PRIVACY SCORECARD REPORT

Mauritius, Zimbabwe, Kenya & Uganda

NOV 2023

PRIVACY Scorecard

Written and Compiled by: UNWANTED WITNESS "Amplifying Voices, Changing lives"

Inpartnership with: APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

If You Must Collect It, You Must Protect It

www.unwantedwitness.org

PRIVACY SCORECARD REPORT

2023

Authored by:
Unwanted Witness

Contents

Privacy Scorecard Report | 2023

List of acronyms

AI - Artificial Intelligence
EU - European Union
DPA - Data Protection Act
IoT - Internet of Things
LTD - Limited
MRA -Mauritius Revenue Authority
NITA - National Information Technology Authority, Uganda
NIRA -National Identification and Registration Authority
NPDPD - National Personal Data Protection Director
ODPC - Office of the Data Protection Commission
OECD - Guidelines on Privacy OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data
PDPO - Personal Data Protection Office
POTRAZ – Postal and Telecommunications Regulatory Authority
SACCO -Savings and credit Cooperative
SLAs -Service Level Agreements
SMEs - Small and Medium-sized Enterprises
UNGPs - The United Nations Guiding Principles on Business and Human Rights
ZIMBRA - Zimbabwe Revenue Authority

List of respondent companies

Mauritius Companies

- Emtel Limited
- Mauritius Telecom Ltd
- Swan Life Limited
- ABSA Bank (Mauritius) Limited
- Pick and Buy Limited
- Intermart (Mtius) Ltd
- Supertote
- StevenHills
- FinClub
- Fundkiss
- Mauritius Revenue Authority(MRA)
- The passport and immigration office

Zimbambwe Companies

- Econet
- TelOne
- CBZ Bank
- Empower Bank
- Ubuy Zimbabwe
- Shumba Africa
- Africabet
- Bezbets
- Ecocash
- Zibuko
- E-Visa Department
- Zimbabwe Revenue Authority

Kenyan Companies

- Safaricom
- Zuku
- Stima
- Equity Bank
- Jiji
- Jumia
- Betika
- Mcheza
- Branch
- Tala
- E-Citizen
- Huduma

Ugandan companies

- Lycamobile
- MTN Uganda
- Stanbic
- Pride Microfinance Ltd
- Jiji
- Jumia
- Fortebex
- IxBet
- Dove Cash
- Mangu Cash
- Immigration Uganda
- National Identification & Registration Authority

About Unwanted Witness Uganda

Unwanted Witness Uganda – UW is a civil Society Organisation founded in 2012 to promote online freedoms and protect digital rights in Uganda. UW has become a leading voice in advocating for internet freedoms, and digital rights, particularly the right to privacy, digital identity, digital inclusion, and freedom of expression.

The organization aims to create a safe and secure digital environment for citizens and promote the responsible use of technology. It aims to empower citizens to use technology in a safe, secure, and effective manner while holding public and private entities accountable for digital rights violations.

UW achieves its mission through research, advocacy, and capacity building. UW conducts research to identify digital rights violations, trends, and threats and uses this information to advocate for policy and legal reforms. The organization also provides digital security training and support to human rights defenders, journalists, and vulnerable groups to help them protect themselves online.

In addition, UW engages in public education and awareness campaigns to promote digital literacy and responsible online behavior. It also monitors digital surveillance and censorship and responds to issues of concern by advocacy and awareness raising.

Vision: An open free secure internet that contributes to the realization of human rights and good governance in Africa.

Mission Statement: To contribute to good governance through effective and efficient use of the internet/online activism through networking and strengthening capacities of citizens for collective advocacy and synergy.

Corporate Values

- Equity and Equal Opportunities
- Integrity
- Collective Action
- Commitment and Teamwork
- Transparency and Accountability
- Tolerance
- Efficiency and Effectiveness

Acknowledgements

Unwanted Witness acknowledges the support of key civil society organisations in the performance of its functions. UW appreciates financial support from development partners particularly, APC – Association for Progressive Communications and Open Society Foundations (OSF) who extend their financial and technical support to ensure the successful production of this report annually.

Unwanted Witness acknowledges its Research and Advocacy Unit in particular Ms Freda Nalumansi-Mugambe and the team of researchers: Ms Yuxi Wang, Ms Deepti Luchman, Mr Brian Kiira, Mr David Kasibante and Ms Saphirah Kubakurungi. Special gratitude to the members of the editorial board particularly, the Executive Director Ms Dorothy Mukasa, the Head of Programmes Mr Allan Sempala Kigozi and the Research and Advocacy Lead Ms Freda Nalumansi-Mugambe. UW also recognizes efforts of other staff for supporting the production of the report.

UW further acknowledges the contributions made by individuals and organizations during the process. We thank Price Media for their contributions to the graphics and layout. These contributions provided during the development and review helped in enriching the report.

Executive Summary

This is the Unwanted Witness third annual Privacy Scorecard Report. The report in 2023 took stock of compliance with data protection and privacy laws and regulations in four countries – Mauritius, Zimbabwe, Kenya and Uganda. The report is cognisant of the implementation of data protection laws alongside growing digital economies and the utilization of an in-depth methodology, which informed the evaluation in line with specific objectives and functions of the Unwanted Witness.

Primarily, the report is informed by: a background to the report; along with a methodology and criteria for the assessment; insights into the four countries highlighting the context, analysis of data protection and privacy landscape, legal and institutional framework in existence, and findings at country sector level as well as overall deductions for impact on personal data protection and privacy rights; challenges; lessons learned and best practices; drawn conclusions and appropriate recommendations to different actors –state and non-state actors. The report is consisted of seven sections summarised hereinafter in this part.

The study highlights the data protection performance of a total of 48 selected companies/entities across six sectors- telecommunication, e-commerce, financial services, e-government, digital loan services and online betting. The assessment utilizes objective and quantifiable variables underpinning six indicators– existence of an accessible and noticeable privacy policy, informed consent, data collection and third party data transfers, practice robust security, accountability and internal redress mechanisms for data breaches for analyzing the policies and practices of the selected data collectors.

Over the past decade, each of the countries has experienced rapid growth in digital services, with extensive adoption of mobile money, e-commerce, ride-hailing applications and digital lending platforms. However, this digital transformation has also increased risks of personal data misuse, data protection breaches, and unauthorized surveillance given the collection of sensitive information like financial transactions, location data and communications by both private sector applications and government systems. The existing legislation set good foundations with the newest in Zimbabwe that was passed in 2021, but turning principles into practice remains challenging. The practical implementation and enforcement of data protection laws and regulations are in their nascent stages. Further concerns surround: insufficient regulatory capacities and resources responsible for overseeing compliance; limited understanding of data protection laws and privacy rights; along with low public awareness; with the importance of safeguarding personal data as an ongoing issue; resource constraints; weak accountability culture; rapid technological changes; political and social tensions; and absence of effective redress mechanisms for addressing data breaches.

The findings revealed an overall index score of 47.3% registered by Kenya and the lowest score as 23.1% registered by Zimbabwe. While, the highest performance at sector level across the countries was 50.1% registered by e-commerce and 11.1% as the lowest score which was registered by e-Government.

In addition, the performance against the six indicators was observed at both country and sector levels. At country level, Kenya was observed in the lead with the highest scores in 3 out of the 6 indicators namely: 85.8% for existence of an accessible and noticeable privacy policy, 59.4% for informed consent and 25% for internal redress mechanisms for data breaches. While, Zimbabwe was observed with the lowest scores in 3 indicators – 55% for existence of an accessible and noticeable privacy policy, 23.4% for informed consent and zero percent registered for accountability and availability of internal redress mechanisms for data breaches. At sector level, Telecommunications was in the lead with the highest scores in 2 out of the 6 indicators– 100% for existence of an accessible and noticeable privacy policy and 12.5% for accountability. While, e-Government was observed with the lowest scores in 3 indicators – 25% for existence of an accessible and noticeable privacy policy, 11.5% for practice robust data security and 9.2% for informed consent.

The study equally highlights experiences and emerging practices that countries under review and the wider region can draw key practical lessons and best practices on effectiveness, enhancing transparency and accountability from each other. These included: highlighting positive leaders; incentivize accountability; combine incentives and deterrence; enforce intelligently; issuance of guides, sectoral toolkits and practice codes; automate monitoring of data systems; multi-stakeholder collaboration; prioritization of consumer rights and organisation; institute complaints handling mechanisms/remedies to address data breaches; carrying-out privacy sweep assessments; conducting market studies; investment in strategic foresight capacities; shaping sandbox regulatory spaces; and managing third party- related risks.

To that end, realising effective data protection that upholds user rights will necessitate action across diverse sectors/industries and stakeholders. As such, the report advanced the following recommendations below;

Recommendations for data controllers and processors:

1. Proactively elevate transparency and implement accountable data practices aligned with Data Protection legislation like the annual release of a transparency report, to demonstrate commitment to accountability beyond passive policies alone. Such a report would be highly effective as it would comprehensively detail the collection of personal data throughout the year, specifying who had access to it, whether government entities, private organisations or individuals.

2. Take steps as the custodians of personal data collection, storage and use, to publish detailed privacy policies prominently displayed, easily accessible, and written in a clear, understable manner for the general public and provide exhaustive inventories of data types, rather than vague summaries.

3. Outline specific retention periods tailored to different categories of user information rather than indefinite storage.

4. Describe security protections in place, whether organizational, physical or technical.

5. Establish functional mechanisms for users to submit access, correction or deletion requests and obtain remedies. This necessitates instituting internal training and access protocols beyond just policy declarations.

6. Comprehensively disclose any third-party entities or affiliates with whom personal data is shared, justifying the necessity rather than blanket statements of obeying legal mandates.

7. Undertake periodic data protection impact assessments to continuously evaluate their privacy risks and harms.

8. Recognize transparency and lawful data governance as not burdensome obligations but ethical imperatives vital for consumer trust and exercising of data protection rights.

Recommendations for data protection regulators:

1. Proactively undertake privacy sweep assessments of organizations across sectors to audit their publicly posted policies and visible practices against applicable transparency requirements. Such sweeps create evidence-based benchmarks and uncover focus areas for regulatory action.

2. Provide guidance for compliance, monitoring enforcement, and establish institutionalise accountability systems to ensure meaningful data protection.

3. Institute programs that highlight entities and sectors with particularly exemplary accountability practices, through awards, certifications, eased requirements or other incentives.

4. Recognise leading performers to motivate wider adoption of transparent data handling

5. Publish user-friendly guidance resources and tools catering to specific sectors and common practices to aid controllers translate legal principles into organizational procedures.

6. Make use of a graduated enforcement approach that relies on warnings, training requirements and minor initial sanctions to aid raising consciousness and build capacities across industries before escalating to major penalties for wilful violations.

7. Build regularly own oversight capacities for compliance monitoring, investigations, audits and enforcement to fulfil mandate under data protection legislation.

8. Operationalise smooth complaints handling, expedient resolution mechanisms and appeal processes for aggrieved users to obtain redress against opaque practices.

9. Maintain independence from partisan or industrial influence to objectively supervise data protection standards in user interest.

Recommendations for policymakers:

1. Enact additional legislation articulating and enforcing rights of data subjects in the digital economy for users to hold companies /organisations accountable due to irresponsible data collection or misuse.

2. Incorporate rights literacy and skills-building on data protection in educational curricula in tertiary schools and professional training programs to social capacity on exercising user privileges and informed consent.

3. Provide adequate budgets and resources for public awareness campaigns that educate citizens across demo-

graphics, languages and media platforms about core data rights, risks, entitlements and complaints channels and continued capacity development of regulators to effectively fulfil their challenging mandate.

4. Make incorporation of 'privacy by design' principles and data protection impact assessments an obligation in public sector digitization programs to uplift state transparency.

Recommendations for technology service providers:

1. Make upholding transparency integral to technical architectures rather than an afterthought
2. Pre-configure tools with strong access controls, encryption, anonymization, compliance dashboards and consent mechanisms.
3. Guide clients on minimal data collection, storage limitation, tailored retention and data mapping.
4. Clearly communicate their own limited data use, prohibit onward sharing and institute third-party audits.
5. Develop robust yet usable data protection capacities within digital infrastructures to enable accountable practice.

Recommendations for users /data subjects:

1. Exercise vigilance and inquisitiveness regarding how your personal information is handled.
2. Thoroughly read privacy policies before accepting terms of use rather than automatically clicking consent. Where possible, users should opt out of non-essential data collection and processing that violates privacy principles.
3. Proactively submit queries and complaints to companies/organizations regarding opaque practices for clarification or remediation. Escalate unresolved grievances to regulators for investigation.
4. Directly call out organizations that demonstrate deficient transparency or disregard for data responsibility through public campaigns on social media or collective petitions.
5. Back up critiques and demands for accountability with evidence and articulate them in constructive ways.

Recommendations for civil society:

1. Undertake independent assessments of data practices of companies/organizations from the perspective of consumer impacts rather than purely technical compliance.
2. Document user experiences involving opaque data collection or privacy harms through complaints data, focus groups and interviews to make such evidence crucial for making opaque practices relatable and centre citizen voices in policy conversations.
3. Publish explainers, guides and advisories on data protection issues tailored for diverse demographics in accessible formats and multiple languages.
4. Advocate for elevated transparency commitments from companies/organizations through campaigns, petitions and dialogue.
5. Proactively partner with responsible industries/sectors and regulators in steering evolving best practices and identifying pragmatic solutions for balanced scholarship and oversight.

Recommendations for academia/scholars:

1. Undertake research monitoring and evaluate data protection accountability based on indicators like policy transparency, security audit results and user perceptions.
2. Study sector-specific data ecosystems to inform tailored oversight.
3. Build interdisciplinary expertise and offer courses educating students on privacy-preserving technology design, ethical data use, and data protection law.
4. Host public forums fostering evidence-based dialogue between policymakers, industry, civil society and users on navigating emerging challenges and trade-offs. Academic input is vital for informed, balanced and farsighted data governance.

Background

In today's digital age, personal data has become one of the most valuable assets in the world. In tandem, the protection of privacy, a constitutionally protected right, has become an important concern for regulatory bodies and organisations in their approach to handling personal data. The Unwanted Witness Privacy Scorecard Report is a data monitoring tool aimed to take stock of adherence to compliance by both data collectors and processors, encompassing both public and private entities with data protection and privacy laws and regulations annually including making appropriate recommendations. In 2023 Unwanted Witness continued to monitor the compliance of data collectors in four countries namely: Mauritius, Zimbabwe, Kenya and Uganda compared to 2022 were compliance was assessed in two countries – Kenya and Uganda.[1]

In addition, to the expansion in the country focus, the 2023 Privacy Scorecard Report assessed performance of data collectors with a deeper methodology adopted that focused on six sectors namely: e-commerce, financial services, digital loan services, online betting, telecom and government agencies. Compared to 2022, were the focus was on three sectors.[2] These were evaluated and assessed against six indicators compared to the five indicators utilized in 2022. The indicators included: existence of an accessible and noticeable privacy policy, informed consent, data collection and third party data transfers, practice robust data security, accountability and availability of internal redress mechanisms for data breaches.

After a rigorous process including a thorough peer review and quality control, organizations receive a credit for their performance across all five indicators for a given category, and results show how companies performed by each category and indicator. Only publicly available privacy policy positions can qualify for credits in this Scorecard and organisations get credits. Privacy positions, practices, or policies that are conveyed privately or internal corporate standards, regardless of how laudable, are not factored into our decisions to award organizations/companies credit in any category.

Requiring public documentation serves several purposes. First, it ensures that companies cannot secretively change an internal practice in the future to hoodwink data subjects, but must also change their publicly posted policies, which can be noted and documented. Second, by asking companies to put their privacy policies and practices in writing, we can examine each policy closely and prompt a larger public conversation about what standards these organisations should strive for. Third, it helps organisations review one another's policies around law enforcement access, which can serve as a guide for start-ups and others looking for examples of organisations standing up for user privacy.

In this scorecard, we strive to offer ambitious but practical standards. To that end, we only include criteria that at least one organisation has already adopted. This ensures that we are highlighting existing and achievable best practices, rather than theoretical policies. Each year, we review the criteria we used in prior years and make any adjustments that may be necessary to ensure the scorecard is keeping pace with modern technology policy trends.

The main objective of the 2023 report is to generate research that could be used to empower data collectors/processors to adopt data protection best practices; and citizens to demand for accountability in the area of personal data protection. The report could also inform legal and policy reform for better management of personal data by especially non state actors. The scorecard evaluates corporate privacy policies and practices in 2023 against internationally accepted standards and national data protection laws. The 2023 report as noted above highlights the data protection performance of 48 selected companies/entities across six sectors.

The assessment utilizes objective and quantifiable parameters for analyzing the policies and practices of the selected data collectors. The study assesses the publicly available policies of the selected companies to determine their compliance with applicable data protection legislation. The report sought to achieve the following specific objectives;

- to determine the legal protection of personal data and privacy in the countries of Mauritius, Zimbabwe, Kenya and Uganda;
- to evaluate changes in compliance (and practices) of selected companies;

1. The Privacy Scorecard Report, 2022 is available at https://www.unwantedwitness.org/download/Privacy-Scorecard-Report-2022.pdf (accessed 23 October 2023).
2. Ibid same as above.

- to evaluate the compliance of data collectors in Mauritius, Zimbabwe, Kenya and Uganda with data protection laws;

- to document the nature of abuse and violations, if any, of the rights to privacy by the assessed companies in each respective country;

- to provide recommendations to improve compliance with data protection laws in Mauritius, Zimbabwe, Kenya and Uganda by private non-state actors;

- to provide a toolkit for evaluating compliance of data collectors that citizens could replicate and rely on for better protection.

Following the evaluation of corporate privacy policies and practices of 48 companies/entities across 4 countries, an overall index score of 47.3% was registered at country level, with e-commerce sector scoring an average score of 50.1%, digital loan services 44.9%, telecommunications and financial services registered a tie and scored 39.7%, online betting 33.8% and e-government 11.1%. The performance against the indicators was observed at both country and sector, with the highest scores registered for the existence of an accessible and noticeable privacy policy indicator. While, the lowest scores were registered for the accountability and availability of internal redress mechanism for data breaches indicators.

Whereas there was an additional indicator making them six and three more sectors bringing the focus on a total of six, the 2023 report still benchmarks on the findings of the previous 2022 Privacy Scorecard Report in assessing whether or not there has been progress in data protection across the selected sectors.

2. Methodology and Criteria

The 3rd annual UW score card report typically gives an overview of privacy practices of 12 selected private companies in each of the four countries in six sectors with a high use of personal data given the volume of their operations and undertakings. Two companies featured for the assessment in each sector and these included; financial services, telecommunication, online betting, digital loan services, e-government and e-commerce.

In all the four countries, the companies were selected on the basis of their market share, with one having the highest market share, and the second with a mid–tier share. Carefully balancing big and relative players in the respective sectors. The selected companies' compliance with data protection and privacy laws and regulations in their countries of operations was assessed against six core indicators. Every indicator is embedded with measurable variables for which a score will be given upon compliance with data protection laws and regulations.

These indicators along with the respective variables included:

a. Existence of an accessible readable and noticeable privacy policy

Compliance with this indicator would have been reached if a company's privacy policy is public, published, noticeable and readable and awarded accordingly. Considerations for a policy being public and published are upon availability on the company's website or mobile App. For a policy notice to be in fine print, a company would not have fulfilled the variable regarding the policy being noticeable. The Hemingway editor, an online tool is utilized to establish whether the policy is readable. It evaluates the text of the different privacy policies for simplicity or difficulties in comprehension for attainment of a rating of good. While, an okay rating will not grant a credit score to the company. Also, the editor evaluates the length of the text and for this assessment, a policy is considered insufficient if it had a word count below 200.

b. Informed Consent

Compliance with this indicator entailed users to be furnished with the following details:

Company's contact details - The – either an address, contact email or phone number should be provided in the policy.

Purpose of data collection – the reason for which the data is collected should be explicitly expressed in the policy.

Types of personal data collected – The first section of the data protection policy should clearly define its scope which includes identifying the types of personal data collected.

Data storage duration – This variable requires the policy to explicitly express the period for storage of the personal data collected. Though companies that pointed out that data storage was in accordance with the law equally earned a credit.

Right to access personal data – This variable requires policies to notify data subjects of their right to access personal data. Data subjects can get more information and a copy of their personal data with this right. Additionally, it gives data subjects the ability to understand how and why businesses are using their data and to confirm that this use is permitted by law.

Right to update, correct, or erase personal data – The right of the data subject to have their personal information corrected, deleted, or erased should be explicitly stated in the privacy policy. This privilege may be used if the company's database has inaccurate information that needs to be corrected or if the data is no longer needed for the purposes for which it was originally gathered or utilized.

Right to restrict or object to data processing - The privacy policy shall advise the data subject of his right to limit or object to data processing. This implies that the usage of data subjects' information can be restricted. This right can be used when there is a dispute over the accuracy of the data, when the data is no longer needed but cannot

be erased due to legal restrictions, or when their objection to processing is still being considered and decided.

Right to withdraw consent at any time - The right to revoke consent at any moment should be mentioned in the privacy policy for the data subject. The data subject must be made aware that they have the option to give consent either orally (for health-related circumstances) or in writing (for financial or e-commerce purposes) prior to giving consent. The withdrawal of consent has no bearing on the legality of processing carried out with that consent before it was withdrawn. For this indicator, a score is given for each of the previously mentioned categories.

c. Data collection and Third-Party Data transfers

The privacy policy should disclose data access and transfers to external parties, ensuring data subjects' information is not unlawfully disclosed to third parties. This indicator was evaluated along the following variables:

Data collection and privacy policy compliance – This variable requires the privacy policy to clearly outline the nature and category of personal data that will be collected.

Data collection compliance – Privacy policies must disclose information usage and flow of data on applications. Privacy International's interception environment tool analyzes data usage by platform developers and third parties, allowing for device-to-device data flow analysis.[1]

Data sharing and privacy policy compliance – The privacy policy should outline access to collected data and potential data transfers to external parties. Technical analysis - software, Ghostery,[2] Blacklight,[3] and Exodus[4] programs is used to identify web trackers on the company's website or mobile application, which collect user information for online services like digital advertising and website analytics, with cookies being the most common.[5]

d. Practice Robust Data Security

Companies must commit to robust data security measures, with data controllers or processors safeguarding personal data from accidental access, erasure, alteration, disclosure, or destruction, and their privacy policy should clearly outline this. The Qualys SSL Labs software is used for a technical analysis of a company's website, grading its setup quality.

A security header software evaluates a website's security, focusing on SSL Server score, privacy policy, and security header score.[6] SSL server scores indicate website setup accuracy, valid address, error likelihood, trustworthiness, and vulnerability to cyber-attacks and data breaches. Privacy policy scores highlight technical and organizational measures for personal data security. Security header scores indicate if the website has security directives for web browsers, preventing client-side vulnerabilities from cyber-attacks and data breaches.

e. Accountability

A company's transparency report, published in the year under review, discloses key metrics and data governance information on a platform. It may include third-party requests for users' private data, content, and platform enforcement measures, depending on company policies, intellectual property laws, and local regulations.

F. Availability of Internal redress mechanisms for data breaches

This indicator requires a company privacy policy to explicitly provide for internal remedy mechanisms for data and privacy breaches, with extra credit given for impartiality, timely processing, and accessibility of these mechanisms.

