PRIVACY SCORECARD REPORT/2024

Rwanda . Tanzania. Mauritius . Zimbabwe . Kenya . Uganda

If You Must Collect It, You Must Protect It

Written and Compiled by:

PRIVACY Scorecard

UNWANTED WITNESS

"Amplifying Voices, Changing lives"

PRIVACY SCOREDCARD REPORT /2024

PRIVACY Scorecard

UNWANTED WITNESS

"Amplifying Voices, Changing lives"

CONTENTS

LIST OF *ACRONYMS*

AI	Artificial Intelligence
APC	Association for Progressive Communications
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CSO	Civil Society Organisations
DPA	Data Protection Act
DPPO	Data Protection and Privacy Office
DPO	Data Protection Office
DPO	Data Protection Officer
EU	European Union
EU GDPR	The European Union's General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IECMS	Integrated Electronic Case Management System
IoT	Internet of Things
ISO	International Organization for Standardization
LTD	Limited
NCSA	National Cyber Security Authority
NIRA	National Identification Registration Authority
NIRA	National Identification and Registration Authority
NITA-U	National Information Technology Authority, Uganda
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
OSF	Open Society Foundations
PDPC	Personal Data Protection Commission
PDPO	Personal Data Protection Office
PDPO	Personal Data Protection Office
POTRAZ	Postal and Telecommunications Regulatory Authority
SMEs	Small and Medium-sized Enterprises
UW	Unwanted Witness Uganda

LIST OF RESPONDENT *COMPANIES*

Rwanda

MTN Rwanda
Airtel Rwanda
Liquid Telecom Rwanda
Murukali
Vuba Vuba
Kikuu
Ubuy
Premierbet
Africabet
Gorilla Games
BetPawa
Bank of Kigali
Access Bank
Equity Bank
Eco Bank
Britam
BK Insurance
Old Mutual Insurance
Prime Insurance
Irembo Go v
Rwanda Social Security Board (RSSB)
Rwanda Revenue Authority (RRA)
Rwanda Information Society Authority (RISA)
University Teaching Hospital of Kigali (Chuk)
King Faisal Hospital
Ruhengeri Referral Hospital
Rwanda Military Hospital
Spenn
Save
Kiva
Pesheza Rwanda

Tanzania

Vodacom
Tigo Tanzania
TTCL
Airtel Tanzania
Jiji Tanzania
Kikuu Tanzania
Inalipa
Kupatana
SportPesa Tanzania
Betika Tanzania
BikoSports
SportyBet
NBC Bank
NMB Bank
Equity Bank
Stanbic Bank Tanzania
Tanzania Regulatory Authority (TCRA)
Tanzania Civil Aviation Authority (TCAA)
e – Immigration Tanzania
Tanzania Work Permit Application Portal
Branch International Tanzania
PesaX Tanzania
Mpokowako Tanzania
TwigaLoan
Lyfplus Tanzania
Regency Medical Center
CRBT Tanzania
Muhimbili National Hospital

Mauritius Companies

Emtel Limited
Liquid Telecom
MyT
AtComm
Bank of Baroda
SBM Bank (Mauritius) Limited
Swan Life Limited
ABSA Bank (Mauritius) Limited
Pick and Buy Limited
Intermart (Mtius) Ltd
Price Guru
Temu Mauritius
Marideal
Woolworths Mauritius Online
Supertote
StevenHills Mauritius
Totelepep
William Hill

Zimbabwe Companies

Econet
TelOne
NetOne
Liquid Telecom Zimbabwe
Stanbic Bank Zimbabwe
NMB Bank
CBZ Bank
Empower Bank
Ubuy Zimbabwe
Shumba Africa
Raines Africa
Tengai Online
Mrbet
Pinnacle Sports
Africabet
Bezbets
Ecocash
Zibuko

CIM Finance
FinClub
Fundkiss
Mauritius Revenue Authority (MRA)
The passport and immigration office
MauPass (Mauritius Personal Access)
Information and Communication
Technology Authority Mauritius (ICTA)
Wellkin Hospital
Clinique Darne
Aegel Clinic
Dr Agarwal's Eye Hospital
SICOM
Jubilee Allianz General Insurance
Eagle Insurance
Mauritius Union Assurance

Kenyan Companies

Safaricom
Zuku
Jamil Telecommunication Ltd
Airtel Kenya
Stima
Equity Bank Kenya
ABSA Bank Kenya
KCB Bank
Jiji
Jumia
Glove Kenya
Kilimali
Betika
1xbet Kenya
BetPawa Kenya
SportPesa
Branch International Kenya
Tala
Zenka
LendPlus
E-Citizen
Huduma
Kenya Revenue Authority (KRA)
ETA (Electronic Travel
Authorisation Kenya
Agakhan University Hospital
Nairobi Hospital
Nairobi Women's Hospital
Karen Hospital
Jubilee Insurance Kenya
Britam Insurance Kenya
ICEA Lion Insurance
CIC Kenya

IM Bucks
eShagi
E-Visa Department
Zimbabwe Revenue Authority (ZRA)
National Social Authority (NSSA)
Karanda Mission Hospital
Mpilo Central Hospital
Baines Avenue Clinic
Pararinyetwa General Hospital (PGH)
Old Mutual Zimbabwe
Zimnat Lion Insurance
Alliance Insurance
Cell Insurance

Ugandan companies

Lycamobile
MTN Uganda
Airtel Uganda
Roke Telkom
Stanbic
Pride Microfinance Ltd
ABSA Bank Uganda
Centenary Bank
Jiji
Jumia
Glove Uganda
Kikuu Uganda
Fortebex
Ixbet Uganda
BetPawa Uganda
22bet Uganda
Dove Cash
Mangu Cash
iSente
Quick Sente
Immigration Uganda
National Identification & Registration Authority
Electoral Communication Uganda

Uganda Bureau of Statistics (UBOS)
Case Hospital
IHK Hospital
Lubaga Hospital
Nakasero Hospital
UAP Old mutual Uganda
Sanlam
Britam Uganda
Jubilee Insurance Uganda

ABOUT *UNWANTED WITNESS*

Unwanted Witness Uganda – UW is a civil Society Organisation founded in 2012 to promote online freedoms and protect digital rights in Uganda. UW has since 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 across Africa.

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

A world where digital rights are respected.

Mission Statement

To empower individuals and advocate for digital rights in Africa.

Corporate Values

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

ACKNOWLEDGEMENTS

Unwanted Witness (UW) extends its sincere appreciation to the key civil society organizations that have supported its work. We are especially grateful for the financial backing from our development partners, notably the Association for Progressive Communications (APC) and Open Society Foundations (OSF), whose financial and technical assistance have been instrumental in ensuring the successful annual production of this report.

UW acknowledges the valuable contributions of its Research and Advocacy Unit, with special recognition to Ms. Freda Nalumansi and the team of researchers: Mr. Brian Kiira, Mr. Harry Mwesigwa, Ms. Mercy Sulel, Mr Nuwe Ahereza Marvin, Mr. Dalton Kisuule, Ms. Joyce Namakoye and Ms. Alyce Namale. Our heartfelt thanks also go to the editorial board members, particularly Executive Director Ms. Dorothy Mukasa, Head of Programmes Mr. Allan Sempala Kigozi, Research and Advocacy Lead Ms. Freda Nalumansi and Mr John Kauta, IT Manager for their essential guidance including the development of the data collection tool and tech analysis in the report. Additionally, we recognize the efforts of other staff members who played a crucial role in supporting the report's production.

