried policies to have data embassies in their countries to strengthen their security in digital infrastructure (Sharwood, 2024).

Despite the technical advantages provided by data embassies, including improved security and recovery of data in case of disaster, the deployment of data embassies provokes substantial concerns relating to national sovereignty, as in the case of African countries like Zambia that are attempting to exercise their jurisdiction over the personal data of their citizens.

This concept is a dangerous trend for African nations that creates a risk of undermining the enforceability of local privacy laws, exposing data to foreign jurisdictions, and suffocating the local innovation ecosystem, the key to digital self-sufficiency (Matinou, 2025; Rashica, 2025).

The mere physical movement to a jurisdiction in a different country puts limitations on the ability of the home state to enforce its laws. The host country has de facto authority over the infrastructure thus potentially exposing the data to foreign surveillance, court demands, or political pressure that is beyond the control of the sending state. Such subversion of independent data control threatens the integrity of trust and deteriorates the safeguarding of citizens' rights (Couldry & Mejias, 2018). Moreover, excessive dependence on the external data infrastructure may suppress national investment and prevent the emergence of local digital spheres that are critical to sustainable development and digital sovereignty (Muchai, 2020).

The reliance on data embassies is a paradox in the African context, where digital sovereignty is being actively sought as a means to reverse historical trends of external (colonial) control, and where this new dependence may well consolidate new dependencies as well as undermine the legal integrity needed to protect human rights. As a result, data embassies can offer a bubble of trust in an occasionally geopolitically complicated setting, but at the same time, challenge the actual conduct of national sovereignty over sensitive personal data (information), which is one of the goals on which data localisation legislations like those in Zambia are based (Banya, 2024).

METHODOLOGY

This study employs mixed research methods that explore the regulation of sensitive personal data in Zambia under the Data Protection Act No. 3 of 2021. The research incorporates a legal interpretation of statutory documents and laws and empirical survey information of a purposive sample of thirty-three (33) organisations from various sectors, such as government agencies, private businesses, civil society organisations, and media houses.

The legal review was carried out with reference to the text of the Act, regulations, and guidelines by the Zambian DPC. Special attention was paid to the definitions, prohibitions, the requirements of the localisation of the data, the rights of the data subjects and the mechanisms of enforcement. The regional frameworks of the AU DPC, the Digital Transformation Strategy of the African Union and the Malabo Convention were also included in the analysis to contextualise the approach of lawmaking in Zambia on a continental level.

The survey was developed to examine organisational awareness, compliance behaviour, difficulties, perceptions of what people know, and perceptions of data sovereignty and new governance approaches like data embassies. Questions were asked on sensitive practices of data storage, registration on the DPC, appointment of Data Protection Officers (DPOs), frequency of security audits, capacity-building requirements, and outreach communication efforts.

The sample population was selected based on diverse provinces and positions as well as organisation sizes so as to create a sample that captures both urban and rural subtleties. The data was anonymised and analysed with the help of descriptive statistics and qualitative thematic coding. Ethics involved informed consent, confidentiality and the safe management of sensitive organisational input.

In this study, the survey was completed by senior personnel with direct institutional responsibility for data protection and data governance. Participants included high-level officials such as the Data Protection Commissioner, alongside other director-level or equivalent decision-makers and technical leads whose day-to-day roles involve overseeing compliance, advising on lawful processing, setting organisational data management standards, or supervising information security and governance functions. The survey was distributed via email to targeted organisations and completed through an online survey instrument, which helped standardise questions and reduce inconsistency in how responses were captured. This combined approach will allow triangulation of legal requirements with the realities on the ground to obtain a broader view of the issues and opportunities related to sensitive data governance in Zambia.

FINDINGS AND ANALYSIS

The survey was completed by 33 organisations in Zambia that handle sensitive personal information during the period July to September 2025. The participants were a wide range of stakeholders that included government bodies, commercial organisations, civil society organisations, and the media. The respondents were mostly occupying executive roles in the form of executive directors, data protection officers, IT managers and community advocates.