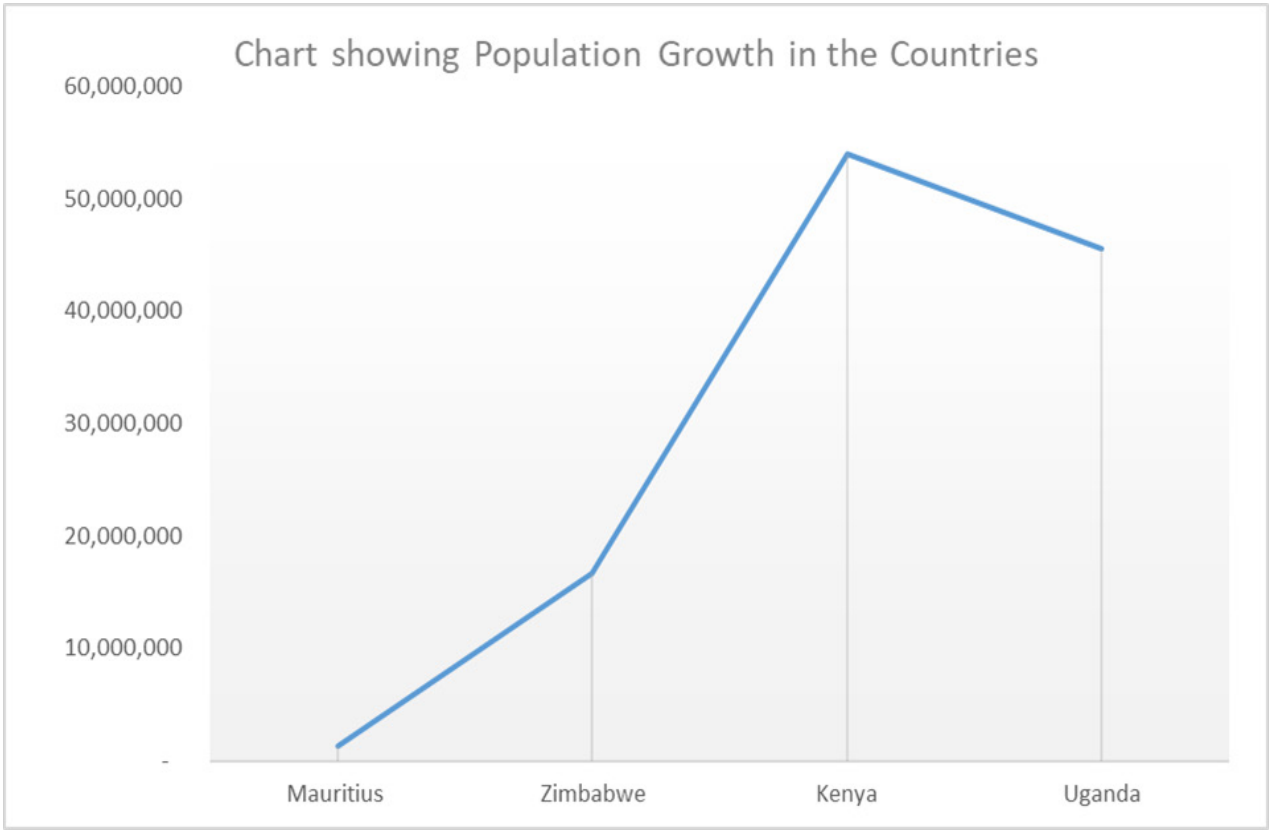
1. 'Data Interception Environment' (Privacy International) at https://privacyinternational.org/learn/data-interception-environment accessed 30 October 2023.
2. https://www.ghostery.com/ at accessed 30 October 2023.
3. https://thermarkup.org/blacklight at accessed 30 October 2023.
4. https://reports.exoduc-privacy.eu.org/en/ at accessed 30 October 2023.
5 M.J Kelly, 'What is a Web Tracker' (Mozilla, 2019) at https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/ accessed 31 October 2023.
6. Security Headers https://securityheaders.com/.

3. Country Insights

This section that is divided into four parts, sets out to give insights into the four countries; highlighting the context in each country, an analysis of the personal data protection and privacy rights landscape, legal and regulatory framework and findings. In turn, these are all discussed in detail below.

3.1 Country Context

This part highlights the context in Mauritius, Zimbabwe, Kenya and Uganda. All four countries, have implemented data protection laws to strengthen the control and personal autonomy of individuals over their personal data, while at the same time ensuring growth and development of their respective digital economies. Two out of the four countries are landlocked – Zimbabwe and Uganda. Kenya and Uganda are characterised by a high population density compared to Zimbabwe and Mauritius. The chart below shows a comparison in population growth across the countries.



3.1.1 Mauritius

Mauritius is a developing island nation off the southeast coast of the African continent in the southwest Indian Ocean with approximated population of 1,262,523 people.1 It is located east of Madagascar the 6th State and the first African country to ratify Convention 108+ established by the Council of Europe.2 Mauritius is a major tourist destination, and the tourism sector is one of the main pillars of the Mauritian economy.

The island nation enjoys a tropical climate with clear warm sea waters, beaches, tropical fauna and flora, complemented by a multi-ethnic and cultural population.3 Whereas the data protection legislation has been in existence for a while, its application has become increasingly relevant over the recent years to keep up with the evolution of digitalization.4 This has seen a growing awareness of the importance of data protection in Mauritius through trainings, interviews and publications in the media by the Data Protection Office.5 Though the data protection legislation upholds international standards, disparities remain. Mauritius's DPO that has been operational since February 2009, is still under the Ministry of Technology, Communications and Innovation (MoTCI). The office is headed by a Data Protection Commissioner who enjoys a wide range of enforcement powers to assist in ensuring that the principles of data protection are observed.

To that end, this office has progressed on a number of aspects particularly, submission of an annual report to the National Assembly of Mauritius provided for under section 55 of the Data Protection Act each year. At the time of writing this report, the 2022 Annual Report was readily available and accessible on its online portal.6 Equally, the office is credited for putting in place different regulations and practice codes to give effect to the Act, such as the Code of Practice for CCTV Systems operated by Mauritius Police Force,7 Code of Practice for the operation of Safe City Systems,8 Data Protection Guide for Financial Sector,9 Guide on usage of unmanned aircraft systems in compliance with data protection, Guidelines -Data Protection Act 200410 and Data Protection (Fees) Regulations 2020.11 As part of its mandate, the office undertakes complaints management where a total of 71 complaints12 in relation to use of CCTV cameras, alleged breach of personal information by government bodies, alleged disclosure of personal data, unlawful use of personal data, etc were received and 57 personal data breach notifications.13 Of the 71 complaints, 36 were closed while five were resolved through amicable settlement.

1. Statistics Mauritius https://statsmauritius.govmu.org/Pages/Statistics/ESI/Population/Pop_Vital_Jan-Jun22.aspx accessed 6 December 2023.
2. Data Protection & Privacy 2023: Trends and Developments, last Updated February 06, 2023 at accessedhttps://practiceguides.chambers.com/practice-guides/data-protection-privacy-2023/mauritius/trends-and-developments#:~:text=-freedoms%20of%20others.- ,Data%20Protection%20Office,especially%20in%20this%20digital%20age.
3. Mauritius – A Country Profile at https://www.nationsonline.org/oneworld/mauritius.htm accessed 30 October 2023.
4. n10 above.
5. Mauritius – Data Protection Overview at https://www.dataguidance.com/notes/mauritius-data-protection-overview accessed 31 October 2023.
6. Mauritius: Office publishes 2022 annual report, 26 September 2023 https://www.dataguidance.com/news/mauritius-office-publishes-2022-annual-report accessed 7 December 2023.
7. Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force https://dataprotection.govmu.org/Pages/Downloads/Publications%20and%20Guidelines/Code%20of%20practice%20issued%20by%20DPC.pdf accessed 12 December 2023.
8. Code of Practice for the operation of Safe City Systems https://dataprotection.govmu.org/Documents/Code%20of%20Practice%20for%20the%20operation%20of%20the%20Safe%20City%20System%28s%29%20by%20MPF.PDF accessed 12 December 2023.
9. Mauritius: Office releases draft data protection guide for financial sector https://www.dataguidance.com/news/mauritius-office-releases-draft-data-protection-guide#:~:text=The%20guide%20aims%20to%20provide,Data%20Protection%20Act%20of%20Mauritius. Accessed 13 December 2023.
10. Data Protection Office https://dataprotection.govmu.org/Pages/Publications-.aspx accessed 13 December 2023
11. Data Protection Regulations https://dataprotection.govmu.org/Pages/The%20Law/Data-Protection-Regulations.aspx accessed 13 December 2023.
12. Mauritius: Office Publishes 2022 Annual Report (n14 above) p31.
13. DPO – Data Protection Office https://dataprotection.govmu.org/Pages/Decisions/Decisions-on-Complaints.aspx accessed 7 December 2023

3.1.2 Zimbabwe

Zimbabwe is a landlocked country in Southern Africa with a population of about 16.7 million people.[1] The economy has struggled with hyperinflation and instability over the past decades but is transitioning to being more market-based. Digital transformation initiatives by both public and private sectors have increased the adoption of technologies like mobile money and e-government services. However, cybersecurity threats and data privacy concerns have emerged as more user data is collected and processed digitally.

Zimbabwe has seen rapid growth in digital financial services and internet-based businesses over the past decade. Mobile money systems like Ecocash have enabled digital payments and remittances, providing financial access to millions. E-commerce platforms like Hwedza Markets allow rural entrepreneurs to sell goods online. Fintech lending apps offer quick digital loans. While such digital services have accelerated, they have also increased risks of personal data misuse, breaches, and surveillance. Financial apps and telecommunications hold extensive customer transactional and communications data. E-commerce sites collect names, addresses, purchases and browsing history.

The lack of comprehensive data protection law prior to late 2021 created an environment of poor data governance. The coming into effect of the Data Protection Act in December 2021, represented a major milestone and a sound foundation for data protection confirming to global norms. The law among other things, designates the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as the national data protection regulator. This dual role under POTRAZ was meant with a lot of criticism during public consultations as concentrating expansive powers within a single entity among other things.[2] While POTRAZ faces the challenges of establishing a new oversight mandate, it is credited for the efforts on advancing the Cyber and Data Protection Regulations, 2020[3] aimed at protecting personal data and privacy in the country in addition to the Data Protection Act that at least equips it with a statutory basis, responsibilities, and powers that simply did not exist under the previous void. The region awaits their operationalisation in line with acceptable international principles and standard. Though, still nascent, the office is credited for the efforts to advance complaints management. At the time of writing this report, the office was to mount investigations following a petition from Misa Zimbabwe on alleged third-party access to personal data.[4]

1. World Population Dashboard Zimbabwe https://www.unfpa.org/data/world-population/ZW accessed 6 December 2023.
2. Misa Zimbabwe. (2021). Analysis of the Data Protection Act. https://zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection- act/#:~:text=The%20object%20of%20this%20Act,their%20representatives%20and%20data%20subjects%E2%80%9D accessed 11 October 2023. Privacy International's Submissions on the Cyber and Data Protection Regulations Bill 2019 to the Parliament of Zimbabwe https://privacyinternational.org/sites/default/files/2020-07/Submission%20on%20the%20Cyber%20Security%20and%20Data%20Protection%20Bill%202019%20to%20the%20Parliament%20of%20Zimbabwe.pdf accessed 11 October 2023.
3. Data Guidance: Zimbabwe: POTRAZ announces the release of draft Cyber and Data Protection Regulations https://www.dataguidance.com/news/zimbabwe-potraz-announces-release-draft-cyber-and-data accessed 13 December 2023.
4. Misa Zimbabwe: POTRAZ to investigate alleged third-party access to personal data https://zimbabwe.misa.org/2023/05/09/potraz-to-investigate-alleged-third-party-access-to-personal-data/ accessed 7 December 2023.

3.1.3 Kenya

Kenya is an East African country with a population of about 54 million people.1 Kenya has one of the largest and most diversified economies in Sub-Saharan Africa, fuelled by a vibrant technology and financial services sector. However, as digital services expand, risks around personal data protection and privacy have emerged given the extensive user information collected by mobile apps, fintech companies, e-commerce platforms and other online businesses operating in Kenya.

While Kenya enacted a comprehensive data protection law - the Data Protection Act - in late 2019, implementation remains ongoing. The law establishes principles around lawful data processing, consent requirements, security safeguards, breach notification and data subject rights. An independent Office of the Data Protection Commissioner (ODPC) has also been set up to oversee compliance. The ODPC is financially independent through budget allocation directly from the National Treasury.2 The ODPC is no longer dependent on the Ministry of ICT, Innovation and Youth Affairs to provide funding, and has a significantly larger budget that was increased from Kshs 24 million ($ USD 156,453.72) to Kshs 270 million ($ USD1,760,104.30) that will allow the Commission to fulfill its mandate.3 As part of the set-up, ODPC has its own premises, independent of the ICT Ministry and empowered to recruit its own staff currently approximated at 60 staff members ranging from data protection officers, investigators, to lawyers and much more.

Equally, the ODPC has, as part of its mandate, been timely in formulating operationalising provisions (regulations) to give effect to the Act; among them are the Data Protection (General) Regulations,4 the Data Protection (Compliance and Enforcement) Regulations,5 the Data Protection (Registration of Data Controllers and Data Processors) Regulations6 and Complaints Management Manual.7

1. Office of the Prime Cabinet Sectary and Ministry of Foreign and Diaspora Affairs https://mfa.go.ke/country-profile/#:~:text=The%20population%20is%20approximately%2054,easy%20connectivity%20to%20the%20region. Accessed 07 December 2023.
2. Vellum: 'Data Protection Commissioner announces opportunities for the ODPC and stakeholders to collaborate during dual data protection report launch' by Amrit Labhuram, 3 December 2023. https://vellum.co.ke/data-protection-commissioner-announces-opportunities-for-the-odpc-and-stakeholders-to-collaborate-during-dual-data-protection-report-launch/ accessed 7 December 2023.
3. Vellum (n17 as above).
4. Data Protection General Regulations https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-General-regulations.pdf accessed 7 December 2023.
5. Data Protection Compliance And Enforcement Regulations https://www.odpc.go.ke/wp-content/uploads/2021/04/THE-DATA-PROTECTION-COMPLIANCE-AND-ENF ORCEMENT-REGULATIONS-2021.pdf accessed 7 December 2023.
6. Registration Of Data Controllers and Data Processors Regulations https://www.odpc.go.ke/wp-content/uploads/2021/04/Data-Protection-Registration-of-data-controllers -and-data-processor-Regulations.pdf accessed 7 December 2023.
7. ODPC Complaints https://www.dataguidance.com/sites/default/files/odpc_complaints_2.pdf accessed 7 December 2023.

3.1.4 Uganda

Uganda like Zimbabwe, is equally a landlocked country in East Africa and bolsters a population approximated at 45.5 million people with 53% of Ugandans below the age of 18 and 76% below the age of 30.[1] Among other things, it is heavily characterized by a growing digital landscape and increasing internet penetration. In recent years, the country has made significant strides in developing its information and communication technology (ICT) infrastructure like the recently unveiled digital transformation road map.[2] The road map aims to strengthen the implementation of enabling policies and laws to accelerate Uganda's Digital Revolution. It will provide an overarching implementation framework for a well-connected Uganda that delivers on the opportunities presented by various technologies.[3]

The data privacy and personal data protection situation in Uganda presents a complex combination of progress and challenges. On the positive side, Uganda has taken significant steps in the realm of data privacy. The enactment of the Data Protection and Privacy Act in 2019 and the Data Protection and Privacy Regulation in 2021 marked a pivotal moment for recognizing and addressing data privacy concerns within the country. This legislation empowers individuals by establishing their rights over personal data and imposes obligations on data controllers and processors. Uganda's flourishing tech startup ecosystem and the rising number of internet users underline the country's increasing reliance on digital services.

In Uganda's evolving data privacy landscape, notable developments include: enforcement action against safeboda –a ride sharing app, that was found to have unlawfully disclosed personal data to third parties without the knowledge and consent of data subjects, following a petition against Safeboda's data processing activities to the Speaker of Parliament by UW[4] and investigations into a security data breach at the Uganda Securities Exchange (USE).[5] Equally, is the rapid digitization of government services, financial transactions, and telecommunication. These innovations offer substantial benefits but simultaneously raise concerns about the security and privacy of personal data. The practical implementation and enforcement of data protection laws and regulations are in their nascent stages. Concerns surround the capacity and resources of the National Data Protection Office, responsible for overseeing compliance including its continued existence under NITA-U which does not constitute an independent authority given it is under the general supervision of the Minister of Information and Communication technology (MoICT). Low public awareness of data privacy rights and the importance of safeguarding personal data is an ongoing issue. The absence of effective mechanisms for addressing data breaches also highlights the need for comprehensive education and awareness campaigns to enable individuals to assert their privacy rights

1. UNDP Uganda Common Country Analysis Report P.4 2020 (updated December 2022) at https://www.undp.org/sites/g/files/zskgke326/files/2023-05/UNDP-UG-CCAReport-2023.pdf accessed 30 October 2023.
2. The Digital Transformation Road Map Launched on 17 August 2023 https://ict.go.ug/programmes/digital-transformation-roadmap/ accessed 8 December 2023.
3. Ibid (n 31 above).
4. Privacy International (PI) 'A win for Unwanted Witness: Uganda's data protection authority finds ride sharing app unlawfully disclosed personal data to third parties' https://privacyinternational.org/news-analysis/4459/win-unwanted-witness-ugandas-data-protection-authority-finds-ride-sharing-app accessed 7 December 2023.
5. Abridged Investigation Report of the Data Security Breach at Uganda Securities Exchange (USE) June 2023 https://pdpo.go.ug/media/2023/07/Abridged-Investigation-Report-of-the-Data-Security-Breach-Uganda-Securities-Exchange.pdf accessed 7 December 2023.

3.2 Situational Analysis of data protection and privacy Landscape in all four countries

All four countries have implemented data protection laws to strengthen the control and personal autonomy of individuals over their personal data, while at the same time ensuring growth and development of their respective digital economies.

In Mauritius, the current data protection legislations provide various levels of protection to its citizens through the Act.[1] It provides for the collection, storage and use of personal data requiring explicit consent of the data subjects before collection and processing of personal data. It imposes stricter rules and regulations on the collection, storage and use of special categories of data including in relation to race, ethnic origin, political views, religious or philosophical beliefs, genetic or biometric data, sexual orientation or preferences which is usually sensitive in nature. Short of express consent from the data subjects, controllers and/or processors can be granted permission to transfer personal data to another jurisdiction upon satisfying that the recipient country has the equivalent or a higher standard of data protection. There is a general prohibition to process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian. Organisations are required by the Data Protection Office (DPO) to consider the need to protect children and design their systems and processes bearing this in mind.

To ensure that national and public security projects are being effectively implemented while also taking into consideration the potential ramifications of violating the fundamental rights of data subjects, the Act requires for a Data Protection Impact Assessment (DPIA) to be undertaken. Equally, Mauritius has ensured a harmonious balance between protecting personal data and surveillance activities and failure to carry out a DPIA due to a higher risk of human rights violations, is a criminal offence.

With the rise of virtual assets and currency worldwide, Mauritius has developed legislation geared towards the protection of personal data in virtual transactions which requires digital transferring, processing, storing and trading of information. However, this poses a risk to users engaged in virtual assets as trading currencies as these transactions are decentralised and unregulated by conventional banks.

Worth noting is Mauritius's proactiveness in ensuring that it meets the latest AI trends in financial technology including modernizing other sectors like the healthcare system. However, AI-oriented technologies pose a real risk to data breaches and security of information despite its revolutionary technological abilities.

In Zimbabwe, the Data Protection Act is only 22 months old following its passage in December 2021 paving way to significantly strengthen the legal landscape for the protection of personal data and privacy rights. This new law provides for consent requirements, security obligations, breach notifications and enforcement mechanisms that did not previously exist bringing the country closer to internationally acceptable standards on data protection and privacy. Like Mauritius, the Act among other things provides for differing levels of treatment in data including classification as sensitive or non-sensitive with corresponding consent requirements. Equally, data controllers/processors are required to disclose their practices transparently, data subject can access and correct their information and independent oversight lies with the data protection authority.

While the above set good foundations, turning principles into practice remains challenging. The regulators must build capacity for monitoring compliance, audits, complaint handling and investigations. Data controllers have to overhaul systems to meet consent, security and breach notice requirements. Lack of expertise and resources at companies is a constraint. Ongoing review and amendments to regulations will be needed. Other key challenges include low public awareness of data protection issues and new rights under the Act, regulatory capacity needs further development, resistance from certain data controllers due to compliance costs is likely and some provisions of the Act have drawn criticism for being potentially overbroad or ambiguous in ways that could enable surveillance overreach.

Additionally, there is increased use of digital loans, fintech and e-commerce platforms that raise new data protection and consent concerns. Equally, cybersecurity policy continues to present tensions around privacy and sur-

1. The Data Protection Act, 2017 of Mauritius.

veillance. As Zimbabwe's economy digitizes further and citizens continue to gain digital access, public awareness campaigns will be key and personal data use cases will multiply, requiring vigilance.

Equally, Kenya's Data Protection legislation closely follows acceptable international standards modelled along precedents like EU's GDPR with adaptations for the country context. It provides for key principles of lawful processing, purpose limitation, data minimization, storage limitation and accountability obligations for both private and public sector data handlers. Requirements like detailed consent rules, breach notification, strong security safeguards, avenues for redress and enforcement powers aimed to restrict misuse and abuse of Kenyans' personal data.

Kenya has seen rapid growth in digital services over the past decade, with extensive adoption of mobile money, e-commerce, ride-hailing apps (applications) and digital lending platforms. However, this digital transformation has also increased risks of personal data misuse, breaches, and unauthorized surveillance given the collection of sensitive information like financial transactions, location data and communications by both private sector apps and government systems. For instance, fintech lenders capture extensive details on applicants including contacts, photos, and SMS logs to determine creditworthiness. E-commerce sites store names, browsing histories and purchases. Telecom operators hold subscriber information, call records and location data.

However, implementing comprehensive data protection remains challenging as controllers, processors and regulators build expertise to align systems with the law. While the ODPC is now formally established and key regulations issued, it continues to scale up staff, frame compliance procedures and plan audit mechanisms for oversight. Training controllers on detailed consent flows, data mapping and rights facilitation is still a work in progress. It has steadily built initial capacity, though its oversight capabilities require continued investment to supervise diverse sectors.

Enforcement actions have begun but remain limited as the ODPC focuses initial efforts on advice giving. Creating awareness among the public regarding their new data rights also lags. Worth noting, so far the ODPC by February 2022, had received so far 400 complaints mostly relating to unsolicited marketing calls and messages with 200 already resolved. This not only demonstrates trust in the authority's redress mechanism that is still in its infancy, but also highlights the need for more training of data controllers/processors on fulfilment of consent requirements. As already noted above ODPC has offered different regulations aimed to foster compliance and issued its first monetary penalty in December 2022 against a school for unlawfully publishing a student's photo without consent. While enforcement actions remain limited currently, the ODPC intends to take a responsive approach based on controller attitude and compliance history.

In sum, while the Data Protection Act has established a progressive legal framework for data protection in Kenya aligned with global norms, turning principles into organizational practices remains at an early stage. There is significant room for growth in transparency, accountable data stewardship and embedding privacy by design into digital services. Effective implementation will necessitate consolidated efforts by policymakers, industry, civil society and technology experts, under the ODPC's oversight. But the law provides a firm foundation for advancing data protection to match the pace of Kenya's digital transformation.