UW would also like to express its gratitude to the individuals and organizations that contributed throughout the development process. In particular, we thank Price Media for their expertise in graphics and layout, which greatly enhanced the report's final presentation. Their contributions during the development and review stages were invaluable in enriching the report.

EXECUTIVE *SUMMARY*

This marks the 4th edition of the Unwanted Witness Privacy Scorecard Report, a monitoring tool rooted in local data protection laws and internationally acceptable principles aims to take stock of compliance and privacy practices of both private and public sectors and the impact on user privacy rights.

This assessment that is conducted annually, expands its scope beyond previous evaluations to include Rwanda and Tanzania, alongside Kenya, Uganda, Mauritius, and Zimbabwe. The 2024 report builds on prior evaluations of data protection and privacy compliance, reflecting the evolving digital landscape and the increasing regulatory attention on safeguarding personal data across the region. As digital economies continue to grow, so do concerns around personal data security, unauthorized surveillance, and data protection enforcement.

This edition introduces a more detailed and robust methodology, evaluating the performance of data collectors across eight sectors: telecommunications, e- commerce, online betting, banks and finance, insurance, government agencies / bodies, health and digital loans. This report assesses the implementation of data protection laws, highlight performance trends over the years and challenges, best practices, using seven key indicators - Registration with the National Regulator, Accessible Privacy Policy, Pre-collection Data Transparency (Data Subject Rights), Third-Party Data Transfer, Practice Robust Data Security, Availability of Transparency Report and Internal Data Breach Resolution.

The evaluation is also structured around: A contextual overview of data protection laws, institutional frameworks and their enforcement; an in-depth country analysis encapsulating sectoral performance insights based on a study of 109 selected companies/entities, findings on key compliance indicators; challenges, emerging trends, and lessons learned from different jurisdictions; and actionable recommendations to enhance privacy protections.

The study assesses how private and public sector entities manage personal data, revealing significant gaps in enforcement, regulatory capacity, and public awareness. While digital services such as mobile money, ride-hailing apps, e-commerce, and digital lending platforms continue to expand, data breaches, unauthorized surveillance, and weak enforcement mechanisms remain critical concerns. Despite legal frameworks being in place - with Rwanda, Tanzania and Zimbabwe being the most recent countries to enact data protection laws in 2021/2022, practical implementation lags due to resource constraints, low compliance culture, insufficient accountability mechanisms, and the rapid pace of technological advancements. The absence of effective redress mechanisms further weakens data protection efforts, leaving individuals vulnerable to privacy violations.

Compared to last year's score of 47.3%, this year's overall index score was 40%, with Kenya recording the highest score. This was followed by Uganda, Mauritius, Rwanda, Tanzania, and Zimbabwe. At the sector level, the overall score was 42%, recorded by the Banks and Finance Sector, closely followed by Insurance at 40%, and a tie between Telecommunications and E-commerce at 39%.

According to the assessment, the performance of selected companies /entities across the different sectors revealed that in the telecommunication sector, MTN Uganda leads with a 69% privacy score, followed by Vodacom Tanzania (62%) and MTN Rwanda (57%), reflecting strong data protection measures. Mid-tier companies like Safaricom (53%) and Airtel Uganda (44%) show moderate efforts but need improvements in encryption, transparency, and user consent. Low performers such as NetOne (4%), TelOne (19%), and Lycamobile (33%) face major privacy risks, regulatory challenges, and potential customer trust issues. High-scoring firms benefit from consumer trust and reduced regulatory risks, while low-scoring ones risk legal consequences and cybersecurity threats.

In the e –commerce sector, Glovo Uganda (58%) and Glovo Kenya (56%) lead in data protection, while Jiji Uganda (47%), Jiji Kenya (50%), and Woolworths Mauritius Online (46%) show moderate commitment. Jumia Uganda (40%), Jumia Kenya (47%), and Kilimall (44%) have room for improvement. Low scorers like Kikuu Uganda (29%), Inalipa (25%), and Raines Africa (23%) pose significant privacy risks, making them vulnerable to data breaches and legal penalties. High-scoring platforms gain consumer trust, whereas lower-rated firms risk reputational damage. Companies need to strengthen security, user consent, and transparency to enhance data protection and compliance.

Privacy and data protection practices among online betting platforms varied significantly. In Uganda, 1xBet and Fortebet score 32%, while BetPawa (23%) and 22Bet (27%) lag behind, highlighting gaps in compliance. Kenya sees Betika (35%) and SportPesa (39%) performing better than 1xBet (25%) and BetPawa (20%). Tanzania's SportPesa (40%) and SportyBet (41%) lead, while Bikosports (24%) and Betika (32%) score lower. Rwanda's Africabet (45%) and Gorilla Games (40%)

perform better, but Premierbet (7%) raises major concerns. Zimbabwe's Pinnacle Sports (41%) and Bezbets (30%) score higher than Africabet (29%) and MrXbet (27%). Mauritius sees extremely low scores, with Stevenhills (4%) and Totelepep (6%) performing poorly, while Supertote (45%) and William Hill (41%) rank higher. The widespread low scores indicate serious concerns over transparency, regulatory compliance, and data security, requiring urgent improvements to meet privacy standards.

The banks and finance sector in East and Southern Africa show mixed performance in data privacy. Uganda's Centenary Bank (57%) leads, followed by Stanbic (53%), Absa (46%), and Pride Microfinance (42%), indicating moderate efforts. Kenya's Equity Bank (52%) performs best, with Stima Sacco, Absa, and KCB at 46%. Tanzanian banks score lower, with NMB Bank (36%), Equity Bank (42%), and Stanbic/NBC (43%) showing weaknesses in compliance. Rwanda's banks perform poorly, with Bank of Kigali (33%) and Access Bank/Equity Bank (35%) struggling. Zimbabwe's CBZ Bank (55%) leads, while other banks, like Empower Bank (34%) and NMB (37%), reveal critical gaps. Mauritius' SBM Bank (44%), Swan Life (42%), and Absa Mauritius (41%) show moderate efforts but need improvement. Overall, most banks score below 50%, pointing to significant deficiencies in third-party data transfers, breach management, and transparency, requiring stronger data privacy measures to meet compliance standards.

For insurance, in Uganda the companies scored between 44% and 53%, with UAP Old Mutual Uganda leading at 53%. Kenya performed slightly better, with scores ranging from 51% to 52%, while Tanzania showed a wider range, from 4% to 54%. Rwanda and Zimbabwe had generally low scores, with some companies scoring as low as 4%. Mauritius performed best, with Mauritius Union Assurance scoring 72%. Overall, significant gaps remain in privacy practices, particularly in data security, transparency, and third-party data transfers.