Registration Rates with the Office of the Data Protection Commissioner by Sector

Sector	Percentage Registered (%)
Government	60%
Private Sector	40%
Civil Society	28%
Media	27%

From a survey of 33 organisations, almost 44% of them are registered with the DPC, while 34% are not sure if they are registered with the DPC. The results showed that governmental organisations were the most compliant of the participants with the mandatory registration clause in the Data Protection Act, with an estimated compliance rate of 60%. This enhanced compliance can be reasonably explained by the fact that there was augmented legal awareness and regulatory scrutiny, thus highlighting their importance in being role models of regulatory compliance.

Organisations in the private sector were registered at a relatively low rate of about 40%, meaning that they were considerably engaged in them, but there were strong compliance gaps that were exposed by the survey results. The survey responses revealed that registration in the private sector is often hindered by a lack of awareness, complexity in the procedures, and insufficiency of resources, especially among small and medium-sized businesses.

The lowest registration rates were recorded among civil society organisations (28%) and the media (27%). Although both sectors routinely handle sensitive information in advocacy and reporting, uptake of registration remained comparatively low. This may indicate limited awareness of the registration requirement, inadequate access to practical registration support, and, potentially, weaker emphasis on formal compliance.

Respondents also noted that there was a need to have simplified registration processes and improved communication by the DPC. One of the media respondents noted that the registration process is not well understood or popularised, particularly in non-major cities.

The fact that this inequality in registration is quite significant reveals the pressing need of targeted campaigns and outreach activities to civil society and media organisations to build capacity and, in the process, promote universal protection of sensitive personal data in Zambia.

Where Sensitive Personal Data is stored

- Local servers only: 70%
- Hybrid model (local + foreign servers): 21%
- Foreign servers only: 7%

Over 70% of the organisations surveyed store sensitive personal data in the servers located within Zambia. This overriding compliance with the statutory localisation is suggestive of an intensifying devotion to digital sovereignty and to adherence to the terms of the Data Protection Act. However, a substantial 21% of the organisations use a hybrid data-storage approach that uses both domestic and remote server systems to store sensitive personal data. These organisations normally defend the strategy with the argument of high prices to have local data centres and the unreliability of domestic electricity. Few organisations store sensitive data on foreign servers completely (7%). This trend is the most common in smaller organisations that have limited resources or have data-intensive processes that do not have sufficient local infrastructure.

A representative of the private sector commented:

"Considering unstable electricity and no option of cheap certified hosting in Zambia, the hybrid cloud implementation was the only feasible option in our case, even though it jeopardises sovereignty."

Security Practices and Audit by Sector

Sector	Regular Audits (%)	Appointed DPO (%) - Data Protection Officers
Government	35%	40%
Private Sector	25%	20%
Civil Society	15%	10%
Media	10%	5%

The survey indicates that there is a major weakness in security governance and compliance practices in organisations that handle sensitive personal data in Zambia. Government agencies also show leadership in routine security audits (35%) and assigning Data Protection Officers (40%), which indicate a greater institutional ability and regulatory push.

The compliance of the entities in the private sector is lower; one-quarter of them conduct regular audits, and 20% of them have formally appointed DPOs. Their predicaments are mostly related to resources and a lack of technical knowledge to manage their data protection in the long term.

Civil society and media organisations are even more behind in this; less than 15% regularly audit their data infrastructure, and fewer than 10% have specific data-protection posts. The low engagement is indicative of high risks of data breach, mishandling, and non-compliance, thus compromising the rights and trust of the data subjects.

Budgetary deficit, a lack of trained staff, and a lack of appreciation of the audit requirements were often cited by the respondents as significant challenges. As one respondent in civil society noted, "Our organisation is virtually incapable of regular data security auditing, unless well-trained and equipped to undertake the task.

Staff Training, Public Awareness, and Outreach by sector

Sector	Staff Trained (%)	Public Awareness Rated as Poor (%)
Government	50%	70%
Private Sector	35%	65%
Civil Society	20%	80%
Media	25%	75%

Although it is an important task, data protection training is often overlooked in different sectors. In governmental organisations that were surveyed, there is a relatively good level of commitment, as about half of the employees have undergone formal education in data protection. This is in line with national requirements, which recommend mandatory role-specific training to all identified data controllers and processors (Data Protection Commission Zambia, 2025).