Uganda, equally is heavily characterized by a growing digital landscape and increasing internet penetration. In recent years, the country has made significant strides in developing its ICT infrastructure. The data privacy and personal data protection situation in Uganda presents a complex combination of progress and challenges.

On the positive side, Uganda has taken significant steps in the realm of data privacy. The enactment of the Data Protection and Privacy Act in 2019 and the Data Protection and Privacy Regulations in 2021 as noted above, marked a fundamental moment for recognizing and addressing data privacy concerns within the country. This legislation empowers individuals by establishing their rights over personal data and imposes obligations on data controllers and processors. Uganda's flourishing tech startup ecosystem and the rising number of internet users underline the country's increasing reliance on digital services.

In Uganda's evolving data privacy landscape, notable developments include the rapid digitization of government services, financial transactions, and telecommunication. These innovations offer substantial benefits but simultaneously raise concerns about the security and privacy of personal data. So far, the National Data Protection Office is taking noticeable efforts to receive and resolve complaints as observed in the cases that have been previously mentioned above.

Overall considerable challenges continue to persist. Particularly, the implementation and enforcement of data protection laws are in their early stages, with concerns about the Data Protection Office's capacity and resources. Low public awareness of data privacy rights and the lack of effective mechanisms for addressing breaches underscores the need for comprehensive education and awareness campaigns.

Equally, the data protection offices are either attached to the ministries of communication/ICT or other governing

authorities, with among other things no power to recruit their own staff. In Uganda, for instance, the DPO is under NITA-U which does not constitute an independent authority given it is under the general supervision of the Minister of Information and Communication technology (MoICT). Mauritius's office of Data Protection is much older but still operates from the Ministry of ICT building and does not have the power to recruit its own staff and continues to suffer from lack of requisite personnel.[2] This is not any different in the case of Uganda's PDPO or Zimbabwe's POTRAZ despite efforts towards adequate staffing levels, awareness within the industry on how to operationalize fair data practices, and building oversight capacity.

Further still, taking stock of the complaints handling function and enforcement mechanisms reveals low levels in executing enforceable actions by the different data protection offices. The existing mechanisms remain limited, in infancy and predominantly untested. The report so far notes ODPC's efforts where the office has received over 400 complaints with half already resolved as at February 2022 and an inaugural monetary penalty issued in December 2022 against a school for unlawfully publishing a student's photo without consent. While Uganda's PDPO, took enforcement action against safeboda –a ride sharing app, that was found to have unlawfully disclosed personal data to third parties without the knowledge and consent of data subjects, following a petition against Safeboda's data processing activities to the Speaker of Parliament by UW[3] and investigations into a security data breach at the Uganda Securities Exchange (USE).[4] Mauritius's DPO has received and resolved complaints[5] in relation to use of CCTV cameras, alleged breach of personal information by government bodies, alleged disclosure of personal data, unlawful use of personal data, etc totaling 71 and also received 57 personal data breach notifications in 2022.[6] Of these, the Office closed 36 complaints, while five other cases were resolved through amicable resolution.[7]

2. Amnesty International Kenya Data Protection Report 2021, p18 https://restoredatarights.africa/wp-content/uploads/2021/12/Amnesty-International-Kenya-Data-Protection-Report-Pages-1.pdf accessed 7 December 2023.
3. Privacy International (PI) 'A win for Unwanted Witness: Uganda's data protection authority finds ride sharing app unlawfully disclosed personal data to third parties' https://privacyinternational.org/news-analysis/4459/win-unwanted-witness-ugandas-data-protection-authority-finds-ride-sharing-app accessed 7 December 2023.
4. Abridged Investigation Report of the Data Security Breach at Uganda Securities Exchange (USE) June 2023 https://pdpo.go.ug/media/2023/07/Abridged-Investigation-Report-of-the-Data-Security-Breach-Uganda-Securities-Exchange.pdf accessed 7 December 2023.
5. DPO – Data Protection Office https://dataprotection.govmu.org/Pages/Decisions/Decisions-on-Complaints.aspx accessed 7 December 2023.
6. Data Protection Office, Annual Report 20 July 2022 at p 31 https://dataprotection.govmu.org/Documents/AR22%20DPO.pdf accessed 7 December 2023. Mauritius: Office publishes 2022 annual report, 26 September 2023 https://www.dataguidance.com/news/mauritius-office-publishes-2022-annual-report accessed 7 December 2023.
7. Mauritius: Office publishes 2022 annual report, 26 September 2023 https://www.dataguidance.com/news/mauritius-office-publishes-2022-annual-report accessed 7 December 2023.

3.3 Existing Legal and Institutional Framework on Data Protection and Privacy

As the potential for increased data sharing with domestic and international private entities grows, challenges and opportunities arise. To address these dynamic data privacy concerns, the different regulatory framework in all four countries and the region at large must adapt to both foster innovation and protect individual rights effectively. The above mentioned developments including enforcement actions so far are a step in the right direction.

3.3. Existing Legal and Institutional Framework on Data Protection and Privacy

As noted above, all the countries under review have in place data protection laws to strengthen the control and personal autonomy of individuals over their personal data. As such, this part shades light onto the existing legislation, policies and regulations on personal data protection and privacy rights which are discussed in detail below;

3.3.1 Legal and Institutional framework in Mauritius

Mauritius boosts a robust framework with the right to privacy expressly provided for in Sections 3 and 9 of Constitution and Article 22 of the Civil Code. These are operationalized by the Data Protection Act 2017 that provides for the collection, storage and use of personal data. Similar to the GDPR, the Act requires the explicit consent of data subjects (i.e., individuals whose data is being collected, stored and processed) before collecting and processing their personal data. Controllers and/or processors have the duty to, inter alia, and inform the data subject on the reasons for collecting their data and where it is being stored. The Act also provides data subjects with individual rights such as the right to access their personal data, the right to request that inaccurate data be amended, and the right to request that their data be deleted.

Additionally, the Act also provides for a) differing levels of treatment in data types- between personal data and special categories of data imposing stricter rules and regulations on the collection, storage and use of special categories of data; b) prohibits processing of personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian. Organisations are required by the Data Protection Office (DPO) to consider the need to protect children and design their systems and processes bearing this in mind; c) sets out clear rules for the transfer of data across foreign jurisdictions; d) appointment of a Data Protection Officer who among other things is the first point of contact for the DPO and for data subjects.

Equally, the Act allows for exceptions to certain protected rights provided they constitute a necessary and proportionate justification- protection of national security, defence or public security, for the purpose of historical, statistical or scientific research; protection of judicial independence and judicial proceedings; prevention, investigation, detection or prosecution of an offence, including the execution of a penalty; an objective of general public interest; and protection of a data subject or the rights and freedoms of others.

Another legislation playing a crucial role in protecting the privacy of data subjects is the Cybersecurity and Cybercrime Act 2021. That aims to protect information, equipment, device, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. More recently, the DPO introduced the financial data protection guide as part of the efforts to put in place regulations and codes of practice to facilitate compliance and implementation of the data protection law.

3.3.2 Legal and Institutional framework in Zimbabwe

The primary legislation governing data protection in Zimbabwe is the Constitution as the supreme law of the land which explicitly recognizes the right to privacy in section 57.[1] This right includes; the right not have one's home, premises or property searched, not to have the privacy of communications infringed upon or health condition disclosed. This is operationalized by the Data Protection Act, enacted recently in December 2021 as the newest legislation in the region. This law establishes a comprehensive legal framework for personal data protection in ac-

1. Law Portal Zimbabwe https://lawportalzim.co.zw/cases/civil/974/constitutional-rights-re-privacy accessed 11 December 2023.

cordance with globally acceptable standards and best practices. The Act outlines key principles, rights, obligations, and procedures pertaining to the collection and processing of personal data by both state and private entities. It represents a major evolution of the legal regime from one lacking robust safeguards on data privacy to one that empowers oversight and individual rights.

The Data Protection Act requires data controllers and processors to meet certain transparency, security, and accountability requirements when handling personal information. It mandates that consent must be obtained from data subjects prior to collection and use of their personal data, while allowing some exceptions. Different rules apply for consent depending on whether data is classified as non-sensitive or sensitive. The law also facilitates important rights of data subjects such as rights to access, correction, and deletion of their information. Violations can attract steep penalties. Overall, the Act provides the core elements of a modern data protection law.

Prior to the Act, there was the Access to Information and Protection of Privacy Act, 2002 which made it an offence to unlawfully disclose personal information held by public bodies, establishing some basic confidentiality safeguards. However, it was criticised as focusing more heavily on access to information provisions rather than robust personal data protections. It does not provide the comprehensive protections, oversight mechanisms, or individual rights enshrined in modern data protection regimes. It established limited confidentiality protections for personal data held by public bodies. Previously also, was the implementation of certain sector-specific regulation for data protection under the financial services and telecommunication regulator. Meaning that data collection and processing activities were governed primarily by principles of contractual consent rather than statutory protections enforceable through an independent authority.

Thus, the Act equips Zimbabwe with a legal basis to uphold principles of lawful, fair, transparent, and accountable data collection and processing in tune with international human rights standards on privacy. It contains key elements that enable the realization of data protection in practice such as mandatory consent procedures for collecting different types of personal data, requiring informed, specific, opt-in consent enabling persons to control use of data instead of passive acceptance of any terms; clear disclosure by data collectors of their data processing activities to understand how information is handled; implementation of adequate technical, administrative and physical safeguards to prevent unauthorized access ,theft, misuse or loss of data; reporting to regulators data breaches within 24hrs to incentivise accountability and rapid response.

3.3.3 Legal and Institutional framework in Kenya

As is with the other countries, the Kenya Constitution in Article 31 protects the right to privacy. This includes the right not to have one's person, home or property searched, possessions seized, information relating to family or private affairs unnecessary required or revealed or the privacy of communications infringed. This is operationalised by other legislation in place particularly, the Information and Communications Act of 2009 and complimentary Regulations of 2010 and; the Data Protection Act, 2019 that closely mirrors global standards exemplified by precedents like the European Union's landmark General Data Protection Regulation (GDPR), 2016. It enshrines principles of lawful, fair and accountable data collection and processing applicable universally to all private and public sector entities as opposed to sector-specific regulation. The Act also contains several key elements that collectively constitute a robust legal scaffolding to translate principles of ethical data protection into organizational practices.

Particularly, the Act, enshrines core data protection principles that mirror standards worldwide, requiring personal data to be processed lawfully, fairly, transparently, collected for explicit and legitimate purposes, limited to what is necessary, accurate, securely retained and accountable. Thus, offering a statutory articulation of fair data handling applicable across the board.[2]

The Act empowers data subjects and confers several rights upon individuals to take control of their personal information, including rights to access, rectification, erasure and objecting to processing subject to reasonable constraints.[3] These entitlements thus, operationalize the principles of autonomy, dignity and redress. Equally, the Act institutes lawful processing mandates and provides for lawful grounds for data processing that balance individual privacy with legitimate interests. Processing must adhere to principles like consent, contract necessity, legal obligations, protection of vital interests and purpose limitation.[4] As noted above, Kenya boosts multiple data protection regulations – Data Protection General Regulations, Data Protection Compliance and Enforcement, Registration of Data Controllers and Data Processors Regulations and Complaints Management manual to foster compliance

2. Section 25, The Data Protection Act, 2019.
3. Ibid Same as above Sections 26 – 27.
4. Ibid Same as above Sections 30 – 32.

and implementation of the data protection laws.

3.3.4 Legal and institutional framework in Uganda

Like the rest of the countries, Uganda has put in place a comprehensive legal framework to address data protection and privacy concerns. The cornerstone of this framework is Article 27 of the Ugandan Constitution, established in 1995 which guarantees the right to privacy, emphasizing the sanctity of a person's home, correspondences, communication, and property. This constitutional guarantee reinforces and supports the data protection and privacy principles laid out in the Data Protection and Privacy Act of 2019 that came into force in February 2019. This Act is designed to protect individuals' privacy and personal data by regulating the collection, processing, storage, and dissemination of personal information. It not only defines the rights of data subjects but also outlines the responsibilities of data collectors, processors, and controllers. To complement the Data Protection and Privacy Act, the Ugandan government issued Data Protection and Privacy Regulations in May 2021. These regulations provide detailed guidelines for implementing the provisions of the act, ensuring a more practical approach to data protection.

The legal foundation for data privacy in Uganda extends beyond the Data Protection and Privacy Act. Moreover, data protection provisions have been incorporated into sectoral laws that regulate specific activities and industries. These laws, including the Electronic Transactions Act, 2011, Computer Misuse Act, 2011, Electronic Signatures Act, 2011, National Information Technology Authority, Uganda Act (NITA-U Act), and the Access to Information Act, 2005, all ensure that data protection considerations are embedded in various sectors of the Ugandan economy.

Uganda's commitment to international data protection standards is evident in the alignment of its legal framework with various international agreements and obligations. The Data Protection Act adheres to international instruments like the International Covenant on Civil and Political Rights, Universal Declaration of Human Rights, UN Convention on the Rights of the Child, United Nations Convention on Migrant Workers, African Charter on the Rights and Welfare of the Child, and African Union Principles on Freedom of Expression. These agreements guarantee that Uganda complies with global data protection norms.

The Data Protection and Privacy Act extends its application to foreign entities, encompassing both natural persons and incorporated bodies. This broadens the reach of the law and ensures that data protection rights and obligations apply to all, whether they are local or foreign entities operating in Uganda. In line with international best practices, the Act defines and emphasizes critical data protection principles such as accountability, fair and lawful processing, specification and purpose limitation, data retention periods, quality assurance, transparency, and the involvement of data subjects.

The Act also defines various offenses related to personal data and prescribes penalties for these offenses. While the penalties have been criticized for their severity, they aim to deter unauthorized data acquisition, disclosure, destruction, deletion, concealment, alteration, and the sale of personal data.

By and large, the frameworks in Mauritius, Zimbabwe, Kenya and Uganda reflect commitments to safeguarding individuals' privacy and personal data while aligning with international data protection standards. These comprehensive frameworks take into account various aspects of data protection, from defining rights and responsibilities to outlining penalties for offenses. However, there are ongoing discussions and criticisms, particularly regarding the extent of implementation of these laws in various sectors including telecommunications, online betting, financial services, e-government, e-commerce, and digital loan services as will be analyzed in this report.

3.4 Findings

This part presents detailed findings from analysis of selected entities' privacy policies, security measures, and transparency practices. It examines how the 48 selected companies/organizations across the six sectors- telecommunication, e-commerce, financial services, e-government, digital loan services and online betting are addressing personal data protection based on their public disclosures. The analysis focuses on evaluating available information on each entity's website against key scoring criteria underpinned by six indicators previously discussed in detail under the section on methodology and selection criteria above. The analysis which is two-pronged namely- country sector findings and an overall assessment of the performance and impact of the findings on personal data protection and privacy rights is discussed in detail below.

3.4 Country Sector Findings

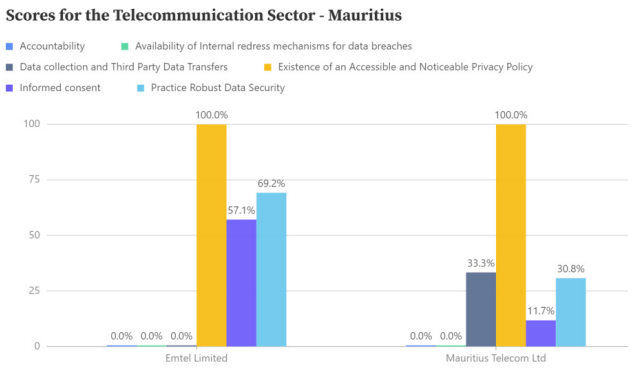
The findings are in respect of eight (8) different companies/entities across the four countries in each of the sectors with some already registered with their respective regulators. Registration with regulators stands as an initial step towards achieving data protection compliance. Two (Uganda and Kenya) out of the four regulators, had readily available published registers of companies on their online portals that had fully registered indicating those with an active status and those that needed to renew their registration.[1] Their respective performance was assessed against six indicators with a selection of two companies/entities per sector as detailed in the earlier parts of this report. The study findings are as follows.

3.4.1.1 Country findings for Telecommunications Sector

In respect of the telecommunications sector, the report focused on the following companies namely: Emtel Limited and Mauritius Telecom Ltd from Mauritius, Econet and TelOne from Zimbabwe, Safaricom and Zuku from Kenya and, Lycamobile and MTN Uganda from Uganda.

a. Emtel Limited and Mauritius Telecom Ltd in Mauritius

Both Emtel Ltd and Mauritius Telecom Ltd, registered the highest score – 100% in respect of the indicator regarding existence of an accessible and noticeable privacy policy and the lowest score –zero percent in respect of indicators -accountability, availability of internal redress mechanisms for data breaches and data collection and third party data transfers. Whereas Emtel Ltd registered better scores than Mauritius Telecom Ltd, but this was only in three out of the six indicators. The figure shows more details of the performance and further discussion on the two companies are below.



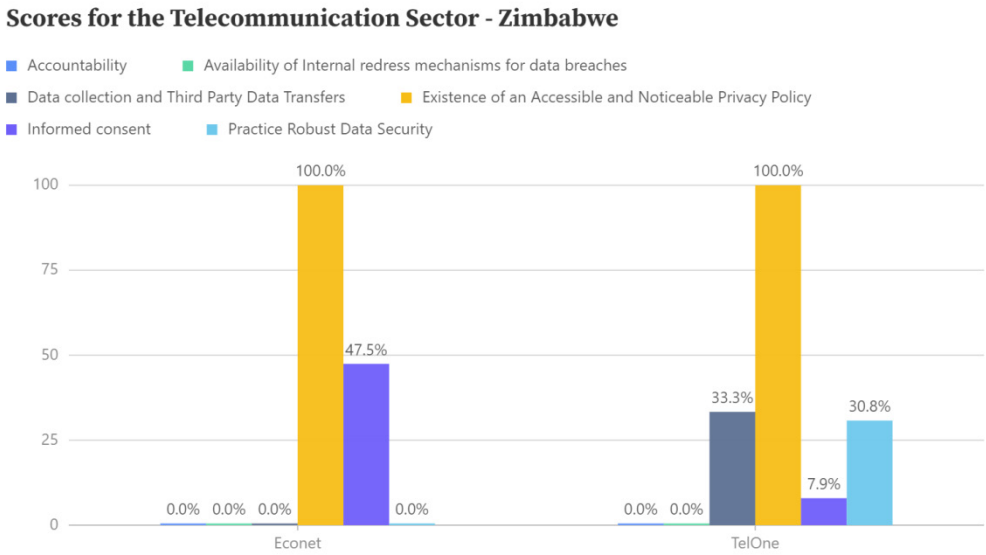
EMTEL has an adequate Privacy Notice. The Privacy Notice's link is prominently displayed on the website's landing page, and the content is written in a clear and easily understandable language. EMTEL privacy notice consists of over 3000 words, and provides users with a comprehensive repository of information essential for them to understand the handling of their personal data before they can avail themselves of services offered by EMTEL.

The Privacy Notice mentions the company's contact details, including the address and phone number; explicitly outlines the purpose of data collection; specifies the different types of data gathered and the purposes for which they are collected; includes information about the data subjects' entitlement to access their personal data; mentions the data subjects' rights to correct their personal data and the right to request the deletion or erasure of personal data; mentions details regarding the data subjects' rights to restrict or object to data processing and explicitly state that data subjects have the right to withdraw their consent at any time. It also provides a summary of the nature and category of personal data to be collected; mentions the entities with whom personal data is shared to provide the service and partially outlines the data security measures implemented to safeguard personal data. However, a transparency report is not currently available, and neither is it mandated by the Data Protection Act of Mauritius and does not include details regarding an internal remedy mechanism for data breaches.

Equally, Mauritius Telecom has a Privacy policy, located on the landing page and its content is presented in a straightforward and easily comprehensible language. It consists of over 1200 words, and provides users with a comprehensive repository of information essential for them to understand the handling of their personal data before they can avail themselves of services offered by Mauritius Telecom and explicitly outlines the purpose of data collection. However, it does not include the company's contact details; does not specify the types of data collected; does not specify the data retention period, does not mention the data subject right to access the personal data, does not mention the data subject right to correct personal data and the right to delete or erase personal data, does not mention the data subject right to restrict or object to data processing; does not mention the data subject right to withdraw consent. It also does not provide the nature and category of personal data to be collected, does not mention the third-party entities with whom personal data is shared to provide the service and does not mention the data security measures implemented to safeguard personal data. Like Emtel Ltd, a transparency report is not currently available, and it is not mandated by the Data Protection Act of Mauritius and it lacks as well information regarding an internal remedy mechanism for redressing data and data breaches.

b. Econet and TelOne in Zimbabwe

Like in Mauritius, Econet and TelOne in Zimbabwe, both registered the highest score for the indicator on existence of an accessible and noticeable privacy policy. The lowest score was registered by both companies in respect of accountability, availability of internal redress mechanisms for data breaches and data collection and third party data transfers indicators. Whereas Econet registered slightly higher scores than TelOne, but this was only in two out of the six indicators. Below, is a figure showing the performance of the two companies and further detailed discussion on the same.



Econet has a published privacy policy but it is difficult to find on its website. The policy uses legalistic and technical wording that hampers readability. It mentions broad data categories collected such as contact, usage, and location but lacks exhaustive specifics. Brief data use purposes like service delivery and regulatory compliance are listed. No data retention period is specified. Contact information includes postal address and email. The policy does not discuss user rights to access, correct, restrict or delete data. It vaguely states data may be shared "where required" without detailing third party recipients. With 9 trackers identified, Econet's website lacks optimal security. Without a transparency report, Econet provides a policy lacking key details and clarity needed to evaluate its data practices.

Econet's privacy policy lacks clarity due to legal and technical wording. It does not comprehensively disclose per-

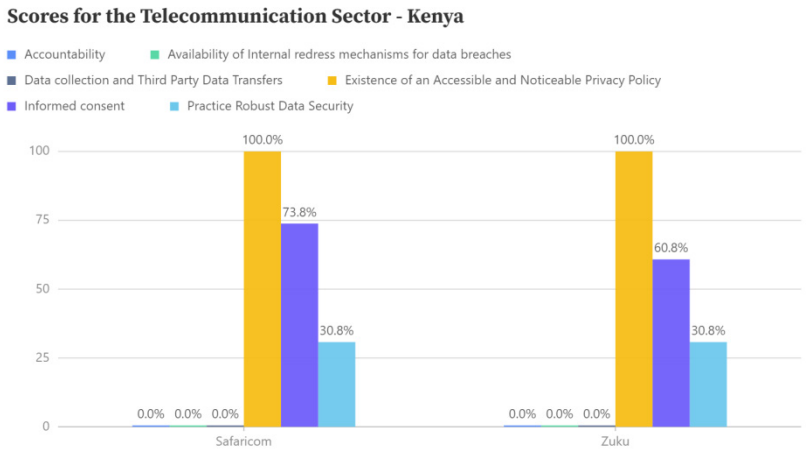
sonal data collected or retention periods. User rights to access, correct, restrict or delete data are not discussed. Third party sharing is only vaguely addressed. With 9 trackers found on the site, Econet lacks optimal security. It does not publish transparency reports. Overall, the policy lacks key details needed to evaluate Econet's data practices.

TelOne on the other hand has a privacy policy published on its website, but positioned inconspicuously in the footer links. The policy employs significant technical jargon making it less readable. It mentions collecting user contact, financial, technical and related data but does not list specifics. Brief purposes like service orders and analytics are noted, while no retention period is specified aside from keeping data per lawful requirements. Contact information provides an address and phone number. User rights to access, correct, restrict or delete data are not mentioned. The policy does not name any third parties with whom data is shared. With only 1 tracker identified on the website, TelOne has moderately strong security measures. In the absence of a transparency report, TelOne's policy lacks key details around data practices and user rights.