Government agencies across the assessed countries struggle with privacy compliance. Uganda's agencies performed poorly, with scores as low as 3%. Kenya had mixed results, with KRA scoring 47% but others as low as 3%. Tanzania, Rwanda, and Zimbabwe's agencies also had low scores, reflecting serious deficiencies in data protection. Mauritius had similarly weak performance, with some agencies scoring below 10%. Overall, there is a widespread lack of transparency and security in handling citizens' personal data.

Equally health facilities showed weak compliance with data protection laws. In Uganda, IHK Uganda (55%) performed best, but most hospitals scored poorly. Kenya had similarly low scores, with Nairobi Women's Hospital at just 4%. Tanzania, Rwanda, and Zimbabwe's hospitals exhibited extremely poor privacy practices, with some scoring as low as 0%.

Mauritius performed slightly better, but significant gaps remain in transparency and data security. Overall, the health sector urgently needs reforms to ensure patient data protection.

While, digital lending platforms varied in compliance. Uganda's Mangu Cash led with 45%, but most platforms scored below 35%. Kenya's Zenka (50%) and Tala (47%) performed better but still showed weaknesses in third-party data transfers. Tanzania's platforms scored as low as 4%, reflecting major compliance gaps. Rwanda and Zimbabwe had similarly poor performance, while Mauritius' Cim Finance (59%) led in compliance. Overall, most platforms struggle with transparency, security, and regulatory compliance, posing risks to users' personal data. Across all sectors, major gaps in data protection and privacy compliance persist, exposing consumers to security risks and potential data misuse.

On the other hand, the performance trends over the years at the country level revealed that Kenya leads in data protection, peaking at 47.3% in 2023 before dropping to 40.0% in 2024, indicating challenges in sustaining progress. Mauritius also declined from 39.5% to 35.0%, highlighting the need for stronger regulatory frameworks. Uganda saw improvement in 2022 (47.4%) but declined to 38.0% in 2024, reflecting enforcement issues. Zimbabwe remains at the bottom with low scores (23.1% in 2023, 25.0% in 2024), showing major gaps in data protection. Rwanda and Tanzania, both newly assessed, scored 30.0% and 29.0% in 2024, respectively, indicating early-stage data protection frameworks. Overall, while Kenya leads, most countries struggle with maintaining or strengthening data protection laws, requiring enhanced enforcement and alignment with global standards.

While the trends in performance of various sectors revealed both progress and setbacks in their privacy and data protection practices. The e-commerce sector declined from 52% in 2022 to 39% in 2024, reflecting growing challenges in safeguarding customer data. Digital loans saw a sharp drop from 44.9% in 2023 to 32% in 2024, likely due to weak security and regulatory gaps. Telecommunications remained relatively stable, improving from 33.8% in 2022 to 39% in 2024 but still facing data protection gaps. The banks & finance sector declined significantly from 53% in 2022 to 29% in 2024, signaling major privacy compliance challenges. Online Betting stagnated at 29% in both 2023 and 2024, showing persistent regulatory weaknesses. Government agencies improved slightly from 11.1% in 2023 to 20% in 2024 but continue to struggle with weak data handling and enforcement.

The health sector remains the weakest, scoring just 19% in 2024, up from 0% in 2021, highlighting severe data security concerns. In contrast, insurance improved from 23% in 2021 to 40% in 2024, showing progress but still requiring stronger privacy measures. Overall, while some sectors like insurance show positive trends, critical areas such as e-commerce, digital loans, government, and health face urgent data protection challenges that need to be addressed to ensure compliance and build trust.

The Path Forward in ensuring effective data protection and privacy rights enforcement requires coordinated action from governments, businesses, regulators, and civil society. The report calls for stronger enforcement, increased transparency, and more proactive engagement in order to turn legal principles into real-world protections. Specific, actionable steps that each of these key stakeholders can take to enhance data protection and privacy are outlined below;

Recommendations for Governments

1. Establish independent data protection offices (DPOs) with adequate financial resources to function effectively and impartially.
2. Amend data protection laws to provide clear guidelines on audits, data retention, and breach notification procedures aligned with international best practices (e.g., GDPR, Malabo Convention).
3. Implement strict judicial oversight for government surveillance and ensure transparency in surveillance programs.
4. Countries like Tanzania should sign and ratify the African Union Convention on Cyber Security and Personal Data Protection to strengthen their commitment to privacy.

Recommendations for Policy Makers

1. Align national data protection laws with international standards such as GDPR and OECD privacy guidelines.
2. Ensure data protection laws specify clear penalties (e.g., percentage-based fines) to enhance enforcement without discouraging investment.
3. Promote cross-border collaboration on data protection to address global challenges in data governance.

Recommendations for Data Protection Regulators

1. Address legal gaps by introducing regulations on dispute resolution, appellate procedures, and mandatory transparency reporting.
2. Conduct large-scale sensitization initiatives targeting schools, businesses, and rural communities to educate citizens about their data rights.
3. Maintain a public registry of compliant data controllers and processors for easy verification by businesses and consumers.
4. Implement periodic audits to ensure organizations adhere to data protection laws and ethical data governance practices.

Recommendations for Data Controllers and Processors (Businesses and Tech Providers)

1. Adopt strong data security measures and publish annual transparency reports to demonstrate commitment to privacy.
2. Limit data collection to only what is necessary and ensure secure storage and timely disposal.
3. Mandate internal DPOs to oversee compliance with legal requirements and ethical data governance.
4. Report data breaches promptly to the regulatory authority and affected individuals.

Recommendations for Data Subjects (Individuals)

1. Utilize legal channels to report non-compliance and enforce privacy rights through complaints to data protection authorities or legal action.

2. Educate themselves on personal data rights and best practices for protecting their information online.

3. Hold businesses and service providers accountable by requesting information on how their data is collected, stored, and used.

Recommendations for Civil Society Organizations (CSOs) and the Media

1. Lobby for amendments in data protection laws to include enhanced rights for data subjects, such as the right to be forgotten and algorithmic accountability.