Conversely, the training penetration rate decreases significantly in the private sector and in the civil society organisations, where the proportions of employees receiving formal training on data handling, privacy principles, and regulatory compliance from the sample are less than 35% and 20,% respectively. Similar shortcomings can be found in the uptake of training by media organisations surveyed. This deficiency compromises the ability of personnel to capture evolving legal requirements and technical security provisions that cannot be ignored in the protection of confidential personal details.

Public awareness of data rights and privacy was assessed as low. Over 65% of respondents rated the general population's awareness of their rights to the protection of personal and sensitive data as insufficient. Respondents further indicated that this gap is more acute in rural and low-literacy contexts, where language barriers and limited outreach can restrict access to information and reinforce existing information asymmetries.

The surveyed organisations also show intentions to expand outreach programs, including workshops, participation in the community, and the use of media channels. However, the capacity and available resources are limiting the scale of the mass educational drive.

Companies announce the desire to increase outreach efforts, such as providing workshops, community engagement projects, and utilising media platforms. However, constraints of capacity and resources still affect the broad use of educational programs.

Attitudes towards Data Embassies and Digital Sovereignty.

- Data embassies: 52% against
- Conditional assistance that is based on legal protection: 30%
- Unconditional support: 18%

The survey findings indicate pronounced scepticism among the Zambian organisations surveyed towards adopting a regional "data embassy" approach. In this context, "data embassy" was understood in the diplomatic sense: although the data would be physically hosted in another African state, it would remain Zambia's sovereign property under an agreed governance arrangement. Nevertheless, more than 52% of respondents reported being completely opposed to such an arrangement.

About 30% of the respondents expressed conditional approval, which required any approval of data embassies to be conditional upon the creation of strong legal protection that would safeguard the substantive sovereignty and enforceability of data protection over the data of citizens.

A minority of respondents (18%) expressed unconditional support for the data embassy model, citing potential gains in technical resilience and the value of regional cooperation. However, even within this group, respondents stressed that robust oversight mechanisms would be required to ensure that Zambia's national interests are not subordinated.

These quantitative results are supported by qualitative responses. Survey respondents from civil society emphasised the risks of data exploitation and surveillance in the cases where data are moved beyond Zambian jurisdiction, whereas the respondents from the government and private sector articulated the complexities of the infrastructural realities in contrast to the sovereign demands of states, noting that:

- Data embassies can provide security, but without strong controls, they can weaken the legal power of Zambia over its own data.
- The quoted observers go on to state that: "Local storage should be kept as a base, and regional solutions sought only in cases where capacity constraints and clear governance can be seen to be insurmountable.

Such an established preference for localised data storage is in line with the wider strategic priorities of Zambia and the AU in terms of digital sovereignty and developing a measure of confidence in the citizens regarding data management, as enshrined in Zambia's Data Protection Act.

Challenges in Storing Sensitive Data Securely

- Financial/resource constraints
- Infrastructure limitations (power, servers)
- Limited technical expertise
- Legal/operational compliance complexity

Organisations in Zambia are faced with a significant obstacle to safely store sensitive personal information. The overriding obstacle, as mentioned by 60% of the organisations that participated in the survey, is the issue of financial and resource limitations that jeopardise the sustainability of compliant data-handling infrastructure.

Another 55% of the respondents cited infrastructural constraints, specifically unreliable power supply and the lack of certified local data centres, as obstacles towards complete regulatory compliance. The absence of technical knowledge (at least partially), 50% of the respondents claimed, only adds to the operational compliance, with about 35% also struggling with the legal and procedural complexity implicit in the Data Protection Act.

All these multilayered challenges undermine the concept of effective data governance and highlight the urgency to have a coordinated effort and investment to increase organisational capacity.