TelOne's policy uses technical jargon that hampers readability. It does not provide an exhaustive list of personal data collected or retention periods. User rights are not mentioned. Third party sharing is not addressed. With only 1 tracker identified, TelOne has decent security measures. Still, the lack of transparency around data practices is a concern without public reporting.

c. Safaricom and Zuku in Kenya

In the sector, Safaricom and Zuku in Kenya equally registered the highest performance -100% against the indicator-existence of an accessible and noticeable privacy policy. Both companies had a marginal performance in three similar indicators out of the six, with a 30.8% score registered in respect of the practice robust data security indicator and the lowest score registered against accountability, availability of internal redress mechanisms for data breaches and data collection and third party transfers indicators. Below is a figure showing details of the performance and further discussion on the two companies.



Safaricom, Kenya's largest telecommunications provider, publishes a clear privacy policy listing specific personal data types gathered from over 40 million subscribers. This includes details like identities, age, locations, financial information and usage logs. Service delivery and marketing are stated as purposes of data processing. However, Safaricom's policy lacks specificity regarding data retention schedules for the detailed subscriber information captured. References to security safeguards are high-level without mentioning technical controls adopted. The policy outlines user rights to access and correct data but lacks deletion request procedures. Third party sharing statements only cover obeying lawful requests generically.

Given the sensitivity of communications and individual metadata captured by a telecom of Safaricom's scale, concrete retention periods for logs and location data warrant articulation. More disclosures on specific security measures and surveillance request partnerships would strengthen alignment with privacy by design expectations under Kenyan data protection law.

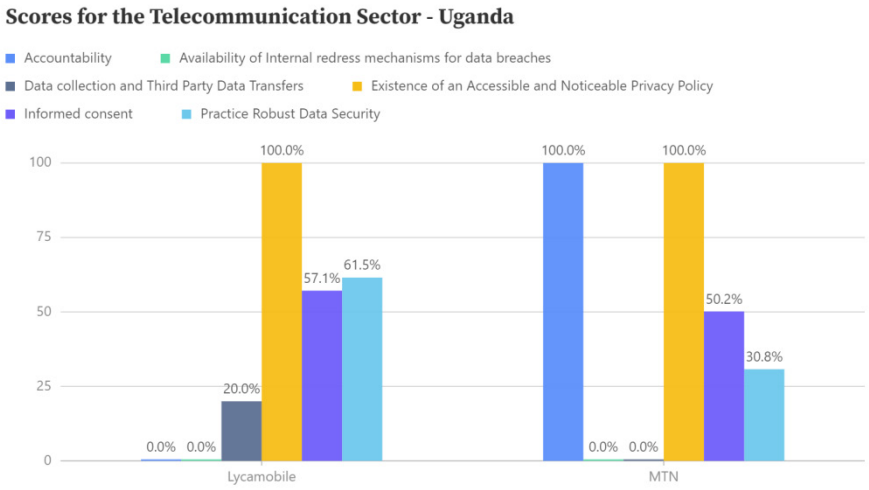
Zuku, a home internet, television and landline provider in Kenya, captures various customer data through subscription and usage like contacts, IDs, financial details, location and traffic logs. Zuku's privacy policy summarizes the types of personal data gathered and purposes like service delivery and marketing. However, it offers limited transparency regarding retention periods for specific data categories. The policy also lacks clear communication

of security technologies and organizational controls adopted. User rights are outlined but deletion request procedures are unspecified. Third party disclosures only cover legal mandate obligations generically.

Given Zuku's role as an internet access provider, concrete retention schedules tailored to browsing histories, usage logs and dynamic IP address records could demonstrate stronger data protection commitments. Listing precise third-party sharing partners rather than blanket statements would also aid accountability. But the presence of a baseline policy is positive.

d. Lycamobile and MTN Uganda in Uganda

Lycamobile and MTN Uganda both registered the highest score for the existence of an accessible and noticeable privacy policy indicator. Equally, MTN Uganda registered the highest score for the accountability indicator. Though, both companies had noticeable scores in 4 out of the 6 indicators, they registered the lowest scores against availability of internal redress mechanisms for data breaches, accountability and data collection and third party transfers. The figure shows details of the performance and further discussion on the two companies below;



Lycamobile and MTN Uganda, across various data privacy indicators, both companies have noticeable privacy policies in place. When it comes to data collection and third-party data transfers, Lycamobile doesn't specify all third-party entities but also, it doesn't allow personal data sharing with advertisers, while MTN's policy doesn't clarify whether data can be shared with advertisers and doesn't list all third-party entities.

Regarding informed consent, Lycamobile generally lists the personal data collected, provides clear reasons for data collection, and mentions data storage as required by law. It includes contact details and grants data subjects the right to access, correct, restrict or object to data processing, though objections are limited to certain types of processing. Unfortunately, data subjects can only access their personal information at a cost of UGX shs 43, 000/-(approximately £10, $USD12), which raises profound concerns about the intersection of data privacy, individual rights, and corporate practices. UW has previously challenged this practice, as privacy should not come at a price.[2] It also doesn't allow permanent deletion of personal data and does not provide for data breach notifications.

MTN's policy generally lists collected data, explains the purposes, but lacks information about data storage duration and explicit contact details within the policy. It grants data subjects unconditional rights to access and correct data but does not mention the right to restrict or object to data processing or consent withdrawal.

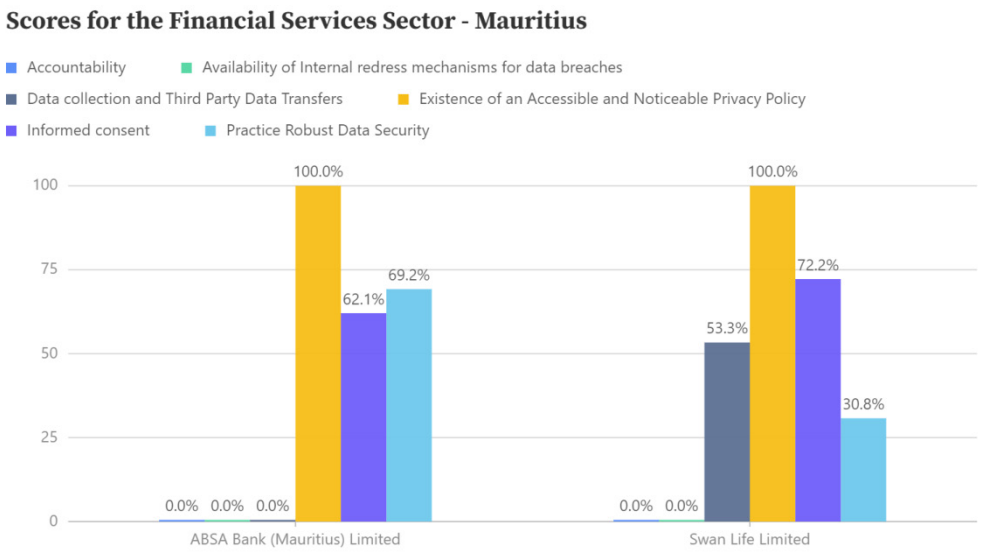
Like Lycamobile, MTN does not provide a straightforward process for permanent data deletion, and its policy does not provide for data breach notifications. In terms of data security practices, Lycamobile has a privacy policy score of 55, a security score of 0, with Privacy Badger blocking 7 potential trackers. It also receives a D grade for security headers. On the other hand, MTN's privacy policy scores 48.6 with a security score of 0, and 4 potential trackers blocked by Privacy Badger. It receives an F grade for security headers. Finally, in terms of accountability, Lycamobile has not published a transparency report since 2022, while MTN has published one during the same period.

3.4.1.2 Country findings for Financial Services Sector

In the Financial sector, the report focused on the following companies namely: Swan Life Limited and ABSA Bank (Mauritius) Limited from Mauritius, CBZ Bank and Empower Bank from Zimbabwe, Stima Sacco and Equity Bank from Kenya and, Stanbic Bank and Pride Microfinance from Uganda.

e. Swan Life Limited and ABSA Bank (Mauritius) Limited in Mauritius

In the sector, Swan Life Ltd and ABSA Bank Ltd in Mauritius registered the highest score for the existence of accessible and noticeable privacy policy indicator. Also, both companies performed relatively well under the informed consent indicator with a difference of 10.1% in the scores and registered very low scores for accountability, availability of internal redress mechanisms for data breaches and data collection and third party data transfers indicators. The figure shows more information the performance and further discussion on the two companies below;



SWAN has a well elaborated Privacy Notice on its website. The link to the Privacy Notice is located on the website's homepage, and its content is presented in a straightforward and easily comprehensible language. SWAN's Privacy Notice comprises of more than 3000 words, offering users a comprehensive source of information that is vital for them to grasp to understand how their personal data is managed before they can access SWAN's services.

The Privacy Notice mentions the company's contact details, including the address and phone number, outlines the purpose of data collection, specifies the different types of data gathered and the purposes for which they are collected, includes information about the data subjects' entitlement to access their personal data, mentions the data subjects' rights to correct their personal data and the right to request the deletion or erasure of personal data, mentions details regarding the data subjects' rights to restrict or object to data processing, explicitly state that data subjects have the right to withdraw their consent at any time. However, it does not specify the data retention period.

The Privacy Notice mentions the nature and category of personal data to be collected, mentions that data is shared with authorities and their business partners for the process of delivering the service. The policy mentions that restricted amount of data is shared with third parties and partially outlines the data security measures implemented to safeguard personal data. However, a transparency report is not currently available, and it is not mandated by the Data Protection Act of Mauritius and does not include information regarding an internal remedy mechanism for redressing data and data breaches.

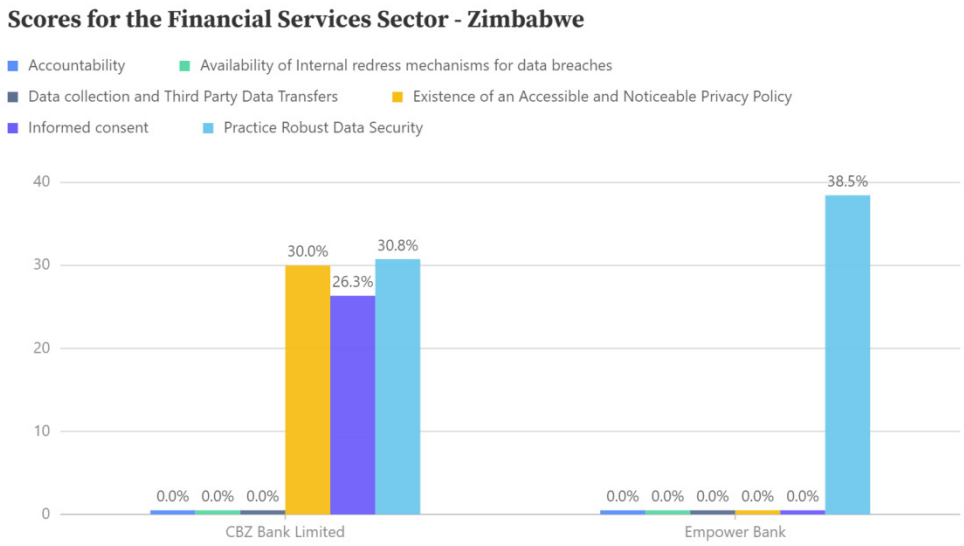
ABSA has an elaborated Data Privacy Statement. The Data Privacy Statement's link is prominently displayed on

the website's landing page, and the content is written in a clear and easily understandable language. It consists of over 1900 words, and provides users with a comprehensive repository of information essential for them to understand the handling of their personal data before they can avail themselves of services offered by ABSA; mentions the company's contact details, including the address and phone number; explicitly outlines the purpose of data collection; specifies a summary of data gathered and the purpose for which they are collected; includes information about the data subjects' entitlement to access their personal data; mentions the data subjects' rights to correct their personal data and the right to request the deletion or erasure of personal data; mentions details regarding the data subjects' rights to restrict or object to data processing; explicitly state that data subjects have the right to withdraw their consent at any time; provides a summary of the nature and category of personal data to be collected; outlines the data security measures implemented to safeguard personal data.

However, The Data Privacy Statement does not specify the data retention period; nonetheless, it does clarify that data is destroyed as soon as is reasonably practicable and in line with prevailing record retention legislation. It does not mention the third-party entities with whom personal data is shared to provide the service; a transparency report is not currently available, and it is not mandated by the Data Protection Act of Mauritius and does not include information regarding an internal remedy mechanism for redressing data and data breaches.

f. CBZ Bank and Empower Bank in Zimbabwe

Unlike Mauritius, Kenya and Uganda in this sector, the two companies in Zimbabwe registered relatively very low scores. Empower Bank in Zimbabwe registered 38.5% as the highest score under the practice robust data security indicator. Closely followed by a 30.8% score of CBZ Bank which, equally registered a 30% score for the existence of an accessible and noticeable privacy policy. The figure below shows more details of the performance and a further discussion on the two companies;



CBZ Bank has published its privacy policy prominently on the website footer and under terms and conditions, making it clearly noticeable. The policy is reasonably readable, though contains some legalistic wording. It uses a phrase like “including” rather than exhaustively listing all personal data collected. Whereas it explains the purposes of data use such as orders, security and legal compliance, but it does not specify the retention period for the data. Contact information including address, email and phone are provided. The policy does not mention user rights to access data or restrict processing. It states data may be shared where required by law or regulation without detailing all third parties. With 6 trackers identified on the site, CBZ has moderate security gaps. No transparency report is published. While more visible than other policies, CBZ's privacy policy lacks important details around data retention, user rights, and third-party sharing.

CBZ Bank has a privacy policy readily visible through website links and footers. The policy uses legalistic language but is reasonably clear. It does not provide an exhaustive list of all personal data collected. Purposes are explained generally. No data retention period is specified. User rights to access, restrict processing or delete data are not discussed. It states data may be shared as required by law without naming third parties. With 6 trackers found on the site, CBZ has some security weaknesses. No transparency report has been published by the bank.

The website of Empower Bank, a commercial banking services provider in Zimbabwe, does not contain any published privacy policy detailing its practices and policies around customer data processing, protection and sharing. Even if there is a small link at the bottom of the website that is labelled with ‘Privacy Policy’, this link leads to an

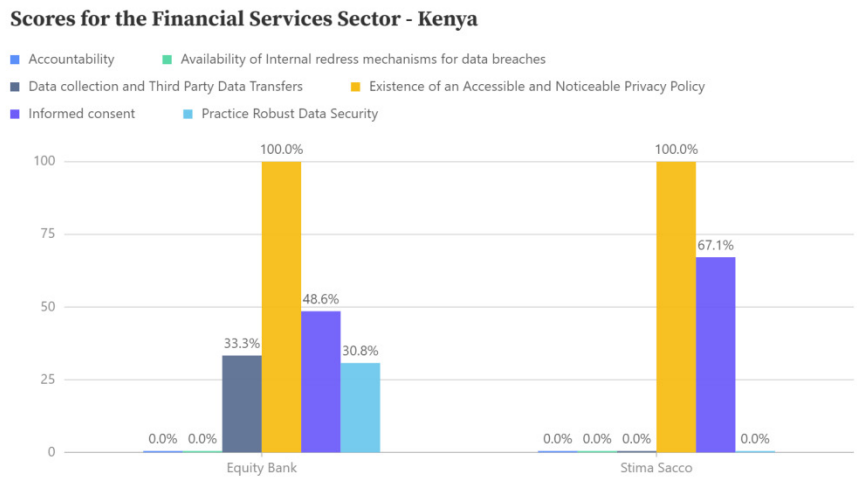
empty website, with nothing published on it. As a financial entity managing sensitive user information like transaction records, income details, identification data, credit history and more, this complete lack of a privacy notice represents a serious omission violating norms of transparency and lawful data handling.

Banking customers entrust various private details to Empower Bank with the expectation their data will be handled confidentially per norms of financial sector regulation. The absence of any visibility into the bank's data collection, purposes of use, retention durations, internal controls, security systems or third-party sharing arrangements precludes informed consent by account holders regarding use of their personal data. It also undermines trust that robust cybersecurity measures are applied to safeguard systems given the lack of any public attestation.

While Empower Bank's website showed only 4 trackers indicating decent baseline security controls, the bank still has an imperative as a regulated financial entity to articulate its data practices, risk assessments and safeguards through a clear, comprehensive published statement of privacy policy. As more services digitize, conveying transparent assurances to account holders through such disclosure is vital to maintain legitimate data processing aligned with Zimbabwe's data protection law.

g. Stima Sacco and Equity Bank in Kenya

As is with companies in Mauritius and Uganda in this sector, Stima Sacco and Equity Bank in Kenya registered the highest score – 100% under the existence of an accessible and noticeable privacy policy, closely followed by 67.1% and 48.6% scored respectively for the informed consent indicator. Below, a figure shows more details of the performance and a further discussion on the two companies;



The privacy policy published by Stima Sacco, a savings and credit cooperative (SACCO) providing financial services to 140,000 members, demonstrates partial transparency on personal data practices for aspects like shares, deposits and loans. The policy lists general data types collected, covering names, IDs, contact details, photographs and financial records. Broad purposes like managing accounts, fraud prevention, regulatory requirements and marketing are outlined as well. However, no specific retention schedule or deletion protocol is detailed for different data types like transactions versus identities. References to data security safeguards are also nonspecific.

Rights to access and correct personal data are stated without conditions, but data erasure requests require contacting Stima Sacco creating a barrier. Third parties receiving data are only described vaguely as legal and regulatory authorities. Overall, Stima Sacco's policy provides an overarching summary of member data practices but lacks the specificity expected under the Data Protection Act for security, retention and sharing.

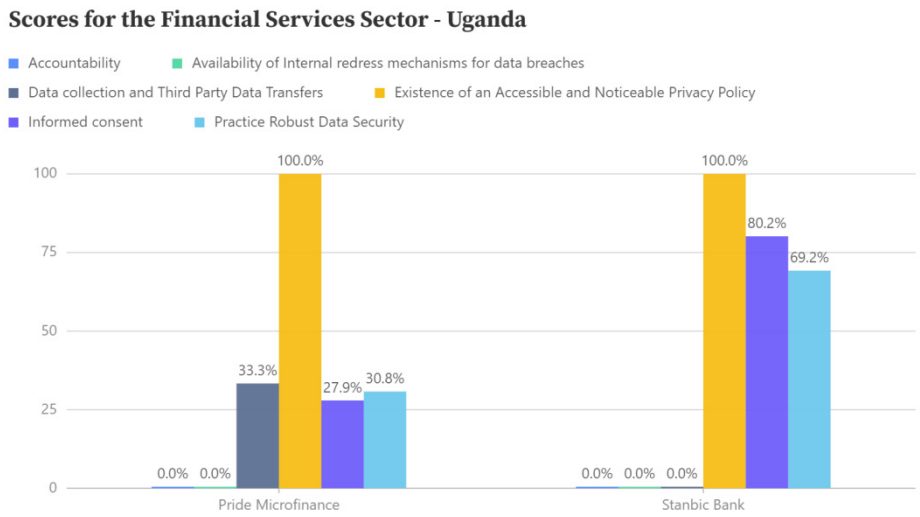
Equity Bank, a commercial bank serving over 14 million account holders in Kenya, publishes a relatively clear privacy policy but lacks exhaustive details in key areas. Personal data types like identities, contacts, financial history, devices and biometrics are listed in summary form rather than as a comprehensive inventory. While purposes such as orders and fraud prevention are outlined, data retention schedules and deletion protocols are absent. The policy states account holders can access their data but makes no reference to correcting or deleting records on request. Data security is only described in generalized language without elaborating safeguards adopted. Third party sharing is mentioned as obeying legal requirements without naming specific recipients like credit agencies or government authorities.

Given the volumes of sensitive financial information processed from customer activities, transactions and third-party integrations, Equity Bank warrants more granular transparency into data handling, retention, security

mechanisms and sharing partnerships. While it has a baseline policy, strengthening specificity in disclosures would boost compliance.

h. Stanbic Bank and Pride Microfinance in Uganda

Both Stanbic bank and Pride Microfinance equally registered the highest score – 100% for the existence of an accessible and noticeable privacy policy indicator. Very low scores were registered for accountability, availability of internal redress mechanisms for data breaches and data collection and third party transfers indicators. Though Stanbic Bank registered relatively good scores, but this was only in three indicators out of the six. Below, the figure shades more light on the performance and a further detailed discussion on the two companies;



In the realm of financial services, both Stanbic Bank and Pride Microfinance have noticeable privacy policies in place. However, when it comes to data collection and third-party data transfers, Stanbic Bank's policy allows sharing personal data with advertisers but does not explicitly list the third parties involved. In contrast, Pride Microfinance's policy does not specify whether it allows sharing with advertisers and neither does it list third-party entities.

In terms of informed consent, Stanbic Bank's privacy policy generally lists the personal data collected and provides clear explanations for data collection. It mentions the right to access and correct personal data without conditions and grants the right to restrict or object to data processing or withdraw consent, though permanent data deletion is only allowed under certain conditions. Pride Microfinance's policy, on the other hand, doesn't specify the personal data collected and only mentions data storage duration as required by law. While they do mention providing a description of personal information and allowing objections to certain types of data processing, Pride Microfinance does not provide a clear option for permanent data deletion.

Stanbic Bank demonstrates robust data security practices with a privacy policy score of 67.5, a security score of 5, and Privacy Badger blocking 7 potential trackers. It also receives an A grade for security headers. In contrast, Pride Microfinance's privacy policy scores lower, with a privacy policy score of 34.6 and 5 potential trackers blocked by Privacy Badger. It receives an F grade for security headers.

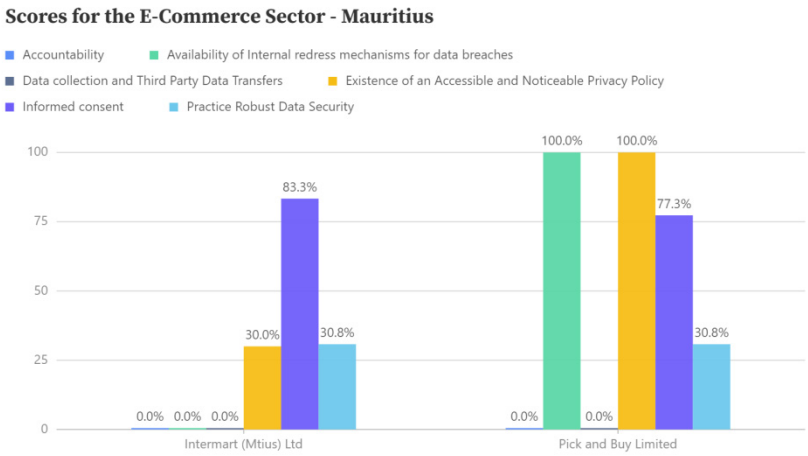
In the accountability aspect, neither Stanbic Bank nor Pride Microfinance has published a transparency report since 2022. Overall, Stanbic Bank exhibits stronger data privacy practices and robust data security, while Pride Microfinance lags behind in data policy comprehensiveness and security measures.