2. Investigate and document privacy breaches and raise awareness through media campaigns.

3. Encourage the use of encryption, anonymization, and circumvention tools to enhance personal data security.

Recommendations for the Technical Community

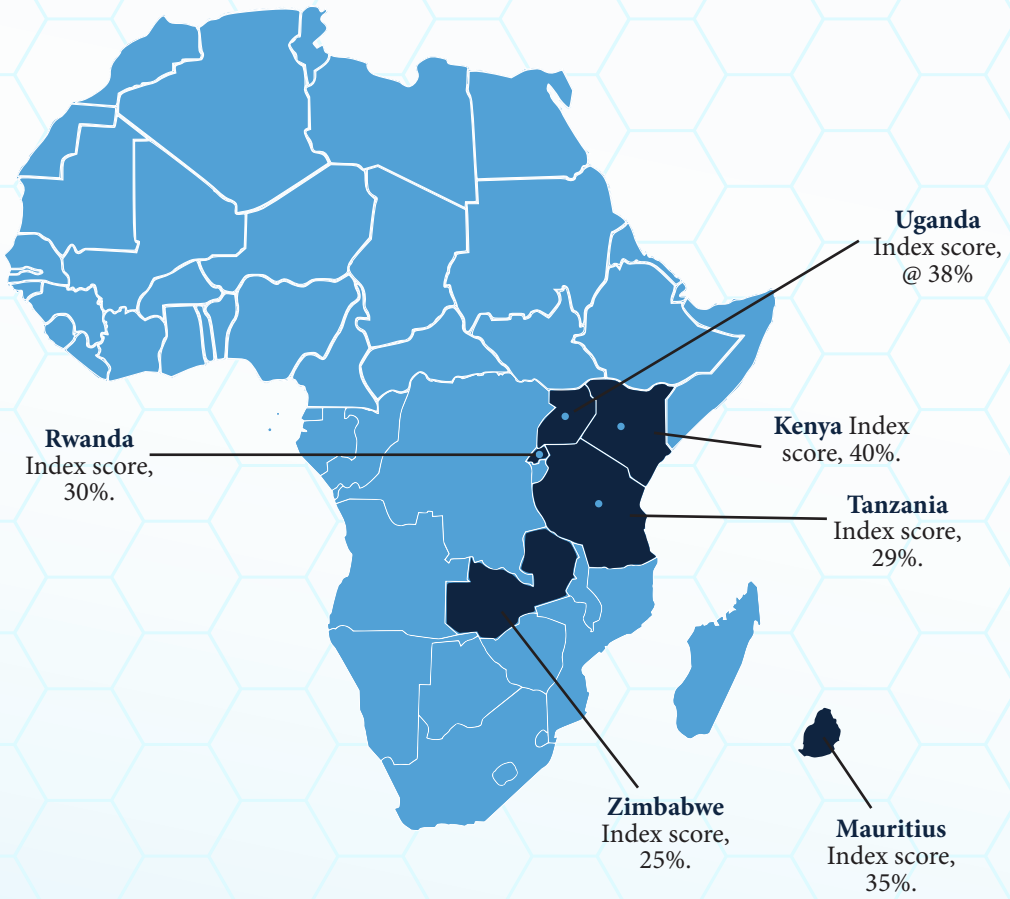
1. Offer insights on the impact of emerging technologies on data privacy to guide lawmaking.

2. Innovate tools that help individuals control their data and enhance security.

3. Equip businesses and individuals with skills to safeguard personal data against cyber threats.

As Rwanda and Tanzania join this year's assessment, the findings offer valuable insights into the state of data protection across East and Southern Africa. Strengthening enforcement, boosting regulatory capacity, and fostering a culture of compliance will be crucial to protecting personal data and advancing digital rights in the region.

190 companies / entities were assessed - overall index score for each country:



1. INTRODUCTION

In the current digital landscape, personal data has become one of the most valuable assets worldwide. Alongside this, ensuring the protection of privacy—a fundamental constitutional right—has emerged as a critical concern for regulatory bodies and organizations handling personal data. The Unwanted Witness Privacy Scorecard Report is a comprehensive monitoring tool designed to evaluate the compliance of both data collectors and processors, including public and private entities, with data protection and privacy laws. The report also provides actionable recommendations to enhance compliance.

In 2024, Unwanted Witness expanded its monitoring scope to include six African countries—Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda—compared to the four countries-Mauritius, Zimbambwe, Kenya and Uganda in 2023 while two countries -Kenya and Uganda were the only countries assessed in 2022. The latest report introduces a more detailed and robust methodology, evaluating the performance of data collectors across eight sectors: telecommunications, e- commerce, online betting, banks and finance, insurance, government agencies /bodies, health and digital loans. This expansion builds on the focus of the report in previous years. The assessment in 2024 was conducted using seven key indicators, as opposed to the six used in 2023. These indicators include: Registration with the National Regulator, Accessible Privacy Policy, Pre-collection Data Transparency (Data Subject Rights), Third-Party Data Transfer, Practice Robust Data Security, Availability of Transparency Report and Internal Data Breach Resolution.

Following a rigorous process, which includes peer reviews and quality control, organizations receive a score based on their performance across these indicators. The results are categorized, showing how each organization performed on specific indicators. Only privacy policies that are publicly accessible are eligible for credits in the Scorecard; internal policies or private practices, however well-intentioned, are not factored into the scoring.

Requiring publicly available documentation serves several important purposes. First, it ensures that companies cannot secretly change their internal practices without also revising their public policies, thus preventing deceptive tactics. Second, it allows us to scrutinize each organization's policies closely, fostering a broader public conversation about the standards companies should adopt. Third, it enables organizations to review each other's privacy policies, particularly regarding law enforcement access, providing a benchmark for startups and other entities seeking to implement strong privacy practices.

The Scorecard strives to set high yet achievable standards. We only include criteria that at least one organization has already adopted, ensuring we focus on practical best practices rather than theoretical goals. Each year, we revisit and refine the criteria to keep the Scorecard in line with current technological and policy developments.

The main objective of the 2024 report is to produce research that can empower data collectors and processors to adopt best practices in data protection, while also enabling citizens to hold organizations accountable for the management of their personal data. This report is also intended to contribute to legal and policy reforms that will improve personal data management, particularly among non-state actors. The Scorecard evaluates the privacy policies and practices of one hundred and ninety (190) organizations/ entites across eight sectors in 2024, assessing their compliance with both international standards and national data protection laws.

This report uses objective and quantifiable parameters to evaluate the publicly available policies of these organizations, examining their adherence to relevant data protection laws. It also documents any violations or abuses of privacy rights by the assessed companies in each country. The study seeks to accomplish the following specific objectives:

- To assess the legal protection of personal data and privacy in Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda
- To track changes in compliance and practices among the selected organizations
- To evaluate the adherence of data collectors in these countries to data protection laws
- To document any privacy violations or abuses by the companies assessed

- To provide recommendations for improving compliance with data protection laws in Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda, with a focus on private non-state actors
- To offer a practical toolkit that citizens can use to evaluate data collectors' compliance and advocate for improved data protection practices

The 2024 report continues to build on the findings of previous years' Privacy Scorecard Report, evaluating whether progress has been made in data protection across the selected sectors, despite the inclusion of an additional indicator

2. METHODOLOGY *AND CRITERIA*

The 4th edition of the UW Scorecard Report offers a snapshot of the privacy practices of 190 private and public companies, spanning six countries and eight industries, all of which manage substantial amounts of personal data due to the size and scope of their operations. From each sector, namely: telecommunications, e-commerce, online betting, banking and finance, insurance, government agencies/bodies, health and digital loan, four (4) companies were selected for assessment.

In all six countries, the companies were chosen based on their market share, with one representing the highest market share and the other holding a mid-tier position, creating a balance between major and mid-sized players within each sector. The assessment focused on the companies' compliance with data protection and privacy laws in their respective countries, evaluating them against seven core indicators. Each indicator includes measurable variables, with scores assigned based on the companies' adherence to data protection laws and regulations. These indicators and their corresponding variables include:

A. Registration with the National Regulator

This indicator in the Privacy Scorecard evaluates whether an organization has been formally registered with the designated data protection regulator in their jurisdiction. Registration with the national regulator is often a foundational step towards demonstrating an organization's commitment to protecting individuals' privacy rights.