Types of Sensitive Personal Data organisations store

- Biometric data
- Health data
- Political opinions
- Religious beliefs
- Financial information
- Other (including ethnicity, genetic data)

The fact that the political views and religious convictions are also included in organisational datasets also makes the necessity of privacy tools and safeguards more prominent, since the misuse of such information may initiate persecution or discrimination. Though minimised more frequently, financial and genetic data still have extra layers of complexity in terms of consent, confidentiality, and data minimisation principles.

Organisational Views on Policy Inclusivity for Marginalised Groups

- Policies inclusive of youth, persons with disabilities, and linguistically diverse: 30%
- Partially inclusive: 45%
- Not inclusive: 25%

The survey indicates that gaps in the inclusivity of data protection policies of Zambia are still evident. Less than a third of organisations surveyed (30%), are of the perception that existing policies are sufficient to support marginalised populations, such as youth, persons with disabilities, and linguistic minorities.

A larger share, 45%, stated that the policies are only partially inclusive, and they recognise that some provisions do exist, but they cannot see how the policies are practically applied or how they can be practically implemented. At the same time, 25% of the respondents noted that the policies are not inclusive, which indicates systemic barriers to fair realisation of data rights.

The closure of these gaps will require a specific policy formulation, legal translation, and participation of the communities in question to result in participatory and accessible protections.

Does your Organisation have Formal Written Policies on Sensitive Data Storage and Protection

- Yes: 40%
- No: 34%
- Don't know: 15%
- In development: 12%

The findings indicate that only 40% of organisations surveyed have formal documented policies on the storage and protection of sensitive information. One-third (34%) of respondents mention lack of such policies, which puts the risk of data inconsistency and non-compliance on the agenda. Another 15% do not know whether policies exist in their organisational scope, whereas 12% are in the process of formulating them. This findings reveals one of the key points of capacity building and governance consolidation that must correspond to the statutory requirements and ensure the privacy of the data.

Specific Training Needs for Staff
Top training topics: Data Protection Act familiarisation, incident response, data protection best practices, IT security, breach management, storage management

Companies have identified a wide range of training needs that would be necessary in the management of sensitive information. Some of the leading requirements are certification training of Data Protection officers, incident management and breach management, general data protection best practices, and expertise in IT security. The comparatively balanced distribution of the topics denotes that there is a broad requirement in the overall capacity development, which has a different level of organisational maturity and technical background.

Public and Organisational Outreach

The surveyed organisations generally viewed public awareness of data protection rights as limited, with most rating awareness as low or, at best, average. Respondents further indicated that this gap is more pronounced in rural and low-literacy communities, where access to information is constrained by language barriers and limited outreach. In particular, they noted that most training materials and public communications are available primarily in English, which reduces accessibility for many communities, including groups that may require enhanced protection in practice, such as migrants, refugees, and stateless persons.

In some survey responses, the respondents of the civil society and the media urge the government to pursue wider outreach programs that can encompass local languages and multimedia formats, to ensure a reduction in communication gaps and improve the active participation of the general population.

CONCLUSIONS AND RECOMMENDATIONS

Recommendations

The recommendations below are based on the findings of this research, i.e., the limited level of awareness of data protection among the population, the provable need to demonstrate more specific guidance, as well as more effective support in compliance, and the importance of protecting sensitive personal data in Zambia. The recommendations are categorised based on stakeholder groupings, i.e. government bodies and the regulatory authority, civil society and media outlets, the private sector, and regional partners, to be sure that each actor is assigned a specific set of responsibilities aimed at raising awareness, strengthening localisation and infrastructure, and increasing transparency, accountability, and implementation.

Zambia Government and Data Protection Commission (DPC).

1. **Raise Awareness and Streamline Sensitisation Programmes**

As per the survey conducted in this study, there are low levels of awareness regarding the Act, particularly among rural and less literate communities. The government and regulator should embark on large-scale, culturally and linguistically sensitive awareness campaigns on the importance of data protection as a human right.

2. **Enhance localisation of Data and Development of Infrastructure**

Develop, finance and fund secure and certified domestic data centres with domestic partners if necessary to ensure that they comply with the data localisation requirements and safeguard the information of citizens inside national borders, which guarantees digital sovereignty.