3.4.1.3 Country findings for e-commerce sector

In the e-commerce sector, the report focused on the following companies namely: Pick and Buy Limited and Intermart (Mtius) Ltd from Mauritius, Ubuy Zimbabwe and Shumba Africa from Zimbabwe, Jiji and Jumia Kenya from Kenya and, Jiji and Jumia Uganda from Uganda.

i. Pick and Buy Limited and Intermart (Mtius) Ltd in Mauritius

In this sector, Pick and Buy Ltd registered the highest score -100% in for both the availability of internal redress mechanisms for data breaches and existence of an accessible and noticeable privacy policy indicators. Closely followed by 83.3% and 77.3% scored respectively by Intermart (Mtius) Ltd and Pick & Buy Ltd for the informed consent indicator. While, very low scores were registered for accountability, data collection and third party transfers and availability of internal redress mechanisms for data breaches. The figure below gives more insights into the performance and a further discussion on the two companies;



Pick and Buy has a satisfactory Data Privacy policy. The data Privacy Policy link is clearly noticeable on the website. The content is written in a clear and easy to read language. It elaborates sufficiently the data privacy practices as recommended in the Data Protection Act 2017. The Data Privacy policy (about 4500 thousand words) gives the users a comprehensive set of information that they need to know about their own data before they can engage themselves for services with Pick and Buy. The company defines appropriately in the Privacy policy about the data that it collects directly and indirectly as well. It lists all the types of data that are collected from the user. The Policy mentions the nature and category of personal data that are collected and that data may be shared to Pick and Buy partners and service providers.

It also mentions that necessary measures are put in place to secure data at all times. The security services may be provided by its partner and third parties and strict access to data is provided whenever needed. Equally, a Data Protection Officer was appointed who is responsible for overseeing matters relating to this privacy notice and compliance with the law generally. For any issue related to Data privacy, users should contact the DPO.

Whereas the privacy policy general contact details are available on the website, it does not include specific contact details for Data Privacy related matters. It does not specify the duration of keeping personal data.

The privacy policy mentions about the users' rights toward the collected data. User may request to update, correct, or erase data. However, since the Organisation is bound by regulations, it is not possible in all cases to erase his/her personal data. The user may request to restrict the use of his/her personal data. While the privacy policy clearly mentions about the consent taken while collecting data, it does not mention about consent withdrawal. There is no transparency report and currently it is not a requirement as per the Data Protect Act of Mauritius.

Intermart, has a legal information link on the extreme footer of its website rather than a Data Privacy policy, where information about personal data is available. It has also another section called "Personal Data and Cookies". However, there is no information about personal data in that section. Therefore, it can be relatively difficult for a regular user to figure out infor-

mation related to data privacy on the website. The legal page mentions that the site is the institutional website of the group and not a commercial website. The legal page elaborates satisfactorily the personal data policies of the organisation. This page displays full contact details of the organisation including physical address, email address and telephone number, mentions the purpose of personal data collection, which is mostly for better interaction with its users, and mentions the kind of personal data that the organisation collects, mostly through subscription which includes data appearing on the subscription form such as your last name, first name, date of birth, postal, telephone and electronic contact details.

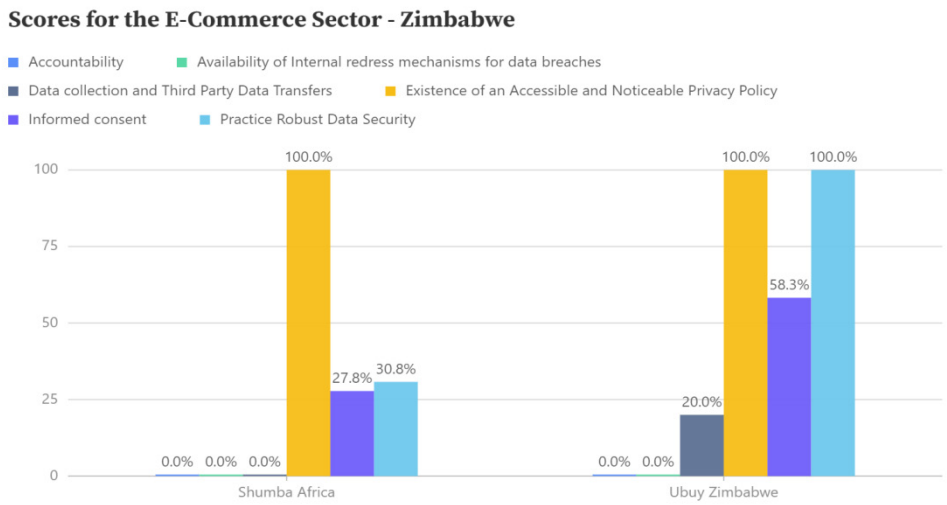
Data storage duration is specifically mentioned and are as per the local regulations. As per the legal page, users have the right to access his/her personal data. The user has the right to access, rectification, erasure, unless they are necessary for the Organisation to comply with its obligations. The legal page mentions that the user may request to restrict the use of his/her personal data.

The legal pages specify the recipients with which personal data is shared. They are basically the communication services, IT services and information systems security. They may also share the data to IT service providers, service providers operating in the advertising sector. However, the names and identity of the contractors and service providers are not mentioned. By default, the organisation also has the obligation to share the data with regulators and authorities as per legal requirements. The legal page mentions that appropriate technical, physical and organizational measures are in place to preserve the security and confidentiality of personal data and prevent them from being distorted, damaged or accessed by unauthorized third parties. It does not mention the specific technology used to secure data.

While the legal page did not mention data categorization, it specified the type of data collected and mentioned that the nature and category of personal data to be collected as well as attainment of data upon User's consent. However, it does not specify that the user can eventually withdraw consent. The legal page mentions. There is no transparency report and currently it is not a requirement as per the Data Protect Act of Mauritius. Though the legal page of Intermart does not really indicate remedy mechanisms, it however, describes how the user should proceed if he/she wants to exercise his/her rights. A written and signed request should be sent to the provided email address of the company.

j. Ubuy Zimbabwe and Shumba Africa in Zimbabwe

Both Ubuy and Shumba registered a high score of 100% for the existence of an accessible and noticeable privacy policy and practice robust data security indicators. While, the lowest scores were registered under accountability, availability of redress mechanisms for data breaches and data collection and third party data transfers. Find below a figure showing the performance against the six indicators and a further detailed discussion on the two companies;



Shumba Africa is an e-commerce platform with a published privacy policy on its website, although it takes some searching to find at the bottom of the terms and conditions page. The policy provides only a general overview of the types of user data collected such as orders, communications, posts, demographic information and browsing data. The purposes of use outlined such as processing transactions, analytics, feedback and marketing are also described only broadly.

Shumba's policy however, lacks specifics and exhaustive inventories of all data points gathered. It does not mention any data retention schedules or deletion protocols for user information. Whereas it is stated that data may be shared with third party service providers, it does not name specific entities or apps integrated within the platform. The policy also declares the platform may share personal data with authorities if "required by law" but without transparency into what requests are received. It does not discuss facilitating user rights to access, modify or delete their information either.

With 4 trackers identified on the site, Shumba exhibits some cybersecurity weaknesses though not major risks. More concerning is the lack of visibility into security practices and safeguards in the privacy policy itself.

Overall, while Shumba does have a published policy, it lacks sufficient granular details on data handling, retention, sharing, rights and protections. The gaps in specificity undermine meaningful user consent and control over data collection. As an e-commerce operator, more proactive transparency commitments are needed from Shumba to comply with Zimbabwe's Data Protection Act.

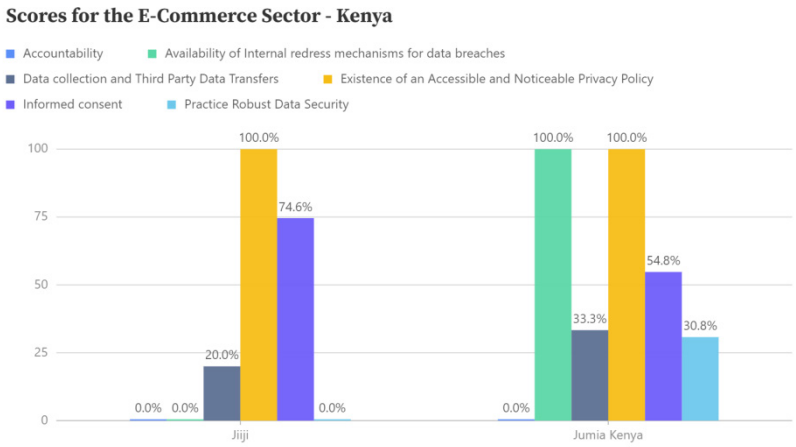
Ubuy Zimbabwe equally has a published privacy policy on its website, despite it taking some searching to find it located in the tiny footer area of the contact page. The policy is reasonably readable in plain language, though lacks specifics in certain areas. In terms of personal data collected, it uses vague phrasing like “such as” instead of exhaustively listing all data types.

Purposes of data use are explained generally such as for orders, analytics and communications. The policy states data will be retained as long as the user account is active and up to 3 years after, earning partial points for specifying a retention period. Contact information including corporate address, email and phone are provided in full.

The policy however, does not mention user rights to access, restrict processing, or delete data. It states data may be shared with service providers but does not comprehensively disclose all third parties. With 6 trackers identified by Privacy Badger, the site has moderate security gaps. No transparency report is published. Overall, Ubuy's privacy policy provides partial transparency but lacks details on key aspects like user rights, retention, and third-party sharing. Though, the policy is in existence on its site, it is inconspicuously located. Also, the policy lacks specifics in areas like data retention, user rights, and third-party sharing. User rights to access, restrict processing, or delete data are not mentioned. It provides a vague summary of personal data collected rather than an exhaustive list. Purposes of data use are outlined generally. The policy states data may be shared with service providers without detailing all third parties. With 6 trackers identified on the site, Ubuy has some security gaps and there is no transparency report published.

k. Jiji and Jumia Kenya in Kenya

Both Jiji and Jumia in Kenya registered a high score-100% for the existence of an accessible and noticeable privacy policy and availability of internal redress mechanisms for data breaches indicators. Closely followed by 74.6% and 54.8% scored respectively for the informed consent indicator. Very low scores were registered for the availability of internal redress mechanisms for data breaches, accountability and practice robust data security indicators. Overall, Jumia exhibited fair scores registered in 5 indicators out of the six. Find below a figure showing details of the performance and further discussion on the two companies;



Kenyan e-commerce platform Jiji outlines its personal data handling in a privacy policy encompassing categories like identity, contact, financial, transactional, device and usage data. The policy lists purposes like orders, customization, communications and marketing. Rights to access, correction, restriction and erasure are detailed without conditions, showing strong commitment to user control.

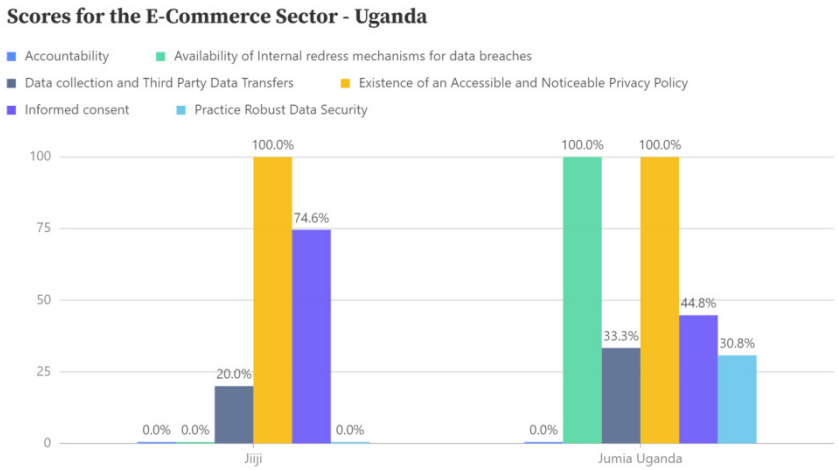
However, data retention duration is not specified, calling for improvement and data security practices and safeguards are not elaborated in the policy. Third party sharing is stated as occurring with service providers, but partners are not exhaustively listed. Neither was there evident transparency reporting. While Jiji's policy provides reasonably clear transparency, public disclosure of its retention schedules, detailed security measures and comprehensive third-party sharing arrangements would enhance alignment with accountability expectations under Kenyan data protection law.

Jumia privacy policy outlines broad categories of customer data used to provide its e-commerce services and marketing. But the policy lacks exhaustive specifics on exact data types gathered. Similarly, while purposes like orders, personalization and advertising are listed, detailed explanations of data usages are absent. No retention schedule or deletion protocol is published. The policy offers vague references to user rights, stating people can request data erasure without explaining detailed access procedures. Data security practices are summarized without elaborating technologies or safeguards implemented. Third party sharing is only mentioned broadly as obeying legal requirements and supporting services. With 5 third-party trackers found on Jumia's site, its security stance requires strengthening.

Given Jumia's extensive digital commerce operations, concrete transparency into granular data points collected, retention durations tailored for each dataset, and comprehensive profiling of sharing with platforms and advertisers is highly recommended. While Jumia has a baseline policy, its brevity contrasts with the user data processed from activities like browsing, purchases and social logins.

I. Jiji and Jumia Uganda in Uganda

Both Jiji and Jumia in Uganda registered a high score-100% for the existence of an accessible and noticeable privacy policy and availability of internal redress mechanisms for data breaches indicators. Closely followed by 74.6% and 44.8% scored respectively for the informed consent indicator. Very low scores were registered for the availability of internal redress mechanisms for data breaches, accountability and practice robust data security indicators. Overall, Jumia exhibited fair scores registered in 5 indicators out of the six. Find below a figure showing more details of the performance and further discussion on the two companies;



Jiji and Jumia in Uganda both maintain accessible and noticeable privacy policies. Jiji's policy permits the sharing of personal data with advertisers and provides a comprehensive list of third-party entities. In contrast, Jumia Uganda's policy does not specify whether it allows data sharing with advertisers and lacks a detailed list of third-party entities.

In terms of informed consent, Jiji's privacy policy generally lists the personal data collected, provides clear explanations for data collection, and grants rights to access, correct, restrict or object to data processing, withdraw consent, and permanently delete personal data using an automated mechanism. However, it does not mention data storage duration or include contact information. On the other hand, Jumia Uganda's policy generally lists the personal data collected, clarifies the purposes, and mentions the right to access and correct personal data, though these rights come with certain conditions. It also provides the right to restrict or object to data processing and withdraw consent, but there is no clear process for permanent data deletion.

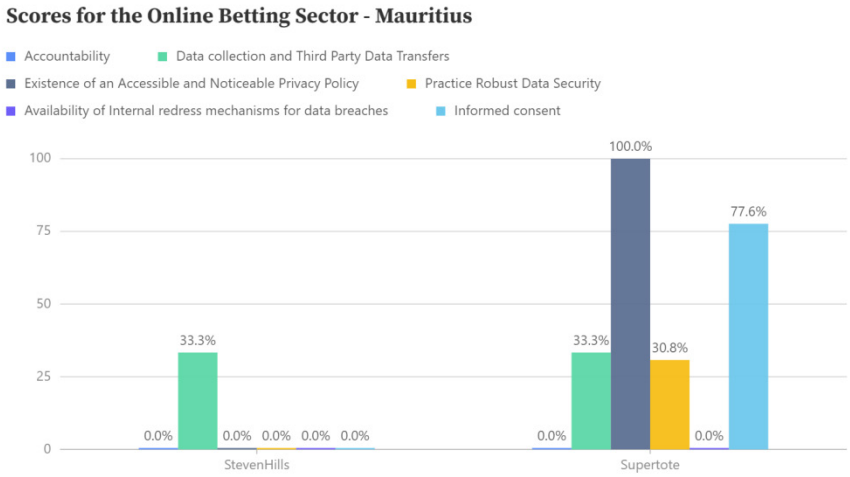
Regarding data security practices, Jiji's privacy policy registered a very low score, and Privacy Badger blocking 4 potential trackers. It receives a security headers grade of B. Jumia Uganda's privacy policy registered a score- 30.8%, and Privacy Badger blocking 2 potential trackers. It receives a security headers grade of C. In terms of accountability, neither Jiji nor Jumia Uganda has published a transparency report since 2022. In summary, both companies maintain noticeable privacy policies with variations in data collection, informed consent, and data security practices. Jiji had a relatively low score in data security but with a good score for informed consent and comprehensive data subject rights, while Jumia lagged in these area, it was clearer regarding data storage and contact information.

3.4.1.4 Country findings for Online Betting Sector

In the e-commerce sector, the report focused on the following companies namely: Supertote and Steven Hills from Mauritius, Bezbets and Africabet from Zimbabwe, Betika and Mcheza from Kenya and, Fortebet and 1XBet from Uganda.

m. Supertote and Steven Hills in Mauritius

Supertote registered the highest score-100% for the existence of an accessible and noticeable privacy policy, closely followed by 77.6% scored for the informed consent indicator. While, StevenHills did not have an existing privacy policy and generally registered very low scores for 5 indicators out of the six; with the highest score as 33.3%, that was equally registered by Supertote for the data collection and third party data transfers indicator. Below, is a figure showing details of the performance and further discussion on the two companies;



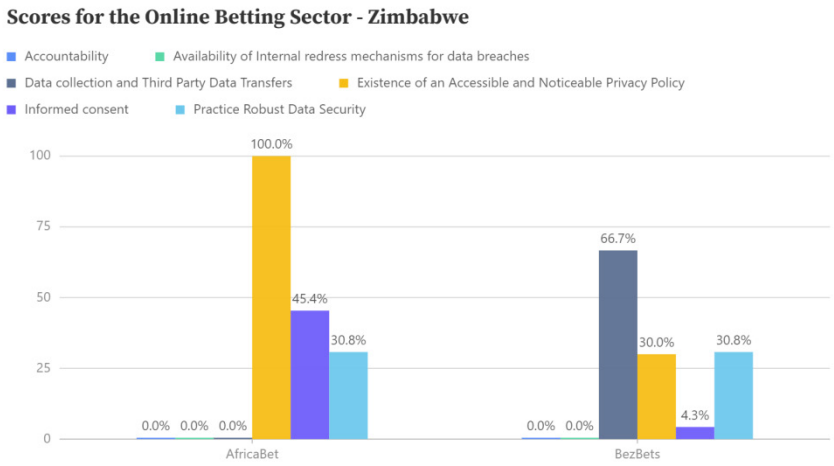
Supertote had a satisfactory Privacy Policy. The Policy was prominently featured on the website's landing page, and the content was composed in a clear and easily comprehensible language. The Policy comprised of more than 1000 words and offers users a comprehensive source of information crucial for them to comprehend how their personal data is managed before they can access the services provided by Supertote. The Privacy Notice clearly stated the purpose of data collection, specified both the types of data collected and the purposes for which they are collected, mentioned the data retention periods and the company's contact details, and address, but was missing a contact phone number. It contained information about data subjects' ability to access their personal data, outlined data subjects' rights to rectify their personal information and to request the deletion or erasure of their data, provided details on data subjects' rights to restrict or object to the processing of their data. It stated also that data subjects had the right to withdraw their consent at any time, and provided details of the nature and category of personal data to be collected.

However, it did not mention in detail the third-party entities with whom personal data is shared to provide the service nor did it mention the data security measures to safeguard personal data. A transparency report was not currently available, even though it is not mandated by the Data Protection Act of Mauritius. It also lacked information regarding internal redress mechanisms for data breaches.

On the hand, SteveHills does not have any privacy policy on its website. As such, it was difficult to assess it against any of the indicators except for the data collection and third party data transfers indicator where it registered a score of 33.3%. Though it was the highest score, it was still far below, as some elements were not fulfilled. To this end, a data privacy policy should be put in place so that anybody registering or applying for a service through the website are aware about their personal data, the purpose of collection, how it is kept and the duration for keeping it. The policy should as well highlight how, and which data is shared with other organisations. Equally, the company should assure users about the security measures being taken to keep data secure.

n. Africabet and Bezbets from Zimbabwe

The highest score was 100% registered for the existence of an accessible and noticeable privacy policy by Africabet. Closely followed by 66.7% registered for data collection and third party data transfers indicator by Bezbets. Both companies registered 30.8% scored for the practice robust data security indicator. While, the lowest scores were registered for the accountability, availability of internal redress mechanisms for data breaches as well as data collection and third party data transfers indicators. Find below a figure showing the performance and a detailed discussion on the two companies;



Africabet had a privacy policy published on its Zimbabwean website. However, the policy utilized ambiguous and vague language when outlining the types of user data collected. It stated that the platform gathers undefined "personal information", "transaction details", "data about transactions", "products you access" and "other data" without concrete specificity of actual data points. Such opacity violates requirements for transparency around exact personal data collected.

The policy was also overly broad when describing "general business purposes" as the rationale for data gathering rather than clearly defined purposes for specific usage justified on lawful grounds. No data retention schedules are specified at all to indicate duration of storage. Nor were user rights to access, modify, restrict processing or delete their information discussed. Third party sharing was only mentioned in a blanket manner as obeying "applicable laws" without naming partners.

With 7 trackers identified on its site, Africabet lacks stellar cybersecurity measures though risks seem lower than other platforms examined. But the larger concern was the policy itself skirting key transparency requirements through vague explanations that did not foster meaningful user understanding or control over data practices. As a financial platform, provision of unambiguous specifics on data handling, security and sharing in its privacy policy is vital for Africabet to align with data protection standards.

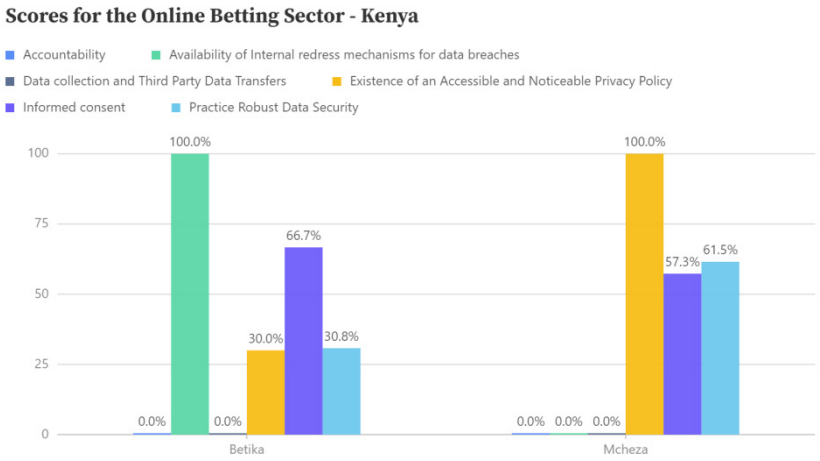
Equally, Bezbets online sports betting platform had a privacy policy published on its Zimbabwean website. The policy outlined in general terms the various categories of user data collected such as identity, contact, demographic, financial transactional information, technical device data and tracking data from site cookies. It states this data is used for purposes like verifying eligibility, fraud prevention, profiling, analytics and marketing.

However, the policy lacks specifics around exhaustive data inventories, retention schedules tailored for each data type, or deletion protocols. User rights to access, correct or erase their data are not mentioned. Third party sharing is briefly addressed but not in comprehensive detail. With 8 trackers identified on Bezbets' site, it exhibits noticeable security gaps though risks are not as high as some other betting platforms. More concerning is the lack of transparency about security practices and safeguards within the privacy policy itself.