This indicator underscores the importance of regulatory compliance in safeguarding individuals' privacy rights. By ensuring that organizations register with the national regulator and maintain active registration status, stakeholders can have greater confidence in the organization's commitment to protecting personal data and complying with applicable data protection laws.

To earn a credit under this indicator, an organization must fulfill the following;

- The organization's jurisdiction must have data protection laws that mandate registration with the national regulator before collecting any personal data. This requirement may vary from one jurisdiction to another, as not all countries have mandatory registration systems.
- The organization's registration status with the national regulator must be indicated as "Active." This signifies that the organization has completed the registration process and is in compliance with the regulatory requirements.

B. Accessible Privacy Policy

The indicator assesses the extent to which organizations prioritize transparency and accountability in their data handling practices. To qualify for credit under this indicator, organizations must meet stringent criteria, ensuring that their privacy policies are readily accessible, publicly available, noticeable, and easily understandable to the general public.

A publicly available and understandable privacy policy fosters trust and accountability between organizations and their users. It demonstrates a commitment to transparency and ethical data handling practices, enhancing the organization's reputation and credibility in the eyes of stakeholders. Ultimately, organizations that fulfill the criteria earn a credit within the Privacy Scorecard report, signaling their dedication to promoting transparency, accountability, and user empowerment in the realm of data privacy.

This evaluation only involves the privacy policy and it has meet the following;

- Public and published

Organizations must have a publicly accessible privacy policy, typically hosted on their website or other prominent platforms. This policy should be easily discoverable by users seeking information about the organization's data handling practices. If it exists, then it's considered public and published

- Noticeable

The privacy policy should be prominently displayed and easily noticeable to users. Whether it's through a dedicated webpage, a link in the website footer, or incorporated into the signup process, the policy should not be hidden or difficult to find.

- Readable

The language used in the privacy policy should be clear, concise, and comprehensible to the average user. Technical jargon and legalese should be minimized, ensuring that individuals without specialized knowledge can grasp the content and implications of the policy. The Hemingway Editor will be used to evaluate the readability of the privacy policy. Only if the privacy policy scores good on the platform, it will be considered readable.

- Length

Length of the privacy policy for a company will be collected. If it's below 200 words. The company won't get a star.

C. Pre-Collection Data Transparency (Data Subject Rights)

To earn a star in this category, companies/agencies must promise to oblige with the provisions of the respective Data Protection Laws and inform users clearly at the time of collecting their data about at least:

- who your company/agency is (your contact details, and those of your DPO if any)
- why your company/agency will be using their personal data (purposes)
- the nature and category of personal data being collected
- the legal justification for processing their data;
- for how long the data will be kept;
- who else might receive it;
- that they have a right to a copy of the data (right to access personal data) and other basic rights in the field of data protection
- their right to lodge a complaint with the Regulator;
- their right to withdraw consent at any time;
- the information may be provided in writing, orally at the request of the individual when identity of that person is proven by other means, or by electronic means where appropriate. Your company/organisation must do that in a concise, transparent, intelligible and easily accessible way, in clear and plain language and free of charge.

This indicator entailed users to be furnished with the following details:

- *Company's contact details* – 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 privacy policy must mention the data subject has the right to correct personal data and the right to delete or erase personal data
- *Right to restrict or object to data processing* - The privacy policy must mention the data subject has right to restrict or object to data processing.
- *Right to withdraw consent at any time* - The privacy policy must mention the data subject has right to withdraw consent anytime

D. Third-Party data transfer

This indicator evaluates the transparency and accountability of organizations regarding the transfer of personal data to third parties. This indicator serves as a crucial measure to ensure that data subjects are informed about the sharing of their personal information and the purposes for which it is shared.

Fulfilling these criteria is imperative for organizations seeking to earn credit under the Third-party Data Transfer indicator. By providing clear and comprehensive disclosures in their privacy policies, organizations demonstrate their commitment to transparency and accountability in data handling practices. This not only empowers data subjects to make informed decisions about their personal information but also fosters trust and confidence in the organization's data processing activities.

This indicator was evaluated along the following variables:

- Third-party entities - The privacy policy should identify the third-party entities with whom the organization shares personal data. This includes any external parties, such as service providers, affiliates, or partners, involved in processing or utilizing the data.
- Specific Data Shared –
    1. Organizations must specify the types of personal data that are shared with third parties. This encompasses any information collected from data subjects that is subsequently transferred to external entities for processing or other purposes.
    2. The tech analysis will use the interception environment provided by Privacy International[1] to check what is the application or website of the company actually collecting.
    3. The result should be matched with the privacy policy to decide if there is any personal data being collected but not mentioned in the privacy policy.
    4. The data collector should collect third parties mentioned in the privacy policy
    5. The tech analysis will collect data on which trackers are on the websites and mobile application of the company (if it exists).[2]
    6. The trackers of websites will be collected with blacklight[3] website and Ghostery[4] a browser extension
    7. If the company has any applications, the trackers of the application will be collected with Exodus[5]
    8. The data collector will then locate the company that these trackers belong to with Exodus, Whotracksme and Google searches
    9. The data collector will then match the companies of these trackers with the third-parties mentioned in the companies' privacy policy. If any of the tracker companies wasn't mentioned among the third parties. The company will fail to get a star.

1 'Data Interception Environment' (Privacy International) at https://privacyinternational.org/learn/ data-interception-environment accessed 30 October 2024.
2 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 2024.
3 https://thermarkup.org/blacklight at accessed 30 October 2024.
4 https://www.ghostery.com/ at accessed 30 October 2024.
5 https://reports.exoduc-privacy.eu.org/en/ at accessed 30 October 2024.

- Purpose of Data Transfer - The privacy policy should outline the purposes for which personal data is shared with third parties. This includes detailing the reasons or objectives behind the transfer, such as for service provision, marketing activities, analytics, or any other legitimate business purposes.

D. Practice Robust Data Security

The indicator evaluates the extent to which organizations prioritize and implement robust measures to safeguard the security of data they collect and process.

To qualify for credit under this indicator, organizations must demonstrate their adherence to data security measures as mandated by the respective Data Protection Laws governing their jurisdiction. These measures typically encompass a wide array of technical, organizational, and procedural safeguards designed to protect against unauthorized access, disclosure, alteration, or destruction of personal data. Companies subject to assessment under this indicator must showcase tangible evidence of their commitment to data security, including but not limited to:

- the place or location where the personal data is stored,
- the security measures incorporated into any equipment in which the personal data are stored,
- the measures taken for ensuring the reliability, integrity and competence of the personnel having access to the personal data,
- the measures taken for ensuring the secure transmission of the personal data.

- SSL server score of the company website - The company website will be tested on Qualys SSL Labs. If a company SSL server score is lower than A, the company won't get a star.
- Privacy Policy - The privacy policy should mention how the personal data is secured.
- Security Header score of the company website - The company website will be tested on SecurityHeaders.com. If a company's security headers score is lower than A, the company won't get a star.[6]

E. Availability of Transparency Report

The indicator serves as a pivotal benchmark for evaluating the commitment of organizations to transparency in their data handling practices. To qualify for a credit under this indicator, companies must demonstrate the existence of a comprehensive report detailing the utilization and processing of personal data collected within a specified timeframe, typically a year.