3. **Transparency on Regulatory Direction and Support**

Give accessible, transparent practical guidelines on registration, cross-border data transfer (under strictly conditioned requirements), breach notification and data subject rights, and continuous advisory service.

4. **Capacity Building For Sectors**

Continuously provide training on data protection policies, compliance, and technological protection to officials in the public, regulators, and the actors in the private sector.

5. **Increase Enforcement and Transparency.**

Audit routinely, punish breaches, and have a publicly available audit and maintain a register of data controllers so as to establish trust and accountability.

Civil Society Organisations (CSOs) and Media

1. **Promote Human Rights-Based Data Education**

Make legal and technical concepts of data protection simple to allow the cultivation of the concept of privacy as a basic right, and use local languages and community-specific communication channels.

2. **Empower Citizens through Engagement and Advocacy**

Be watchdogs of data privacy violations, increase awareness and to hold institutions accountable as per the standards of the ACHPR and the national law.

3. **Grow coverage on data protection issues**

Collaborate with government and private sector to expand community awareness on data governance, focusing on rights, responsibilities and the harm of data commodification.

Private Sector and Tech Companies (Including Big Tech)

1. **Demonstrate Respect for Local Data Sovereignty**

The private sector should not provide offshore data storage solutions and should not ignore the data localisation requirements.

2. **Put in place Strong Company Data Protection Policies**

Hire Data Protection Officers, have frequent impact assessments and use up-to-date security measures to protect sensitive information.

3. **Train Staff Continuously**

Make sure that the staff is thoroughly educated on the principles of data privacy, data breach management, and compliance duties to promote the organisational culture aligned with human rights.

4. **Promote Transparency and Accountability**

Enhance communication with users regarding data collection and use, especially for vulnerable populations, and have redress and informed consent mechanisms.

In the case of the African Union (AU) and Regional Partners

1. **Support Human Rights-based Harmonised Data Protection**

Support member states, such as Zambia, to harmonise data policies

2. **Share Infrastructure and Facilitate Regional Capacity Building.**

Encourage the sharing of knowledge, joint training and investments in secure and locally owned digital infrastructure.

3. **Data Rights and Champion Digital Sovereignty at the Continental Level**

Implement strong advocacy campaigns against data embassies or extra-territorial authority of offshore actors in order to maintain African data sovereignty and genuine respect for human dignity.

The paper has shown how the emerging state of data governance in Zambia is founded on a solid sovereignty argument, especially in the handling of sensitive personal data. The legal and normative frameworks underlying the increased protection are effectively summarised in the Malabo Convention, which identifies sensitive information (data) as a distinct category and puts down specific limits and conditions on its processing, and provides enforceable rights of subjects of data and duties of data controllers (Malabo Convention, 2014). Such a rights-based approach is consistent with the policy focus on jurisdictional control and provides a logical explanation of the fact that sensitive personal data must be stored and controlled in the Republic in accordance with domestic law (Republic of Zambia Data Protection Act, 2021).

This argument is also supported by the empirical findings. According to the survey findings in this research, there is a strong inclination towards sovereign dataset nurture at home, as well as strong rejection of a regional "data embassy" arrangement, even though those surveyed also recognised that ownership would be retained by Zambia. At the same time, the results highlight the fact that efficient sovereignty goes beyond the localisation provisions. The respondents emphasised the lack of awareness of the rights to data protection in society, especially among low-literacy and rural populations.

All these legal and empirical observations support the main argument that data sovereignty in all its aspects (particularly concerning sensitive personal data) can best be achieved by the establishment of effective domestic legal protections, viable control and enforcement systems, that make data rights understandable and operational for all.

The case study of Zambia as the path to effective data protection and digital sovereignty is a valuable lesson to other African states that have to cope with similar technological and geopolitical challenges. The foundation of the policy on cultural respect, human rights and pragmatic realities and the careful protection against external reliance will help the creation of a future where the dignity and privacy of citizens will remain intact and the digital opportunities will be fairly distributed.