As an online business handling significant financial transactions and user data, greater accountability is required from Bezbets under Zimbabwe's data protection law. Its policy requires more granular details on exact data points collected, storage periods, nuanced user rights processes, detailed third party affiliates, proactive reporting and stringent cybersecurity measures. While Bezbets does have a baseline posted policy, it needs considerable expansion to qualify as a transparent disclosure empowering informed user consent and control.

o. Betika and Mcheza in Kenya

The highest score was 100% registered for the availability of internal redress mechanisms for data breaches and existence of an accessible and noticeable privacy policy indicators by Betika and Mcheza respectively. Closely followed by 66.7% scored for the informed consent indicator and 61.5% scored for the practice robust data security indicator by Betika and Mcheza respectively. On the hand, very low scores were registered for accountability and data collection and third party transfers indicators. Find below a figure showing more on the performance and further discussion on the two companies;



Betika an online sports betting platform in Kenya outlined categories of account holder personal data processed in its privacy policy, including profile details, usage logs, contacts, financial information and device data. Purposes listed ranged from verifying eligibility to marketing and analytics. Its baseline policy represents a positive step in the right direction. However, the policy lacked comprehensive retention schedules for different datasets. The policy stated that users can access their data but makes no reference to correcting or deleting records on request.

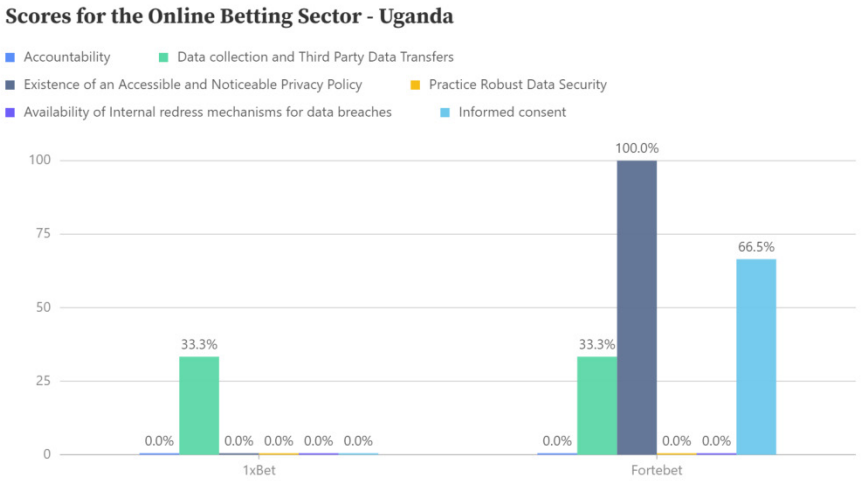
The policy summarized security safeguards without detailing technologies used or organizational controls. Third party sharing is addressed vaguely as obeying lawful requests rather than listing specific recipients and no evidence of transparency reporting. Given the volumes of user identity, transactional and interactive data generated across its platforms, Betika would benefit from enhancing transparency into granular retention policies, security specifics, proactive reporting and stronger user rights facilitation to align with data protection expectations.

Equally, Mcheza a popular online betting site, published a privacy policy that provided reasonable visibility into its personal data handling practices. The policy lists general categories of user information like profile details, usage logs, contacts and financial data used for purposes including verifying eligibility, marketing and analytics. However, the policy offers limited specifics regarding data retention schedules for different types of account-related information. References to security safeguards are summarized without elaborating technologies or controls used. User rights to access and correct data are facilitated, but deletion requests face restrictions. Third party sharing partners are not exhaustively detailed either.

Given Mcheza's handling of sensitive user identity, financial and online activity data, the policy warrants more concrete disclosure around retention durations, security systems, and sharing partnerships based on lawful requests. Proactive transparency reports would also go a long way in aiding accountability.

p. Fortebet and1XBet in Uganda

The highest score – 100% was registered for the existence of an accessible and noticeable privacy policy indicator by Fortebet. Following closely was 66.5% registered by Fortebet for the informed consent indicator. While both companies registered the lowest scores for the accountability, practice robust data security and availability of internal mechanisms for data breaches indicators. More information on the performance is shown in the figure and further discussion on the two companies below;

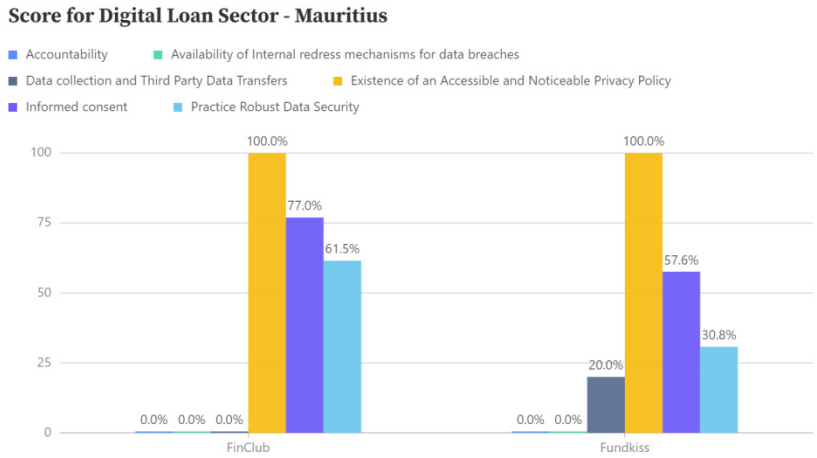


3.4.1.5 Country findings for Digital Loan Services Sector

For the digital loan services sector, the report focused on the following companies namely: FinClub and Fundkiss from Mauritius, Echocash and Zibuko from Zimbabwe, Branch and Tala from Kenya and, Dove Cash and Mangu Cash from Uganda.

q. FinClub and Fundkiss in Mauritius

Both companies registered the highest score 100% for the existence of an accessible and noticeable privacy policy indicator. While, both companies registered very low scores for the accountability and availability of internal redress mechanisms for data breaches indicators. Find below a figure showing the performance and further discussion on the two companies;



FinClub has a well elaborated Data Protection and Privacy policy on its website (over 4500 words), explaining all the measures they have in place to keep the data subject's data safe. The policy is clearly noticeable in the footer of all pages of the website and the various content of the policy was clearly segregated. The company address and phone number was available on the website including stating clearly the purpose and type of data that is collected. The company has the regulatory obligation to keep data for seven years after service has ceased for a client and equally mentioned in the policy.

The policy mentioned that; data is processed based on consent and user can withdraw consent at any time and, the nature and category of personal data to be collected as well as mentioned that restricted amount of data was shared with third parties. It listed down the type of entity with which personal data is shared for the purpose of offering the service. Also, the policy satisfactorily elaborated all the measures taken for information security. The policy mentioned that the data subject had the right to request to update and correct any out-of-date or inaccurate personal data. The data subject may also file any complaint through a provided email address.

Additionally, users may request; to access personal data and access to update, correct, or erase data, and request to restrict use of personal data in the event the data is no longer relevant for the purpose it was collected, or consent has been withdrawn or if unlawfully used.

However, since the organisation is bound by regulations, it is not possible in all cases for a user to erase his/her personal data. There is also no evidence on transparency reporting despite it not being a requirement as per the Data Protection Act 2017 of Mauritius.

FunKiss, equally had a satisfactory Data Privacy policy. The Privacy Policy link is clearly noticeable on the website landing page. The content was written in a clear and easy to read language. It elaborated sufficiently the data privacy practices as recommended in the Data Protection Act 2017. The Data Privacy policy (over 3000 thousand words) gives the users a comprehensive set of information that they need to know about their own data before they can engage for services. The company address and phone number is available on the website and the policy

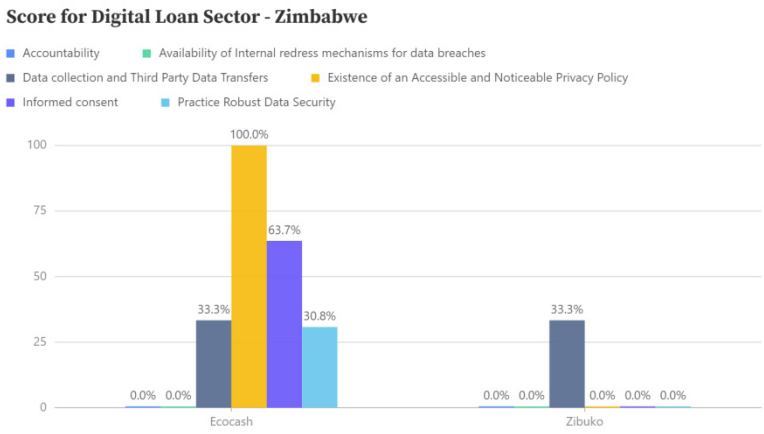
clearly stated the purpose of data collection. It described the various type of data collected and the reasons why they are collected. The policy mentioned that data will be maintained even after service is terminated because of regulatory purposes. Data Processors as per the Data Protection Act, are required to keep data for five to seven years after the service is terminated, depending on the industry.

The policy mentioned that the subject has the right to request to update and correct any out-of-date or inaccurate personal data. The subject may also file any complaint through a provided email address. It further mentioned that the user may at any time request to access his/her personal data, for which a fee may apply depending on the case. It also mentioned that: the user may request to restrict the use of his/her personal data; the nature and category of personal data to be collected; data is shared with authorities and their business partners for the process of delivering the service, example bank; restricted amount of data is shared with third parties; and that SSL certificate was used to prevent the loss, misuse, and alteration of the information. Users may request to update, correct, or erase data.

However, since the organisation is bound by regulations, it is not possible in all cases to erase his/her personal data. The policy did not specifically mention that the user has the right to withdraw consent. But at the initial stage of data collection, the user must consent to the use of his/her personal data. The user may wish to terminate his/her service, but the service provider will still have to keep the data for a particular period for regulatory purposes. Like FinClub, there was no evidence on transparency reporting.

r. Ecocash and Zibuko in Zimbabwe

Ecocash registered the highest score 100% for the existence of an accessible and noticeable privacy policy indicator and following closely was 63.7% scored for the informed consent indicator. While, both companies scored 33.3% for the data collection and third party data transfers indicator, they also registered very low scores for the accountability and availability of internal redress mechanisms for data breaches. More information on the performance is shown in the figure and the discussion below;



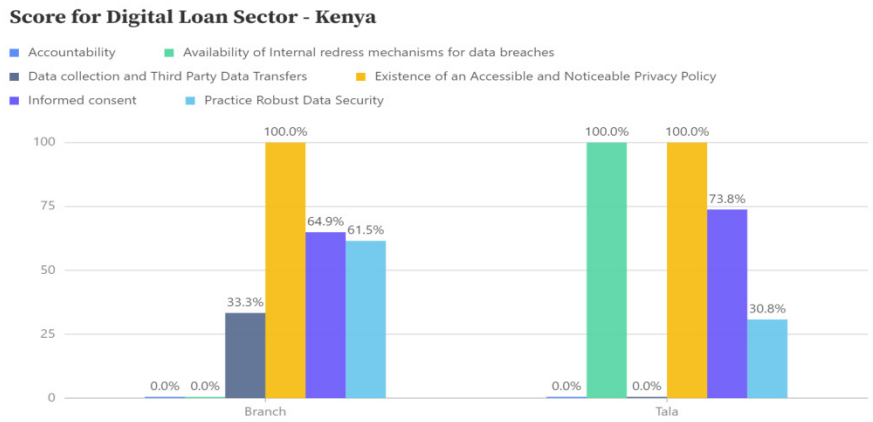
Ecocash has a privacy policy though not specific to its digital loans services. It relies on general terms and conditions for mobile money services that do not provide transparency into loan data practices. These disclosures do not offer details on personal data collected, purposes of use, retention periods, user rights, or third party sharing in relation to the loans services. This likely indicated reliance on blanket contractual consent without robust specifics on handling of loan applicant data. No information is provided on data security protections or trackers associated with the loans platform. With no transparency report, Ecocash shows significant gaps in its policy and practices around its digital loan offerings. There is no evidence suggesting details on loan applicant data collected, purposes of use, retention, user rights, or third-party sharing. This likely indicated dependence on blanket consent without robust loan data specifics.

The digital lending platform Zibuko offers quick personal loans through its mobile application. It has a very barebones and limited privacy policy published on its website that lacks substantive details on its data practices. The policy contains no information whatsoever on the types of personal data and sensitive information collected from loan applicants. It is completely ambiguous on the purposes for which applicant data is processed. No data retention schedule or deletion protocols are outlined. User rights to access, modify, delete or obtain copies of their information are not addressed in the sparse policy. There are no details provided regarding what cybersecurity or organizational security measures are applied to safeguard applicant data. Neither were third party sharing practices mentioned. With only 2 trackers identified on its site, Zibuko appears to have decent baseline security controls, but this is not clearly conveyed in the policy.

Overall, Zibuko's minimalistic privacy disclosure fails to provide meaningful transparency around its handling of sensitive user data central to its lending business model. As a digital financial service drawing increasingly user data, a detailed policy outlining exhaustive data points gathered, purposes of use, retention limits, robust security protocols, rights facilitation and sharing practices is imperative for Zibuko to align with Zimbabwe's data protection law. The existing sparse policy undermines accountability around applicant data and requires major expansion.

5. Branch and Tala in Kenya

Both companies registered the highest score 100% for the existence of an accessible and noticeable privacy policy indicator with Tala equally scoring the highest for the availability of internal redress mechanisms for data breaches indicator. Following closely was the performance for the informed consent indicator were Tala and Branch scored 73.8% and 64.9% respectively. While, a very low score was observed for both on the accountability indicator. The figure below shows more on the performance and further discussion on the two companies;



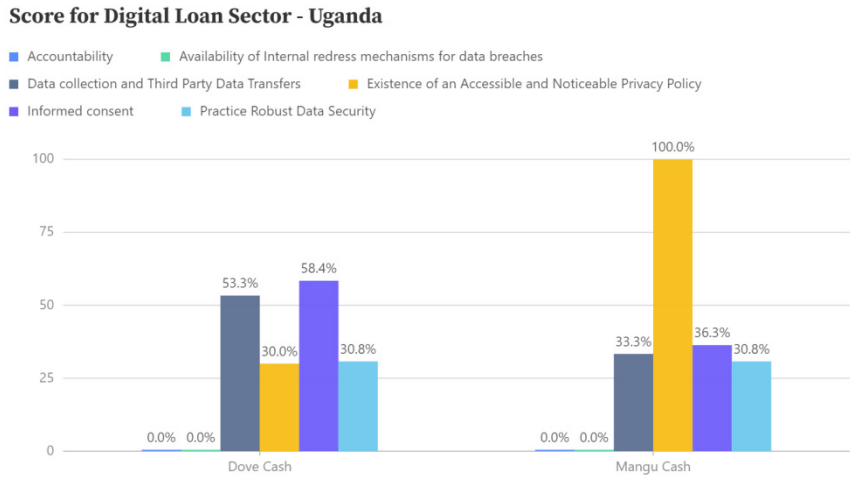
Branch's privacy policy offered reasonably clear transparency into its digital lending data practices. Personal data collected from applicants such as identification details, contacts, financial information, device data and photographs are listed comprehensively. Purposes of use like credit assessment, identity verification and fraud prevention were also outlined. Recent transparency enhancements were announced, like publication of data protection impact assessments.

The policy however, only stated that it retained data for 'as long as necessary' without publishing its precise retention schedules. This prevents accountability regarding data destruction after loan closure. Applicant rights to access and correct data are articulated without conditions, but deletion requests required contacting Branch's Data Protection Officer which creates a barrier. It does not outline data security measures and practices in any detail. Third party disclosures are mentioned but partners were not exhaustively listed. Overall, Branch communicates its lending data practices fairly clearly, but lacks specifics in certain areas like retention and security.

Tala equally, had a privacy policy that provided transparency into its personal data handling practices for digital lending services. Its policy listed in detail the categories of borrower data collected, including identity, contact, financial, device, network, usage and communications data. Purposes were also clearly outlined covering needs like verifying identity, determining creditworthiness and managing lending operations. A precise 10-year retention period is specified in the policy tied to anti-money laundering requirements. This contrasts with vague statements of "as long as necessary" by other entities. User rights to access, correction and erasure were explicitly detailed, highlighting Tala's commitment to data ownership. Security practices were only summarized at a high level, representing an area for improvement. Third party sharing was addressed, though partners other than credit agencies were not exhaustively listed. As a digital lender capturing intrusive information from borrowers' devices and networks, comprehensive articulation of sharing is important for consent. Tala's transparency on key aspects of its lending data practices is ahead of the other companies assessed and sets a positive example.

t. Dove Cash and Mangu Cash in Uganda

The highest score 100% was registered by Mangu Cash for the existence of an accessible and noticeable privacy policy indictor. This was closely followed by the informed consent indicator where Dove Cash and Mangu Cash scored 58.4% and 36.3% respectively. On the other hand, both companies were observed with very low scores for the accountability and availability of internal redress mechanisms for data breaches indicators. Find below a figure showing more on the performance and further discussion on the two companies.



Dove Cash and Mangu Cash, exhibited differences in their data privacy practices. Both companies had privacy policies, but Dove Cash's policy was not noticeable, while Mangu Cash's policy was observed as noticeable.

In regard to data collection and third-party data transfers, Dove Cash's policy did not specify all third-party entities but prohibited sharing personal data with advertisers. In contrast, Mangu Cash's policy allowed the sharing of personal data with advertisers and did not explicitly list the third parties involved. In terms of informed consent, Dove Cash's policy exhaustively listed the personal data collected, explained the purpose of data collection, and grants data subject rights to access, correct, restrict, object to data processing, withdraw consent, and request permanent data deletion. However, it did not mention data storage duration or provide company contact information.

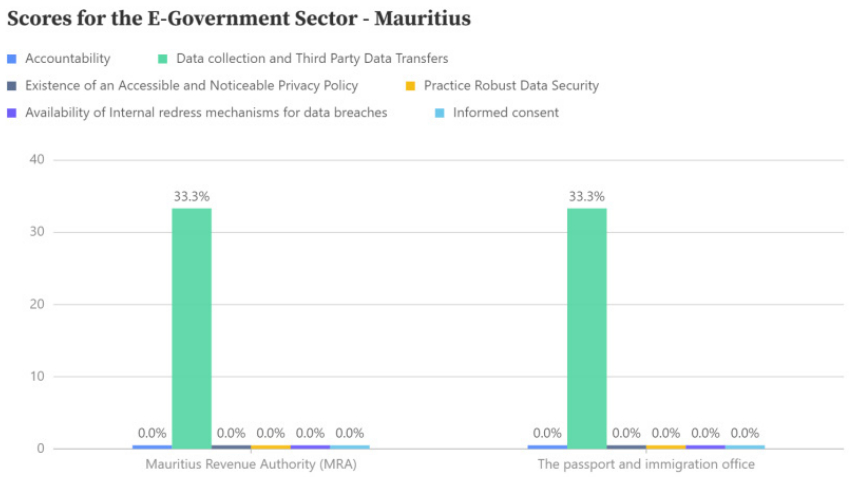
On the other hand, Mangu Cash's privacy policy equally listed the personal data collected and clarified the purpose but mentioned data storage duration only as required by law. It provides data subject rights in relation to access, correction, restricting or objecting to data processing, and withdrawing consent, though permanent data deletion was not clearly outlined. In terms of accountability, neither Dove Cash nor Mangu Cash had published a transparency report since 2022.

3.4.1.6 Country findings for e-Government Sector

The report regarding the e-Government sector, focused on the following companies namely: Mauritius Revenue Authority and Passport and Immigration Office from Mauritius, E visa-Department and Zimbabwe Revenue Authority from Zimbabwe, E-citizen and Huduma from Kenya and, Immigration Uganda and National identification and Registration Authority from Uganda.

u. Mauritius Revenue Authority (MRA) and Passport & Immigration Office in Mauritius

Very low scores were observed across all the six indicators in respect of both entities with the highest score 33.3% registered for the indicator on data collection and third party data transfers. Below is a figure showing the performance and further discussion on the two entities.



Unlike the Passport and Immigration Office that did not have any privacy policy on its website, MRA on the other hand, had a very brief Privacy policy on its website (around 410 Words). It is noticeable on the website with simple and easy understandable language used to describe the privacy policy. Whereas the entity contact details were available on the website, but this was not the case in the privacy policy.

The policy briefly mentioned the purpose of data collection which was for the record and for better service and that the data storage time is as per the authorities. It mentioned the nature and category of personal data collected and, that data may be shared to statutory and regulatory bodies and law enforcement authorities as applicable. It elaborated on the security measures to protect data separately in an Information Security Policy document which was available on the website and clearly visible in the footer of the website.

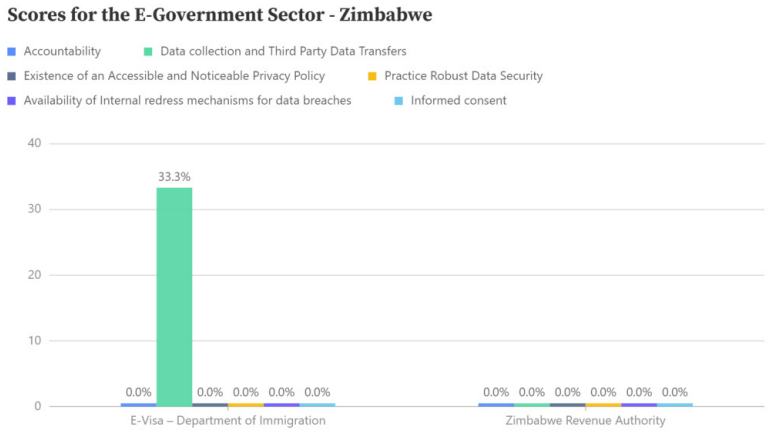
The policy lacked description about access to personal data. It simply mentioned that the user can contact MRA via the communication option that is available on MRA website. There was no information about data subjects' rights in relation to updating, correcting, deletion, or erasing personal data nor the right to restrict or object to data processing. There was no evidence on transparency reporting nor formal procedure for redress mechanisms in place. Instead MRA requested that any inquiries, questions, and complaints related to the privacy policy should be made via the communication options on the website that is, email and phone.

To this end, the Passport and Immigration Office should be put in place a privacy policy so that anybody registering or applying for a service through the website are aware about their personal data, the purpose of collection, how it is kept and the duration of storage. It should also highlight how and which data is shared with other organisations. Additionally, the organisation should assure users about the security measures being taken to keep data secure.

Equally, MRA in addition to its progressiveness; needs to have explicit contact details in the data privacy policy for users to easily reach out on privacy related matters; should elaborate on the purpose of collecting the specific data; put the correct duration for keeping users' personal data, based on the industry it is; should be more specific about the user right to access personal data; should provide information about user's right to update, correct, delete, or erase personal data per the Data Protection Act and; should provide information about user's right to update, correct, delete, or erase personal data per the Data Protection Act.

v. E visa-Department and Zimbabwe Revenue Authority in Zimbabwe

Both entities registered very low scores across all the six indicators with a score of 33.3% by e-Visa for the data collection and third party data transfers indicator. Find below a figure showing more on the performance and further discussion on the two entities;



The E-Visa website run by the Immigration Department of Zimbabwe government did not have any privacy policy published that sets out its data practices. There was lack of transparency around the types of visa applicant personal data collected through the online system, purposes for such data gathering, data retention and destruction policies, security systems protecting applicant information, and whether data is shared with any third parties like foreign governments who issue the visas.

As a digital service handling extensive applicant details and documentation, the e-Visa website has a responsibility to be transparent around safeguarding user privacy as a public sector platform. The visa process often requires individuals to submit sensitive information like financial records, family details, travel history and biometrics that requires careful management as per data protection principles. The total absence of a posted privacy policy outlining the e-Visa system's accountability commitments and measures precluded applicants from making informed choices about their data.