This transparency report serves as a crucial tool for accountability, shedding light on how organizations manage and safeguard individuals' personal information. It outlines the specifics of how collected data is utilized internally, as well as any instances of sharing with third parties. By providing insight into data processing practices, these reports empower users to make informed decisions about their privacy and better understand the implications of sharing their personal information.

The Availability of Transparency Report indicator underscores the importance of transparency in data handling practices. Companies that fulfill this criterion not only enhance their credibility but also contribute to a more transparent and accountable digital ecosystem, where individuals' privacy rights are respected and upheld.

F. Internal Data Breach Resolution

This indicator scrutinizes an organization's privacy policy to determine if it explicitly outlines the mechanisms in place to resolve internal data breaches. To earn a credit under this indicator, the privacy policy must meet several criteria:

- Explicit Remedy Mechanisms

The organization's privacy policy should clearly articulate the steps taken to address data and privacy breaches internally. This includes outlining the procedures for reporting breaches, investigating incidents, and implementing corrective actions.

6 Security Headers https://securityheaders.com/.

- Emphasis on Impartiality

The policy should emphasize impartiality in the resolution process. This means ensuring that investigations into breaches are conducted objectively, without bias or favoritism towards any party involved.

Timely Processing

Timeliness is crucial in addressing data breaches effectively. The policy should specify reasonable timeframes for reporting, investigating, and resolving breaches to minimize the potential impact on individuals affected by the breach.

- Accessibility

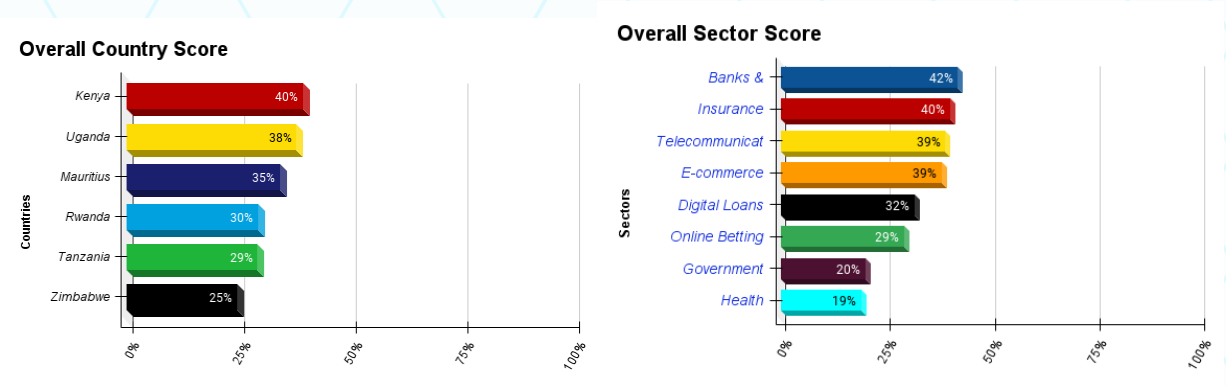
Accessibility of the resolution mechanisms is vital for ensuring that individuals can easily report breaches and seek redress. The policy should outline how individuals can access these mechanisms, whether through designated reporting channels, online platforms, or other means.

3. OVERALL *FINDINGS*

This part, presents a synthesis of the key results and insights uncovered through the assessment and analysis carried out in the preceding sections of the report. The overall findings offer a broad overview of the data collected, revealing significant trends, patterns, and relationships that contribute to a deeper understanding of the privacy policies and practices of the selected companies/entities. These findings serve as the foundation for the conclusions and recommendations that follow, providing critical context for decision-making and strategic planning. By examining these results, we gained valuable insights into the far-reaching implications, which would guide future actions and inform stakeholders of the most relevant outcomes from the assessment.

3.1 Overview of the general compliance landscape

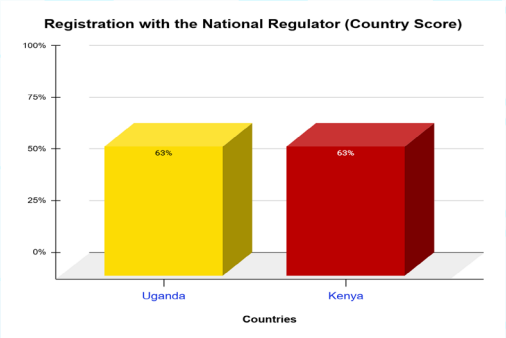
3.1.1 Overall analysis of findings at country and sector levels

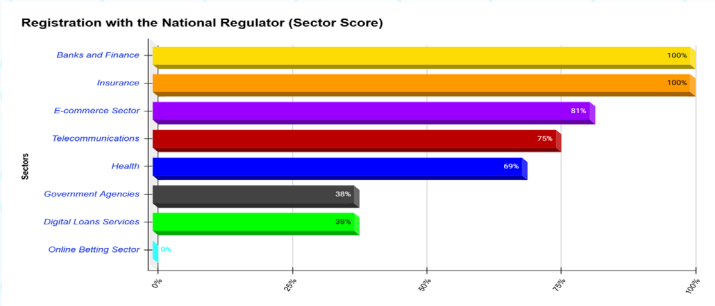


The assessment revealed that the overall index score remained below 50% at both the country and sector levels. Compared to last year's score of 47.3%, this year's overall index score was 40%, with Kenya recording the highest score. This was followed by Uganda, Mauritius, Rwanda, Tanzania, and Zimbabwe. At the sector level, the overall score was 42%, recorded by the Banks and Finance Sector, closely followed by Insurance at 40%, and a tie between Telecommunications and E-commerce at 39%. The Government and Health sectors registered the lowest scores. The figures above provide more details on the country and sector performances.

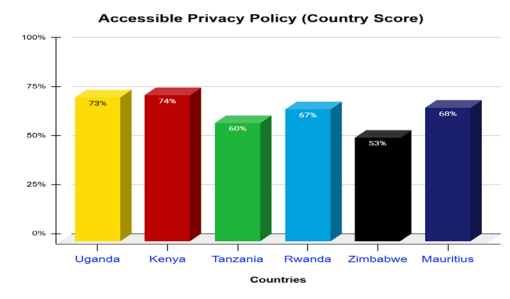
3.1.2 Overall analysis of findings against indicators at country and sector level

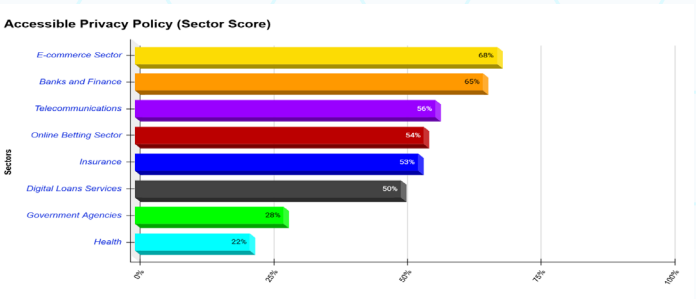
a. **Registration with the National Regulator** - At country level - Registration with National Regulator stood at 63% in both Uganda and Kenya. While, at Sector level, the highest average score was 100% registered by Banks and Finance and Insurance and the lowest average score was 0% registered by Online Betting Sector.