Acknowledgement:

We wish to acknowledge the immeasurable assistance of the Zambian Data Protection Commissioner, Likando Lyuwa. We owe our growth and development to all the stakeholders in Zambia who have put their trust in our research undertaking. I would specifically like to give special credit to the field researcher in Zambia, Nyambe Jere, whose task was key to successfully gathering the evidence for the research. Furthermore, I would like to thank Kristophina Shilongo, the Research Lead, who has provided guidance and support throughout this research.

REFERENCES

African Union. (1981). African Charter on Human and Peoples' Rights. Retrieved from https://au.int/en/treaties/african-charter-human-and-peoples-rights

African Union. (2000). African Union Convention on Cyber Security and Personal Data Protection, African Union. Retrieved from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union. (2020) The Digital Transformation Strategy for Africa (2020-2030). African Union. Retrieved from https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030

African Union. (2022). AU Data Policy Framework. African Union. https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf

Banya, R. M. (2024). Africa's Digital Sovereignty Trap: The Data Center Dilemma. New America. Retrieved from https://www.newamerica.org/planetary-politics/briefs/africas-digital-sovereignty-trap/

Boshe, P. (2024). A Quest for an African Concept of Privacy. In Data Privacy Law in Africa: Emerging perspectives (Chapter 1). Retrieved from https://www.pulp.up.ac.za/images/edocman/edited-collections/data_privacy/Chapter%201.pdf

CIPESA. (2021). Zambia: The Data Protection Act, No. 3 of 2021. Collaboration on International ICT Policy in East and Southern Africa (CIPESA). https://cipesa.org/download/briefs/Insights-into-Zambias-Data-Protection-Act-2021.pdf

Couldry, N., & Mejias, U. A. (2019). The Costs of Connection: How Data Is Colonizing Human Life And Appropriating It For Capitalism. Stanford University Press. https://www.sup.org/books/sociology/costs-connection/excerpt/table-contents

Lemos, L. (2025, February 20). Nations Open 'Data Embassies' to Protect Critical Info. Retrieved from https://www.darkreading.com/cyber-risk/nations-data-embassies-protect-critical-info

Digital Development. (2024). Zambia National ICT Policy 2023. Retrieved from https://www.digitaldevelopment.org/library/zambia-national-ict-policy-2023/

Rashica, V. (2025, March 06). Data Embassies: Protecting Nations in the Cloud. Retrieved from https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/

Freedom House. (2024). Zambia: Freedom on the Net 2024 Country Report. Retrieved from https://freedomhouse.org/country/zambia/freedom-net/2024

Republic of Zambia. (2021). Data Protection Act, 2021. In the Republuc of Zambia. https://www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%203%20The%20Data%20Protection%20Act%202021_0.pdf

Internews. (2023). Impact of cybercrime and cybersecurity laws on media freedom and digital rights. https://internews.org/wp-content/uploads/2023/11/ARISA-IEA-CHAPTER-17-Zambia.pdf

Kinyua, W. (2025). Thorn in the Foot: Is African Culture a Menace to Data Protection Advancements? https://www.africadataprotection.org/KINYUA-WANJOHI.pdf

Lars, E. (2025, February 13). Data Embassy - e-Estonia. Retrieved from https://e-estonia.com/solutions/e-governance/data-embassy/

Makulilo, A. B. (2016). A person is a person through other persons: A critical analysis of privacy and culture in Africa. (Accessible via ResearchGate record.) https://www.researchgate.net/publication/306382562_A_Person_Is_a_Person_through_Other_Persons-A_Critical_Analysis_of_Privacy_and_Culture_in_Africa

Matinou, S. F. (2025). Beyond Borders: Exploring Data Embassies As A Strategy For Digital Sovereignty In Africa [Preprint]. https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/6890b12c23be8e43d6b625fa/original/beyond-borders-exploring-data-embassies-as-a-strategy-for-digital-sovereignty-in-africa.pdf

Ministry of Local Government and Rural Development. (2024). Digital Strategy 2023-2026. Retrieved from https://www.mlgrd.gov.zm/wp-content/uploads/2024/10/DIGITAL-STRATEGY_MLGRD.pdf