While the website only showed 1 tracker, indicating strong baseline technical security, the lack of any information addressing organizational controls, access restrictions, retention schedules or oversight mechanisms raises concerns. As a government administrative system gathering citizen information, proactive transparency through a detailed, readable policy published on the e-Visa site is imperative to uphold applicant rights and data protection under law. Ensuring such awareness and accountability will also be vital for compliance with emerging international data sharing norms.

Equally the Zimbabwe Revenue Authority (ZIMRA) website did not have any privacy policy published that provided transparency into its personal data collection and processing practices. As the tax authority that handles extensive confidential financial and identification information of taxpayers, ZIMRA has a responsibility to be accountable and transparent regarding data protection. However, there are no publicly posted disclosures detailing the types of user or taxpayer data collected, the purposes for which such personal data is used, retention policies, data security provisions, or any third-party sharing arrangements.

ZIMRA's online platforms collect taxpayer IDs, bank details, income information, property records and various other sensitive personal data central for revenue administration purposes. However, citizens have no visibility into whether this data is minimized, how long it is stored after filing taxes, what cybersecurity measures protect servers, or if information is shared with any other government departments. The complete lack of a published privacy policy indicates significant deficiencies in ZIMRA's transparency and accountability around safeguarding taxpayer data.

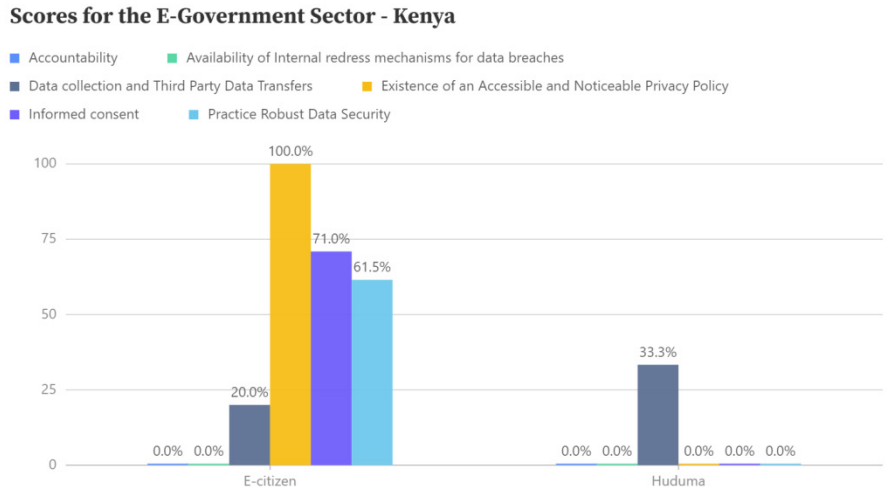
This opacity violates basic fairness principles that taxpayers should understand what data a public authority ob-

tains, stores about them and why such collection is necessary. It precludes informed consent by taxpayers regarding use of personal information. The lack of visibility into security practices also undermines taxpayer trust that systems are robust. ZIMRA's failure to articulate any retention schedule or data destruction procedure also raises risks of excessive retention. The Authority's website also exhibited 6 trackers indicating some cybersecurity gaps as well.

Overall, ZIMRA urgently needs to formulate and publish a detailed privacy policy for its various digital platforms used by taxpayers. This policy must provide specifics on data handling rather than vague legalistic disclaimers. As a public sector entity handling citizen's confidential financial data, transparency and accountability around data protection practices are fundamental for maintaining trust and compliance. The policy should be noticeable on its website rather than buried in small print. ZIMRA must outline lawful purposes for each data type, proper access controls and protections applied, limited retention periods and credible oversight processes.

w. E-citizen and Huduma in Kenya

E-citizen exhibited the highest score 100% registered for the existence of an accessible and noticeable privacy policy indicator, followed closely was the informed consent and practice robust data security indicators. Both entities registered very low scores for the accountability and availability of internal redress mechanisms for data breaches indicators. More on the performance of the two entities is contained in the figure and further discussion



E-Citizen's digital services portal, published one of the most detailed privacy policies among assessed public sector entities. The policy listed specific personal data collected from citizens using the portal, like names, IDs, photos and contact information for services like passport applications. Purposes of use like identity verification and service delivery are also clearly explained.

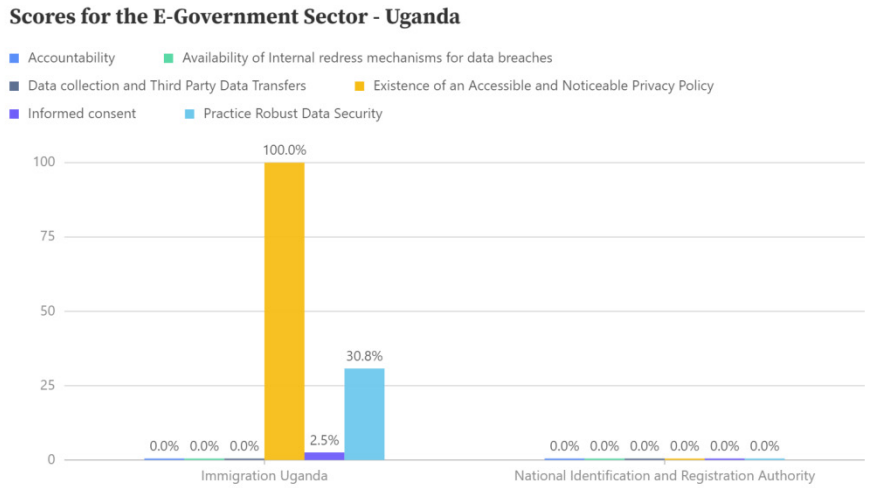
The policy however, offered limited transparency into retention duration, only stating data is kept as per legal requirements. Data security practices are outlined in a generalized manner without technical specifics. As a public sector platform gathering sensitive citizen information, detailed articulation of retention schedules and security safeguards is warranted. Whereas the policy was upfront about citizens' rights to access and correct their personal data, but deletion requests required following unspecified legal procedures, creating opacity. Notwithstanding the current gaps and challenges, e-Citizen's policy represented progressiveness with measures in the right direction among Kenyan government entities and additional commitments would boost compliance with the data protection law.

Huduma Centre for citizen services like ID, passport, marriage applications, etc completely lacked any published privacy policy detailing its personal data practices. This violates basic transparency duties expected of a public sector platform capturing extensive citizen information. Also, there were no details available on types of user data gathered, purposes for collection, data retention durations, security systems implemented, existence of data deletion procedures or mechanisms for facilitating access requests under data protection law. Certain services may require confidentiality, but a broad policy outlining Huduma's general accountability and data risk mitigation commitments is still warranted.

The absence of a privacy policy on a Government data services portal relegates citizens to blind trust rather than informed understanding of how their personal information is handled. As more state functions move online, proactive transparency regarding public agencies' data collection and processing standards is fundamental for lawful and accountable governance.

x. Immigration Uganda and National identification & Registration Authority (NIRA) in Uganda

In the context of e-Government services, there were significant variations in data privacy practices between Immigration Uganda and the National Identification and NIRA. Immigration Uganda exhibited the highest score 100% registered for the existence of an accessible and noticeable privacy policy indicator, followed closely was the practice robust data security indicator. Both entities registered very low scores for the accountability, availability of internal redress mechanisms for data breaches as well as data collection and third party data transfers indicators. More on the performance of the two entities is contained in the figure and further discussion below;



Immigration Uganda has a noticeable privacy policy in place, while NIRA does not have a privacy policy at all. Concerning data collection and third-party data transfers, the policy did not specify if it allowed sharing with advertisers nor comprehensively list third-party entities. On the other hand, NIRA's position on this aspect was unknown. Regarding informed consent, Immigration Uganda's privacy policy lacked several crucial elements. It did not list the personal data collected, provide clear reasons for data collection, specify data storage duration, or include contact information. Additionally, it did not mention data subject rights regarding access, correction, restricting or objecting to data processing, withdrawal of consent, or permanent data deletion.

In terms of data security practices, both Immigration Uganda and NIRA scored poorly. Immigration Uganda's privacy policy scored 30.8%, and Privacy Badger blocking 3 potential trackers. While, NIRA's policy scored Zero percent, and 3 potential trackers blocked by Privacy Badger. Both receive low security headers grades, with Immigration Uganda at D and NIRA at F. On accountability aspects, neither Immigration Uganda nor NIRA had published a transparency report since 2022. In summary, Immigration Uganda has a noticeable privacy policy but lacks comprehensiveness in data collection and data security practices while, NIRA lacks a privacy policy.

3.4.2 Overall Deductions on impact of findings on personal data protection and privacy rights

There were significant variations in data privacy practices. Particularly, the lack of transparency and accountability around personal data handling indicated by this analysis can be expected to negatively impact the future of privacy rights and effective data protection in all four countries. Without detailed disclosures from organizations on their practices, data subjects cannot make informed choices or assert their rights under the various Data Protection Acts.

Ambiguous or non-existent privacy policies create an environment of uncertainty for customers regarding how their information is collected, used, retained and shared. Vague explanations of "sharing where necessary" or "using for service delivery" do not provide meaningful understanding. Lack of comprehension undermines user autonomy and control over private data.

Similarly, the absence of published data retention policies or destruction procedures keeps individuals unaware of how long their information is stored after account closure. Indefinite retention can persist without transparent time limits. Lack of visibility into security practices also prevents assessing risks, leaving consumers unaware of vulnerabilities.

The deficiency of user access, correction and deletion rights facilitation further inhibits people from checking accuracy or deleting their data per the law. Without transparency into third party sharing, users cannot track where their data flows and evaluate secondary uses. Minimal accountability through public reporting of government requests obscures surveillance and hiding overreach.

Overall, low transparency indicates that organizations are collecting and processing increasing amounts of customer data in the digital economy without providing information to data subjects required by the Data Protection laws. This heightens risks of abuse and misuse since collectors face little pressure from consumers empowered with knowledge of practices. Lack of accountability breeds mistrust.

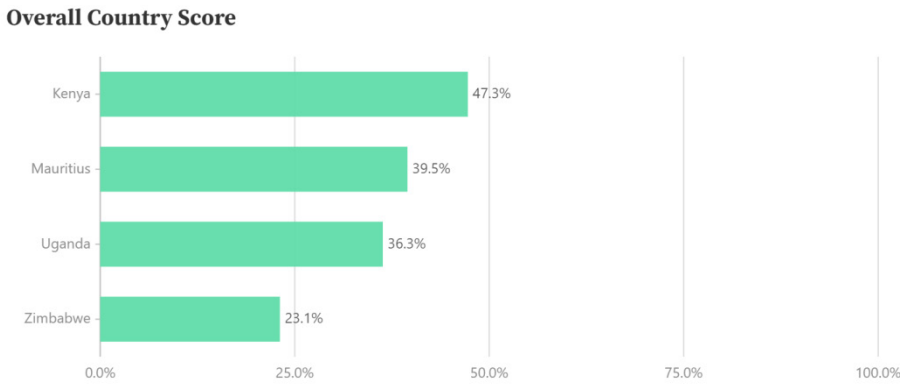
The absence of visibility undercuts enforcement, since gaps are harder for regulators to identify and address if organizations do not reveal specifics. Deficient transparency will make executing oversight functions like investigations, audits, sanctions and remediation under the Data Protection laws more difficult. Regulators cannot verify compliance if organizations do not disclose policies.

Looking ahead, the status quo enables ongoing opaque collection and processing of personal data without sufficient consent, purpose limitation, or security - undermining principles of lawful and fair data protection. It allows continuation of vague, blanket disclosures rather than evolving norms around accountability. Lacking transparency will stymie exercising of individual privacy rights under the different legislation.

Elevating openness and accountability around data practices thus remains critical for empowering user control, regulatory oversight, and responsible data governance aligned with the Act. Organizations must be motivated to move from opacity to transparency. All these impacted on personal data protection and privacy rights observed at country, sector and indicator levels and further highlighted below.

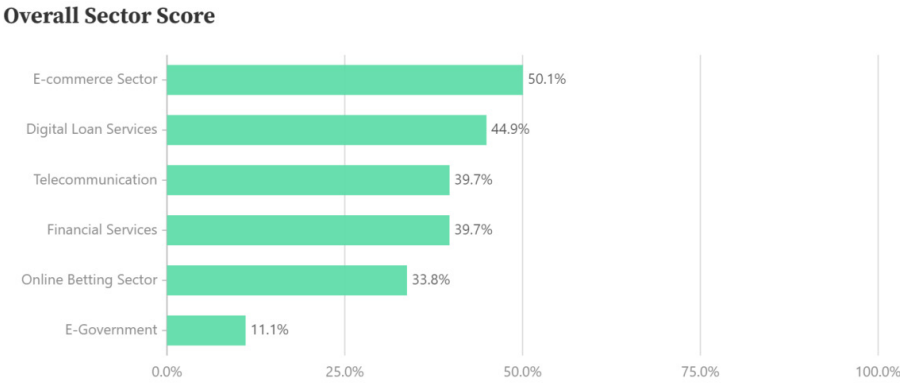
3.4.2.1 Overall analysis of Findings at Country Level

The overall index score was below 50% with 47.3% registered in respect of Kenya as the highest score. While, the lowest score was 23.1% registered by Zimbabwe. The figure below shows more on the performance of the different countries under review.



3.4.2.2 Overall analysis of Findings at Sector Level

Generally the performance at sector level across the countries did not exceed 50% with a score on 50.1% registered by e-commerce. This was closely followed by digital loan services that scored 44.9%. While, the lowest score was 11.1% registered by e-Government. Find below a figure showing more on the performance across the different sectors.

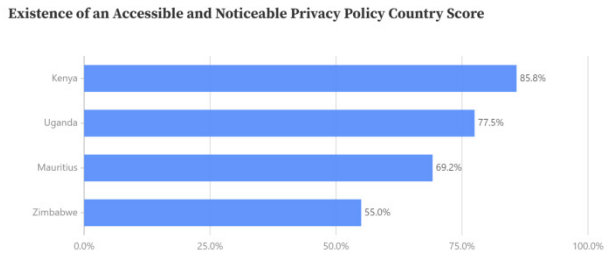


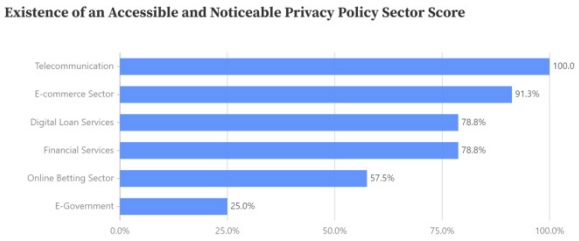
3.4.2.3 Overall analysis of Findings against Indicators at Country and Sector Levels

The performance against the six indicators was observed at both country and sector levels. At country level, Kenya was observed in the lead with the highest scores in 3 indicators out of the 6 namely: 85.8% for existence of an accessible and noticeable policy, 59.4% for informed consent and 25% for internal redress mechanisms for data breaches. While, Zimbabwe was observed with the lowest scores in 3 indicators – 55% for existence of an accessible and noticeable privacy policy, 23.4% for informed consent and 0% registered for accountability and availability of internal redress mechanisms for data breaches.

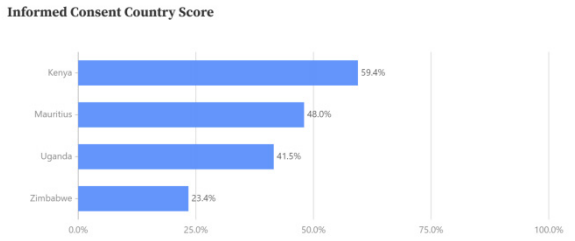
At sector level, Telecommunications was in the lead with the highest scores in two indicators out of the six – 100% for existence of an accessible and noticeable privacy policy and 12.5% for accountability. While, e-Government was observed with the lowest scores in 3 indicators – 25% for existence of an accessible and noticeable privacy policy, 11.5% for practice robust data security and 9.2% for informed consent. The Indicators are highlighted below with figures showing the performance of the different countries and sectors.

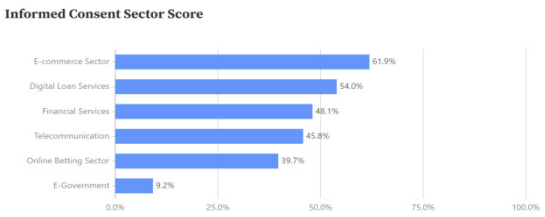
Existence of an accessible and noticeable privacy policy – the highest score at country level was 85.8% that was registered by Kenya and the lowest score was 55% registered by Zimbabwe. While, at sector level, telecommunications registered the highest score and e- Government registered the lowest score. The figures below show more detail on the performance of the different countries and sectors against the indicator;



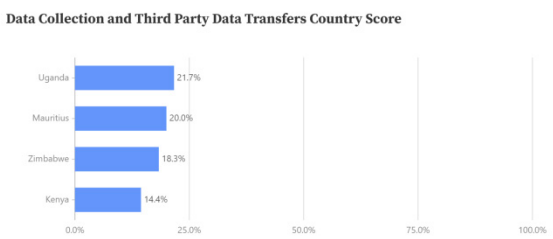


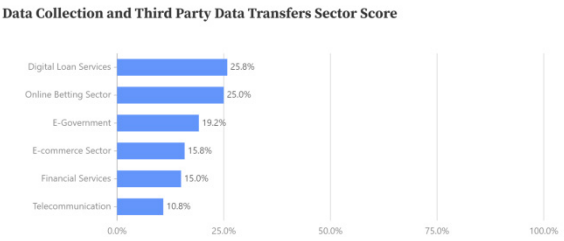
Informed consent – the highest score at country level was 59.4% that was registered by Kenya and the lowest score was 23.4% registered by Zimbabwe. While, at sector level, the highest score was 61.9% registered by e-commerce and the lowest score registered was 9.2% by e-Government. Find below figures showing the performance of the different countries and sectors against the indicator.



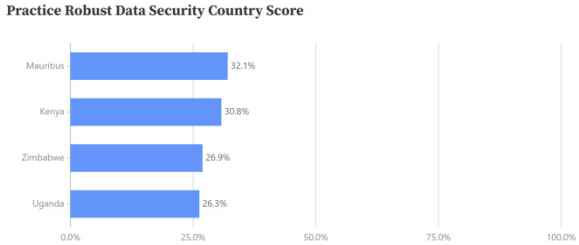


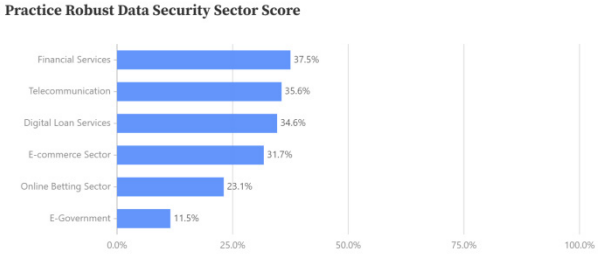
Data collection and Third Party Data Transfers – at country level the highest score was 21.7% registered by Uganda while, the lowest registered score was 14.4% by Kenya. On the other hand, digital loan services was in the lead with 25.8% at sector level and telecommunications registered 10.8% as the lowest score. Below are figures showing the performance of the different countries and sectors against the indicator.



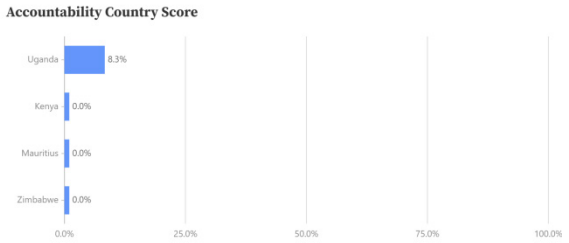


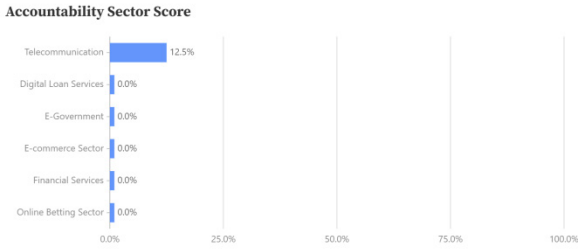
Practice Robust Data Security – Mauritius was observed in the lead with 32.1% as the highest score at country level and the lowest score was 26.3% registered by Uganda. While, financial services was in the lead with 37.5% as the highest score at sector level and the lowest score was 11.5% registered by e-Government. Find below figures showing the performance of the other countries and sectors against the indicator.



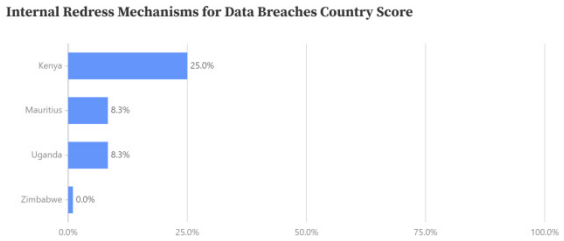


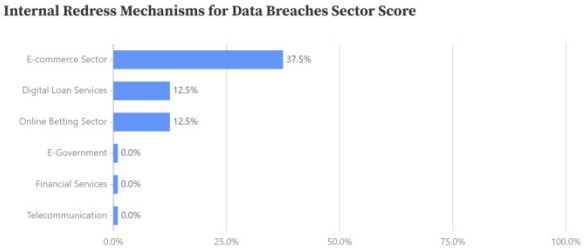
Accountability – Generally poor performance was observed for this indicator with only 8.3% registered by Uganda at country level. While, telecommunications that was in the lead only registered 12.5%. The figures below show the performance of the rest of the countries and sectors against the indicator.





Internal Redress mechanisms for Data breaches – poor performance was equally observed for this indicator. Kenya in the lead at country level registered only 25% while both Mauritius and Uganda scored 8.3%. E-commerce that was in lead at sector level, only registered 37.5% and a score of 12.5% was registered by both digital loan services and online betting sectors. More on the performance of the rest of the countries and sectors is further shown in the figures below.





4. Challenges

Several complex challenges exist cutting across Mauritius, Zimbabwe, Kenya and Uganda that inhibit companies/organizations from enhancing transparency and demonstrating compliance with data protection principles and standards. While the legal foundations have been instituted through the Data Protection Acts, translating provisions into ethical practices across industries remains challenging. These challenges are discussed in detail below.

a. Limited understanding of data protection and privacy legislation: observed in different publicly available privacy company policies, characterized by a prevalence of vague and ambiguous language including use of blanket statements rather than outlining granular data indexes, tailored retention schedules, processing purposes or exhaustive security details as mandated by law. Closely linked is the inadequate expertise on how to operationalise fair information procedures and transparency best practices. Often, policies are buried in obscure website footer links rather than highlighted prominently for users. This indicates that many data controller/processors are currently unaware of the heightened transparency expectations and consent procedures contained in the different data protection and privacy Acts.

Several companies have not yet invested in understanding precise compliance steps. While some organizations have appointed Data Protection Officers and made initial enhancements, capacity at middle management and employee levels remains underdeveloped. Yet, building expertise and changing organizational practices to align with modern principles takes time. Training and educational programs on aspects like consent flows, data mapping, access protocols, risk assessments and reporting metrics are still emerging both within public and private sector entities.

b. Insufficient regulatory capacities: effective oversight relies on regulators having sufficient and skilled staff, technical expertise, and funding to continuously monitor organizations' compliance, enforce provisions, investigate complaints, resolve cases, adapt to new technologies, and impose measured sanctions as warranted.

Several of these entities are in their infancy and are not functioning as fully fledged authorities as they ideally should. For instance Uganda's PDPO operates within the NITA-U building, while Zimbabwe's Data Protection Office is housed in the POTRAZ building. Similarly, Mauritius's Office remains within the Ministry of ICT, lacking full independence as mentioned in the earlier discussions above. In contrast, Kenya's Office has moved out of the Communications Authority building.