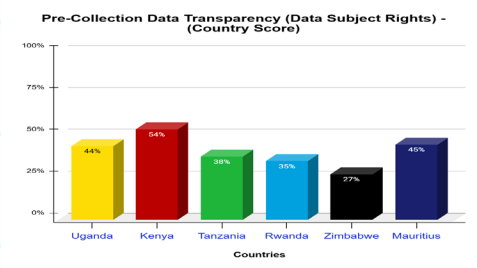


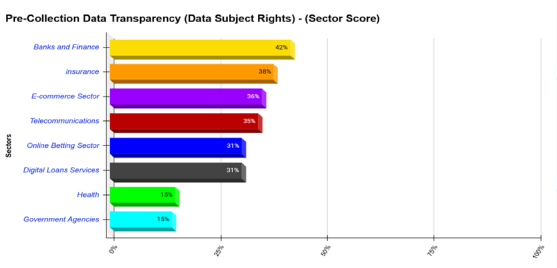
b. Accessible Privacy Policy -At country level - All the assessed countries exhibited adherence to the indicator with an average score of 50%. At Sector level – 6 out of 8 sectors demonstrated more adherence with an average score of 50% and above. Gov't Agencies and Health exhibited the lowest average.



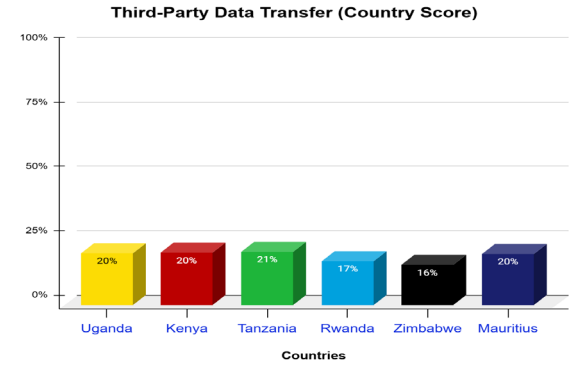


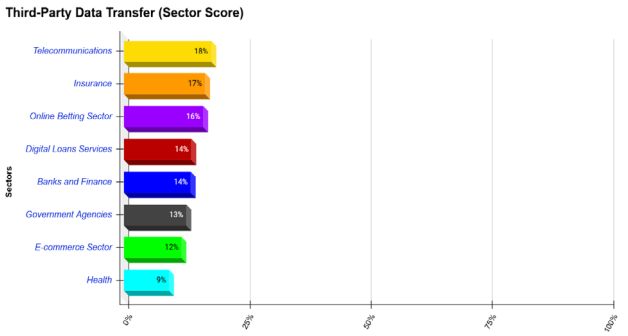
c. Pre-Collection Data Transparency - Whereas all countries demonstrated efforts to comply with the indicator, the highest average score was 54% registered by Kenya compared to last year's 59.4% though the lowest average score was 27%, this was a slight improvement compared to last year's 23.4% registered by Zimbabwe. At Sector level, Banks and Finance topped the list with 42% compared to last year's score- 61.9% registered by e-commerce. Lowest average score was 9.2% registered by e- Government Services.



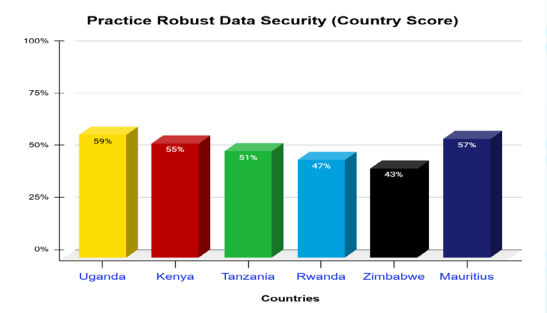


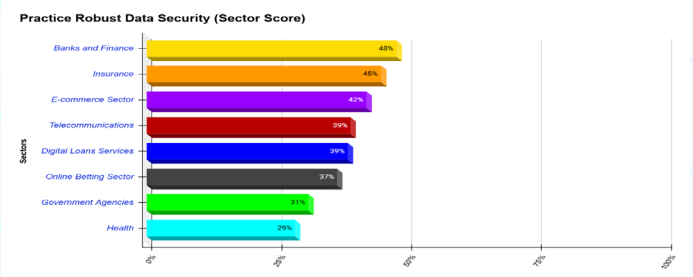
d. Third-Party Data Transfer - Both at country level and Sector level, Whereas there was demonstration of efforts to adhere with the indicator, the performance was below 50%.



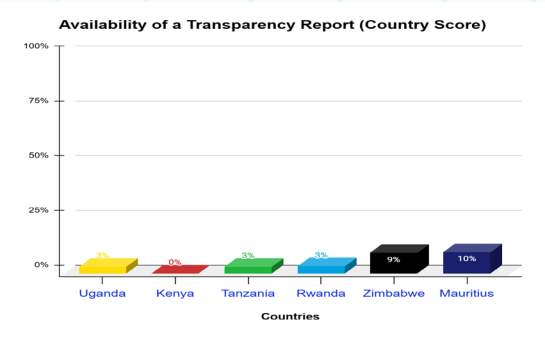


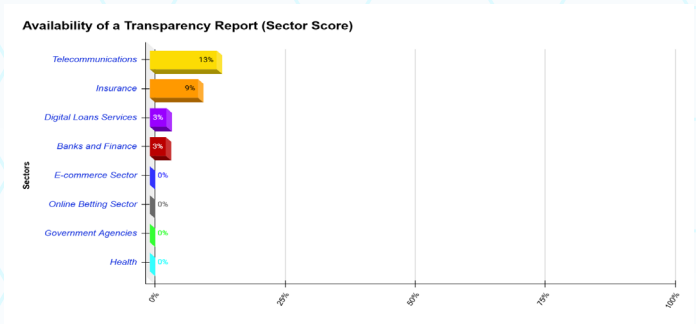
e. Practice Robust Data Security - At country level - 3 of the countries demonstrated more efforts to comply with the indicator registering - Mauritius (57%), Uganda (59%) and Kenya (55%). At Sector level – Though Banks & Finance emerged at the top, the performance for all sectors was below 50%.



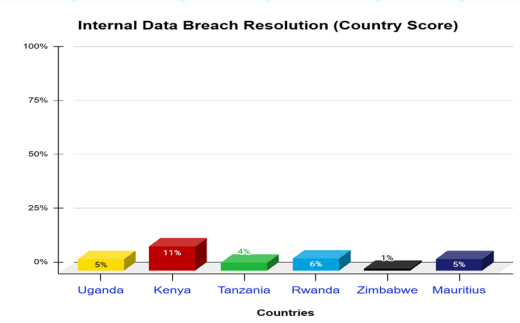


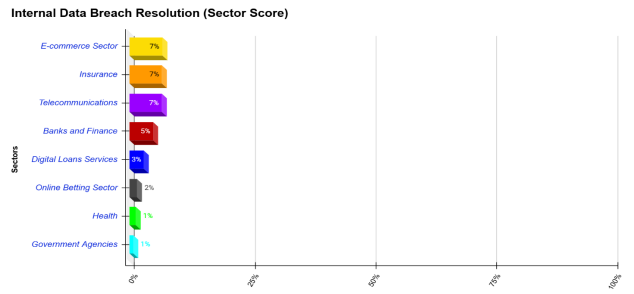
f. **Availability of a Transparency Report** - Both at country level and Sector level. Despite the noticeable efforts to comply, generally there was poor performance exhibited for this indicator.





g. **Internal Data Breach Resolution** - Both at country level & Sector level, despite the noticeable efforts to comply, generally there was poor performance exhibited for this indicator.