Ministry of Technology and Science. (2023). National ICT policy 2023 [PDF]. The Republic of Zambia. https://www.mots.gov.zm/wp-content/uploads/2023/10/National-ICT-Policy-2023.pdf

Ministry of Technology and Science. (2024). National ICT Policy 2023 Implementation Plan. Retrieved from https://www.mots.gov.zm/wp-content/uploads/2023/10/National-ICT-Policy-2023-Implimentation-Plan.pdf

National Electronic Government Plan. (2023). Zambia Government Digital Infrastructure Development. Retrieved from https://www.szi.gov.zm/wp-content/uploads/2023/08/Final-National_e-Government_Plan_-2023-Final-17.08.2023.pdf

Ndakalako, M. (2023). What's in a namesake? The Owambo naming practice of Mbushe, gender, and community in Namibian novelist Neshani Andrea's The Purple Violet of Oshaantu. (pp. 85–103). Springer. https://doi.org/10.1007/978-3-031-13475-3_5

Nwoye, A. (2017). An Africentric theory of human personhood. Studies in African Philosophy, 35(2), 45-60. Retrieved from http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1015-60462017000200004

Republic Of South Africa (2013). Protection of Personal Information Act, 2013. Government Gazette: Vol. Vol. 581 (Issue No. 37067) [Report]. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

Sharwood, S. (2024). "Data embassies" promise bubbles of digital sovereignty, but India just cooled on the idea. The Register. Retrieved from https://www.theregister.com/2024/07/24/data_embassies/

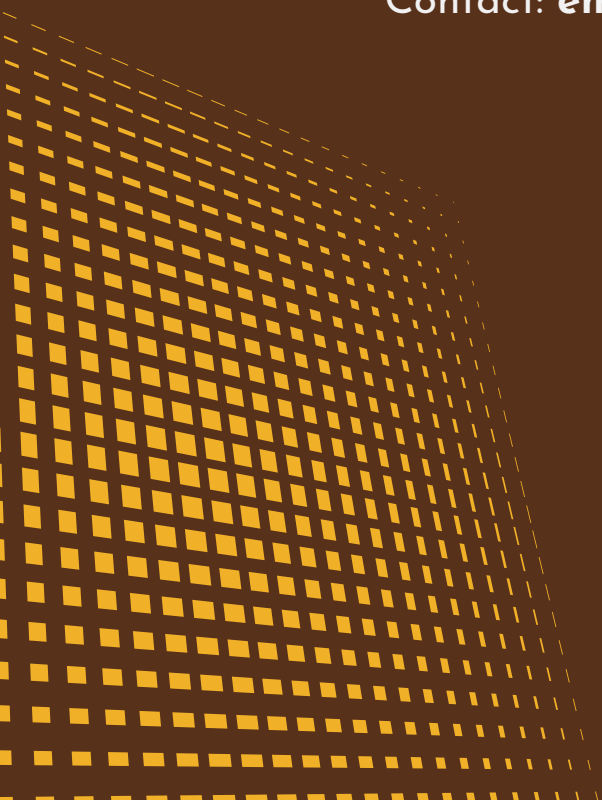
Udechukwu, G. I., & Nnyigide, N. M. (2025). The religious and socio-cultural implications of African names: Igbo naming system as a paradigm. African Journal Online. Retrieved from https://www.ajol.info/index.php/ijah/article/view/139836#:~:text=Africans%20in%20the%20past%20valued,dead%20(spirit)%20as%20witnesses.

United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

World Economic Forum. (2020, July 29). Data is the new gold: How it can benefit everyone. Retrieved July 29, 2020, from https://www.weforum.org/stories/2020/07/new-paradigm-business-data-digital-economy-benefits-privacy-digitalization/

Zambia Information and Communication Technology Authority (ZICTA). (2024). Annual Market Report for the ICT Sector. Retrieved from https://www.zicta.zm/market-reports/2024_annual_market_report.pdf

Author: **Emsie Erastus**
Contact: **emsieerastus[at]gmail[dot]com**



THE DATA GOVERNANCE IN AFRICA RESEARCH FUND