Currently also these entities have limited staff and are not yet equipped for large-scale and rigorous enforcement to sufficiently supervise diverse industries including legacy systems and emerging technologies.

c. Resource constraints: operationalizing extensive procedures around access requests, data protection impact assessments, retention schedule alignment and security enhancements require financial resources that few local companies/organizations currently have. While larger are initiating investments, limited funding inhibits most controllers/ processors from rapidly instituting transparency mechanisms. This is coupled with lack of locally tailored tools and templates. As such, companies are forced to make incremental enhancements slowly over years rather than transform systems overnight.

Extensive investment is required for the realisation of the expansive mandate spanning audits, guidance, sanctions, resolution, research and international cooperation provided for in the different data protection and privacy legislation. Areas like forensic analysis skills, data science expertise, legal aid units and decentralized intake centres must be strengthened. Regulators can issue transition periods/plans for under-resourced entities to progressively meet requirements. However, insufficient funding cannot fully justify opacity – minimum transparency requirements must still apply across the board. Authorities in Mauritius, Zimbabwe, Kenya and Uganda like other counterparts across the region, require sustained budgetary support and partnerships to mature into effective oversight bodies.

d. Weak accountability culture: norms and practices around proactive transparency, access procedures, ethical data use, security protections and reporting have not yet gained strong traction across the public and private sectors. Often, companies still consider data protection primarily through a legal lens focused on avoiding penalties rather than an ethical lens centered on consumer dignity. Notably viewed as burdensome obligations and not core duties to customers and public accountability. Fostering a culture that values user dignity, consent and control necessitates consciousness raising beyond compliance checklists to ethics principles. Whilst regulators and policymakers set the tone through awareness-raising, standards and incentives that make transparent data stewardship an expectation rather than an exception.

e. Rapid technological changes: emerging technologies like Internet of Things (IoT), cryptocurrencies, artificial intelligence (AI), augmented reality and machine learning are transforming data collection and processing capacities in ways that pose unforeseen privacy risks. Equally, narrowly defined regulations risk rapidly becoming outdated as new use cases and business models enabling more intrusive and opaque data gathering emerge across industries. The scale of data accumulated, granularity achieved, secondary uses catalysed and consent dilemmas heightened by new technologies create complex regulatory challenges. What constitutes lawful practice ought to be interpreted to adapt across domains. Regulators thus need both technology expertise and flexibility to apply core principles and protections to new contexts. Consultations with industry on steering evolving data ecosystems while respecting rights will be important. As technologies proliferate, interoperability and consent mechanisms must be strengthened to maintain user control.

f. Low public awareness: Transparency mechanisms imposed on companies/organizations can only be effective if general public awareness around data protection issues is strengthened substantially. However, digital literacy remains low, currently characterised by limited citizen consciousness of privacy risks and rights across demographics. Invariably restricting the ability to demand for accountability through complaints handling and redress mechanisms. Equally, the existence of polarized political environments contributes to misrepresentation of certain transparency efforts as ulterior "activism", inhibiting sincere discourse. Social taboos regarding privacy also persist, deterring victims of abuse from speaking out. Such dynamics hamper public sensitization.

Civil society has a crucial role in translating complex principles into relatable contexts that resonate with citizens' everyday experiences. Both traditional and social media campaigns tailored for different demographics, local languages, and cultural nuances are needed to build widespread user capacity to demand accountability from data collectors and leverage available grievance mechanisms. The data protection journey in these countries and across the region requires bringing citizens across segments to recognize privacy as an everyday, lived experience deserving protection. Thus, collaborative public education between state and non-state actors is critical to activate demand for lawful data governance.

g. Political and social tensions: constraining transparency by state or private sector data controllers including surveillance overreach or hostility towards oversight by activists, civil society, public individuals, politicians, etc attributing ulterior motives. Equally as well, open accountability comes under threat in polarized or authoritarian environments-requiring particular vigilance and alternative means of external pressure. Multi-stakeholder processes bringing together stakeholders beyond 'usual suspects' often present opportunities to foster dialogue and de-escalation. Even amid restrictions, controllers should still strive for greatest achievable transparency with users and demonstrate commitment whilst, it's imperative that regulators maintain independence and objectivity.

5. Lessons Learned and Best Practices

This section sets out to highlight experiences and practices that the countries under review and the wider region can draw key lessons and emerging best practices on effectiveness, enhancing transparency and accountability from each other and other jurisdictions that have implemented data protection laws and oversight framework. These are discussed in detail below;

i. Highlight Positive Leaders: initiatives to institute annual awards/certifications by data protection authorities to recognize companies/organisations with exemplary privacy policies, access procedures, security practices and reporting. Positive recognition incentivizes entities to elevate accountability. A case in point is India's data protection authority that instituted the "Data Security Council of India Privacy Awards" across categories including best privacy policies[1] with exemplary data transparency and protection practices like detailed auditing and reporting among others.[2] Such leading examples motivate peers to emulate transparent practices and incentivises more entities to proactively elevate their accountability and data governance.

ii. Incentivize Accountability: to encourage more entities to strengthen commitments to transparency. 'Data protection trust marks' for audited entities, 'safe harbour' programs for adequate compliance, and reduced requirements for high performers have helped elevate practices. The EU and APEC use self-certification programs allowing member entities to publicly attest to high data protection standards.[3] Positive incentives effectively motivate entities to respect and enforce data privacy practices beyond penalties alone.

iii. Combine Incentives and Deterrence: lessons are drawn from the EU which employs both incentives like certifications for high performers as well as strong sanctions to encourage accountable practices, rather than just penalties.[4] Providing carrots through safe harbour programs, eased audits and recognition, alongside firm penalties for wilful violations pushes transparent data stewardship. The data protection authorities may consider the use of both incentives and graduated enforcement to motivate positive norms.

iv. Enforce Intelligently: to build norms, regulators can use a graduated enforcement approach - initially relying on warnings, remedial orders, training requirements and minor sanctions before major penalties for violations. It enables developing capacities while firmly addressing wilful non-compliance. Lessons to be drawn from the UK ICO example, that responds based on risk and compliance history - education, audit, enforcement and prosecution.[5] A responsive approach brings the greatest impact on overall ecosystem accountability.

v. Issuance of Guides and Sectoral toolkits: user-friendly guidance templates/ tools by regulators for common practices–consent flows, data mapping, retention schedules, access protocols and reporting systems. Lessons drawn from namely; Singapore's regulator who developed sample consent forms, data inventory templates and breach notification formats for organizations[6] and sectors like healthcare and education[7] to adapt; Europe's GDPR catalysed numerous toolkits and training programs catering to sectors[8]; Kenya's Office of the Data Protection Commissioner provides tailored checklists for different entities and model privacy

1. See Indian Data Protection Summit Awards, 2022, at <https://idps2022.in/wp/awards/#:~:text=Privacy%20Champion%20is%20an%20award,entity%20and%20operating%20in%20India> accessed 11 October 2023.
2. Indian Data Protection Summit Awards, 2022, Retrieved from https://idps2022.in/wp/awards/#:~:text=Privacy%20Champion%20is%20an%20award,entity%20and%20operating%20in%20India
3. Clare Sullivan, 'EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era' (2019) Elsevier.
4. Sullivan, C. (2019). EU GDPR vs APEC CBPR: A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. Elsevier.
5. UK Information Commissioner's Office, 'Enforcement' < https://ico.org.uk/for-organisations/guide-to-eidas/enforcement/#:~:text=If%20you%20fail%20to%20comply%20with%20an%20ICO%20Enforcement%20Notice,4%25%20of%20your%20total%20worldwide> accessed 11 October 2023.
6 Lim Chong Kin and Anastasia Su-Anne Chen, 'Singapore: Data Protection and Cybersecurity' (2023) < https://www.legal500.com/guides/chapter/singapore-data-protection-cybersecurity/> accessed 11 October 2023.
7 Lim Chong Kin & Anastasia Su-Anne Chen, (2023) 'Singapore: Data Protection and Cybersecurity' Retrieved from https://www.legal500.com/guides/chapter/singapore-data-protection-cybersecurity/
8 European Parliament, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) European Parliamentary Research Service.

impact assessments.[9] While, developing Zimbabwe's POTRAZ has developed sector-specific playbooks and adaptable resource attuned to diverse data processing activities to aid controllers'/processors' preparedness.

vi. Issuance of Practice Codes: governing specialised data uses like surveillance, direct marketing and research.[10] These provide adaptable guidance for domains facing ethical dilemmas between principles like consent versus public interest. Learning from the UK experience where the regulator has already developed various codes, the data protection authorities in Mauritius, Zimbabwe, Kenya and Uganda should similarly issue practice codes tailored for sensitive contexts to bridge normative grey areas.

vii. Automate Monitoring of data systems: Emerging technologies like machine learning, natural language processing and web scraping tools can help monitor large numbers of privacy policies and disclosures at scale to identify deficient entities for review. A case in point, is the UK-based CHIP tool that uses AI to analyse policies for GDPR compliance.[11] Similarly, South Africa's regulator monitors websites for protection of children's information.[12] Adopting such technical solutions enhances cost-effectively the regulators' oversight capacities, tracking thousands of websites and flagging risks for further audit. As such, automated monitoring compliments manual policy reviews.

viii. Multi-Stakeholder Collaboration: in form of open and ongoing consultations with diverse industries, academic, technocrats, civil society, state and non-state actors fosters perspectives on challenges and emerging solutions including balancing various interests for collective ownership of enhancing accountability. Lessons are drawn from South Africa's regulator who convened and facilitated data value chain-specific workshops including ISPs, banks, marketers, insurers, telecoms, retailers, civil society groups and government agencies[13]and others to understand domain-specific issues. These kind of engagements shape balanced policies attuned to operational realities and viable proposals tailored for legacy systems and new technologies as well as encouraging open dialogue between stakeholders beyond the "usual suspects" to forge collective data governance solutions.

ix. Prioritisation of Consumer rights and organisation: Spotlighting impact of data practices on rights of consumers through data from complaints handling mechanisms including investigations of reported cases, consumer advisories, and public outreach make protection relatable. Best practices are drawn from the Philippines, where consumer guides explaining data protection rights and risks in plain language have been issued.[14] Similarly, Kenya's regulator has investigated consumer complaints regarding digital lenders and fintech apps, securing remedies for injured parties.[15] Thus, centring experiences of users highlights real-life effects, helping to demystify opaque practices. Equally, strengthens user perspectives on oversight through active collaboration with consumer forums and public interest technologists.

x. Institute Complaints handling/redress mechanisms: Fair and responsive mechanisms for individuals to submit inquiries, complaints and appeals provides accountability. Internal grievance officers supplemented by regulator units and tribunal adjudication enable aggrieved data subjects to seek proper recourse against opaque practices. Drawing lessons, under Kenya's data protection law, individuals can first approach an organization's grievance redress officer before escalation to the regulator.[16] Effective resolution buttresses oversight with bottom-up responsiveness.

xi. Carryout Privacy Sweep Assessments: Proactive regulator-initiated assessments[17] of data practices help to gauge transparency and compliance beyond relied-on entity reporting. Lessons are drawn from India where the data protection commission conducted website privacy sweep reviews across multiple sectors to assess compliance gaps even before its law came into force.[18] Such assessments create benchmarks and uncover focus areas

9 Bridget Andele, 'Data Protection in Kenya: How is this right protected?' (2021) Access Now.
10 ICO, op cit.
11 Ibid.
12 Jako Fourie, 'South Africa: Processing of children's personal information in the modern age of technology' (2022) Data Guidance <https://www.dataguidance.com/opinion/south-africa-processing-childrens-personal> accessed 9 October 2023.
13 Hogan Lovells, (2023) 'Recent developments in African data protection laws - Outlook for 2023' at accessed https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45
14 Karen Ocampo, Jude Ocampo and Ma. Cristina Suralvo, 'Data Protected-Philippines' (2022) < https://www.linklaters.com/en/insights/data-protected/data-protected---philippines> accessed 10 October 2023.
15 Mweu, op cit.
16 Nzilani Mweu, 'Kenya: Data Protection Overview' (2023) Data Guidance < https://www.dataguidance.com/notes/kenya-data-protection-overview> accessed 12 October 2023.
17 Global Partners Digital. (2022). Reimagining Data and Power: A Roadmap for putting values at the heart of data. Retrieved from https://www.data4sdgs.org/sites/default/files/services_files/Final%20White%20Paper%20designed%20%28English%29.pdf
18 Global Partnership for Sustainable Development Data, op cit.

beyond visible violations that reactive complaints would indicate. Proactive sweeps enable indicator-based enforcement that provide insights into compliance levels rather than purely relying on reported violations or abuses.

xii. Conducting Market Studies: for in-depth examination of how data is collected, shared and used within specific sectors provides granular insights into novel risks, harms, needs and challenges. Borrowing a leaf from South Africa, the regulator commissioned an in-depth research into the Internet of Things (IoT) ecosystem and gained an understanding of the salient issues including consent, profiling and security safeguards.[19] While, in Kenya practices of digital lenders have been reviewed.[20] With such analysis, tailored recommendations are shaped that move beyond one-size-fits all regulation to address sector dynamics. It builds empirical understanding of the impact of technologies on rights.

xiii. Invest in Strategic Foresight Capacities: Alongside current oversight, to understand socio-technical changes on the horizon that will transform data stewardship expectations. Monitoring technological and business model shifts allows getting ahead of accountability issues before harm scales. Foresight research feeds into adaptable policies attuned to emerging challenges around privacy and autonomy. Lessons are drawn from South Africa's regulator who has in place a strategic future plan to anticipate and prepare policy for socio-technical changes on the horizon that could transform data privacy and governance expectations.[21]

Similarly, data protection authorities in Mauritius, Zimbabwe, Kenya and Uganda ought to consider investment in future literacy and anticipatory skills the experiences of fellow African and Asian states continue to provide useful examples of consultative guidance development, proactive compliance assessments, consumer empowerment, monitoring automation, positive incentives, tailored enforcement, market studies, adaptable codes of practice, experimental regulatory spaces and strategic foresight capacities to strengthen its data protection ecosystem and help guard rights amidst rapid technological changes.

xiv. Shape Sandbox Regulatory Spaces: to enable testing of new technologies and business models regarding privacy impact. A leaf can be taken from Singapore where a "sandbox express" program was designed exempting innovative data-driven experiments by start-ups and SMEs from certain upfront authorizations, provided adequate safeguards and oversight mechanisms are in place.[22] Similarly the data authorities in Mauritius, Zimbabwe, Kenya and Uganda institute calibrated experiments to respond nimbly to emerging developments.

xv. Manage third-party-related risks: Managing third-party risks is essential, as external users with access to your critical systems, including partners, subcontractors, vendors, and suppliers, can pose potential security threats. Even if trust exists, their systems might be vulnerable to cyberattacks. To address this, it's crucial to monitor third-party sessions on-site and in the cloud, clearly define those handling your data, establish service-level agreements (SLAs) with third-party providers, maintain regular accountability for data security, and collaborate with vendors to enhance mutual security measures. This proactive approach helps safeguard against vulnerabilities and strengthens your overall data security posture.

19 McArdle, L. A. (2021). Data Privacy Governance Framework for The Internet Of Things In South African Organisations (Thesis). Cape Peninsula University of Technology, Bellville, South Africa.
20 Leona Annelise McArdle, 'Data Privacy Governance Framework for The Internet Of Things In South African Organisations' (Thesis, Cape Peninsula University of Technology, 2021).
21 McArdle, op cit.
22 The Straits Times (2019) 'MAS Launches Sandbox Express for Faster Market Testing of Innovative Financial Products and Services' Retrieved from https://www.straitstimes.com/business/banking/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial

6. Conclusion

Taking stock of the personal data protection and privacy rights landscape in all the four countries reveals some positive developments alongside incremental achievements in the performance of data controllers or processors across the different sectors. Notably, Zimbabwe is credited for taking laudable steps to ensure data protection by the passage of its Data Protection Act and opportunities to build oversight capacities. While Kenya's ODPC is credited for initial steps on complaints management with 200 resolved cases out of the 400 received including offering several industry specific regulations. Uganda's PDPO efforts are acknowledged towards enforcement and awareness raising and Mauritius's Office for the initiatives on a network for data protection officers, progress with complaints handling and much more.

Despite the overall performance, with Kenya and Mauritius performing slightly better than Uganda and Zimbabwe, the abuses/violations relating to personal data protection in all the countries are largely the same. Significant deficiencies and challenges across the public and private sectors when benchmarked against the different data protection legislation in these countries. From ambiguous policies to absent user right facilitation and minimal reporting, persistent gaps between current practices and accountability.

The path to greater openness around data handling will be long and indeed, there will always be challenges, setbacks and new complexities in governing data flows. However, it is imperative to build trust in digital services through cooperation balanced with regular monitoring of data breaches and compliance, raising accountability and embedding ethical data stewardship. Regulatory oversight, technical guidance, capacity building, incentives and pubic engagement are essential for the realisation of the aspirations pertaining to lawful, fair and responsible data governance under the different data protection legislation. Data controllers and processors ought to evolve from opaque to transparent stewards of user data, which would represent a major collective achievement for consumer rights and dignity. Regulators play a key role in setting this vision and modulating interventions based on risks and conduct. Equally, a wider alliance encompassing policy-makers, technical experts, consumer voices and conscientious companies/organisations is needed to make user-centric privacy preservation a social reality and competitive advantage.

7. Recommendations

Realising effective data protection that upholds user rights will necessitate action across diverse sectors/industries and stakeholders including controllers, processors, regulators, policymakers, technologists, consumer groups and citizens themselves through cooperation, vigilance and dialogue. A multi-pronged approach can best enable the objectives of accountability, lawful collection and ethical use enshrined in most of the data protection legislation. This section sets out to highlight appropriate recommendations made to different actors–state and non-state actors which are detailed below.

Recommendations for data controllers and processors

Data controllers and processors have a crucial responsibility and should:

1) Proactively elevate transparency and implement accountable data practices aligned with Data Protection legislation like the annual release of a transparency report, to demonstrate commitment to accountability beyond passive policies alone. Such a report would be highly effective as it would comprehensively detail the collection of personal data throughout the year, specifying who had access to it, whether government entities, private organisations or individuals.

2) Take steps as the custodians of personal data collection, storage and use, to publish detailed privacy policies that provide exhaustive inventories of data types rather than vague summaries.

3) Outline specific retention periods tailored to different categories of user information rather than indefinite storage.

4) Describe security protections in place, whether organizational, physical or technical.

5) Establish functional mechanisms for users to submit access, correction or deletion requests and obtain remedies. This necessitates instituting internal training and access protocols beyond just policy declarations.

6) Comprehensively disclose any third-party entities or affiliates with whom personal data is shared, justifying the necessity rather than blanket statements of obeying legal mandates.

7) Undertake periodic data protection impact assessments to continuously evaluate their privacy risks and harms.

8) Recognize transparency and lawful data governance as not burdensome obligations but ethical imperatives vital for consumer trust and exercising of data protection rights.

Recommendations for data protection regulators

Regulators as oversight authority under data protection legislation should:

1) Proactively undertake privacy sweep assessments of organizations across sectors to audit their publicly posted policies and visible practices against applicable transparency requirements. Such sweeps create evidence-based benchmarks and uncover focus areas for regulatory action.

2) Guide compliance, monitoring enforcement, and institutionalise accountability ecosystems.

3) Institute programs that highlight entities and sectors with particularly exemplary accountability practices, through awards, certifications, eased requirements or other incentives.

4) Recognise leading performers to motivate wider adoption of transparent data handling

5) Publish user-friendly guidance resources and tools catering to specific sectors and common practices to aid controllers translate legal principles into organizational procedures.

6) Make use of a graduated enforcement approach that relies on warnings, training requirements and minor initial sanctions to aid raising consciousness and build capacities across industries before escalating to major penalties for wilful violations.

7) Build regularly own oversight capacities for compliance monitoring, investigations, audits and enforcement to

fulfil mandate under data protection legislation.

8) Operationalise smooth complaints handling, expedient resolution mechanisms and appeal processes for aggrieved users to obtain redress against opaque practices.

9) Maintain independence from partisan or industrial influence to objectively supervise data protection standards in user interest.

Recommendations for policymakers

To strengthen data protection, policymakers should:

1) Enact additional legislation articulating and enforcing consumer rights in the digital economy for users to hold companies /organisations accountable due to irresponsible data collection or misuse.

2) Incorporate rights literacy and skills-building on data protection in educational curricula in tertiary schools and professional training programs to social capacity on exercising user privileges and informed consent.

3) Provide adequate budgets and resources for public awareness campaigns that educate citizens across demographics, languages and media platforms about core data rights, risks, entitlements and complaints channels and continued capacity development of regulators to effectively fulfil their challenging mandate.

4) Make incorporation of 'privacy by design' principles and data protection impact assessments an obligation in public sector digitization programs to uplift state transparency.

Recommendations for technology service providers

Technology service providers like cloud and analytics companies that develop capabilities leveraged across industries should:

1) Make upholding transparency integral to technical architectures rather than an afterthought

2) Pre-configure tools with strong access controls, encryption, anonymization, compliance dashboards and consent mechanisms.

3) Guide clients on minimal data collection, storage limitation, tailored retention and data mapping.

4) Clearly communicate their own limited data use, prohibit onward sharing and institute third-party audits.

5) Develop robust yet usable data protection capacities within digital infrastructures to enable accountable practice.

Recommendations for users /data subjects

As data subjects, users should:

1) Exercise vigilance and inquisitiveness regarding how their personal information is handled.

2) Thoroughly read privacy policies before accepting terms of use rather than automatically clicking consent. Where possible, users should opt out of non-essential data collection and processing that violates privacy principles.

3) Proactively submit queries and complaints to companies/organizations regarding opaque practices for clarification or remediation. Escalate unresolved grievances to regulators for investigation.

4) Directly call out organizations that demonstrate deficient transparency or disregard for data responsibility through public campaigns on social media or collective petitions.

5) Back up critiques and demands for accountability with evidence and articulate them in constructive ways.

Recommendations for civil society

As representatives of public interest and user rights, civil society groups have a vital role in strengthening data protection accountability ecosystems and should:

1) Undertake independent assessments of data practices of companies/organizations from the perspective of

consumer impacts rather than purely technical compliance.

2) Document user experiences involving opaque data collection or privacy harms through complaints data, focus groups and interviews to make such evidence crucial for making opaque practices relatable and centre citizen voices in policy conversations.

3) Publish explainers, guides and advisories on data protection issues tailored for diverse demographics in accessible formats and multiple languages.

4) Advocate for elevated transparency commitments from companies/organizations through campaigns, petitions and dialogue.

5) Proactively partner with responsible industries/sectors and regulators in steering evolving best practices and identifying pragmatic solutions for balanced scholarship and oversight.

Recommendations for academia/scholars

As impartial observers, academic scholars and institutions input is vital for informed, balanced should:

Undertake research monitoring and evaluate data protection accountability based on indicators like policy transparency, security audit results and user perceptions.

1) Study sector-specific data ecosystems to inform tailored oversight.

2) Build interdisciplinary expertise and offer courses educating students on privacy-preserving technology design, ethical data use, and data protection law.

3) Host public forums fostering evidence-based dialogue between policymakers, industry, civil society and users on navigating emerging challenges and trade-offs. Academic input is vital for informed, balanced and farsighted data governance.

Privacy Scorecard Report 2023

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