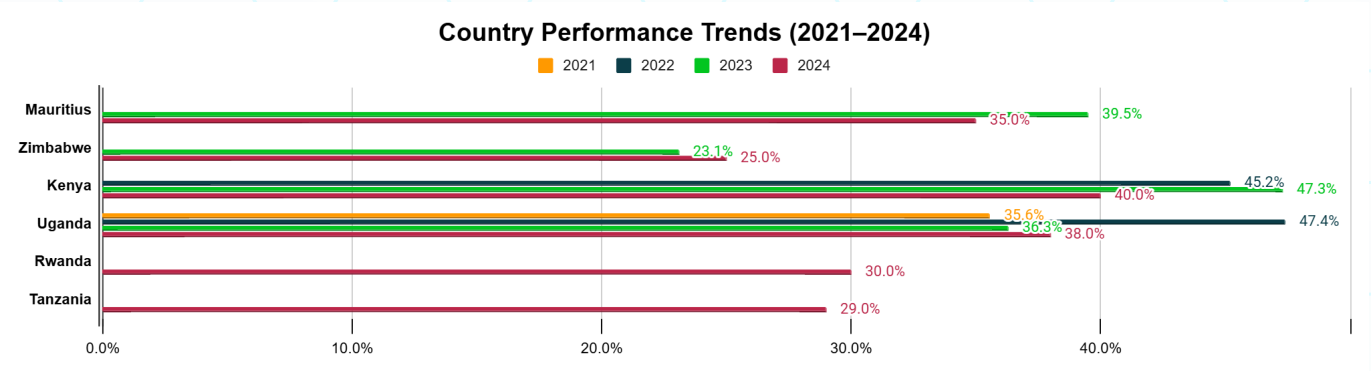




3.2 Highlights of trends/ patterns observed across sectors and countries

This section provides an overview of the key trends and patterns observed across various sectors and countries in the assessment. This analysis highlights the performance variations, identifying areas of strength and areas requiring improvement. By examining the data from both a sectoral and geographical perspective, we can gain valuable insights into the factors influencing these outcomes and better understand the broader dynamics shaping the scores across the different regions and industries.

3.2.1 Performance Trends over the years at Country Level



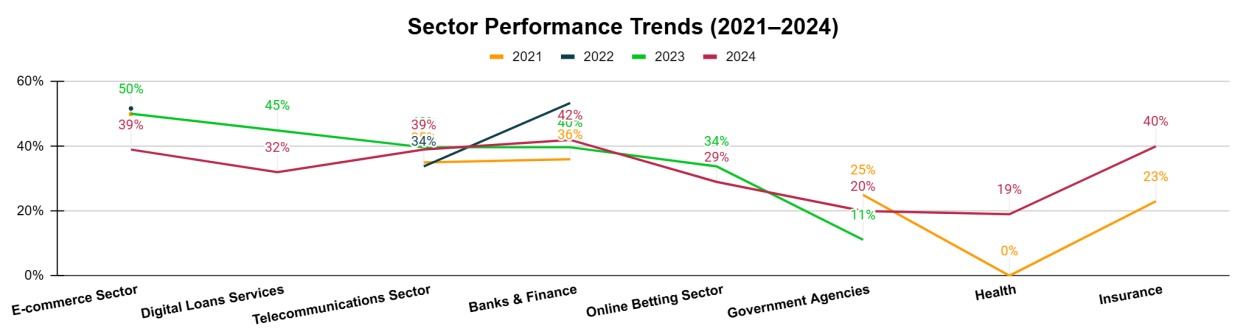
The performance of the different countries assessed over the years shows notable trends. Kenya leads with relatively high scores, peaking at 47.3% in 2023 before experiencing a slight drop to 40.0% in 2024. This decline suggests challenges in maintaining the momentum achieved with the introduction of the Data Protection Act in 2019 and potentially due to emerging data protection issues. Mauritius shows a downward trend, with its score decreasing from 39.5% in 2023 to 35.0% in 2024. strengthening or update privacy laws and regulatory frameworks, are critical for maintaining compliance with global standards. Uganda demonstrated significant improvement in 2022, reaching 47.4%, but experienced a steady decline to 36.3% in 2023 and 38.0% in 2024, reflecting difficulties in sustaining progress and issues with enforcement or implementation of data protection regulations.

In contrast, Zimbabwe remains at the bottom of the spectrum with very low scores—23.1% in 2023 and 25.0% in 2024. These scores suggest substantial gaps in data protection laws and enforcement mechanisms, leaving the country vulnerable to privacy violations. Rwanda that is featuring for the first time in the score card report, also faces challenges, with a score of just 30.0% in 2024, signaling that it is in the early stages of establishing a robust data protection framework. Despite its success in other governance areas, Rwanda struggles to implement effective privacy practices. Tanzania also featuring for the first time in in the assessment, performs similarly to Zimbabwe, with the lowest score of 29.0% in 2024, reflecting significant deficiencies in its data protection laws and regulatory oversight.

Overall, while Kenya stands out as the leader in data protection practices, many other countries, including Mauritius, Uganda, Rwanda, and Tanzania, face difficulties in strengthening or maintaining their data protection frameworks. Zimbabwe, in particular, requires significant efforts to develop foundational data protection laws. These countries need to focus on enhancing regulatory enforcement, updating privacy laws, and ensuring that their frameworks are aligned with international standards to improve their scores and foster greater trust in data privacy.

3.2.2 Performance Trends over the years at Sector Level

The performance of various sectors over the past few years highlights both improvements and ongoing challenges.



The E-commerce sector, with scores of 39% in 2024, 50% in 2023, 52% in 2022, and 50% in 2021, shows a slight decline, indicating a drop in the sector's ability to maintain strong privacy protections despite initially better performance. This decline might suggest the growing challenges e-commerce platforms face in safeguarding customer data amid rapid growth and evolving cyber threats. The Digital Loans sector saw a significant decrease from 44.9% in 2023 to 32% in 2024, reflecting a sharp deterioration in privacy practices, possibly due to inadequate security measures, lack of regulation, or misuse of sensitive customer data in this rapidly expanding sector. The Telecommunications sector remained relatively stable, with minor fluctuations, scoring 39% in 2024 and 39.7% in 2023, compared to 33.8% in 2022 and 35% in 2021. This sector has improved over time but still faces significant gaps in data protection, potentially due to the vast volumes of personal data it handles and emerging security risks.

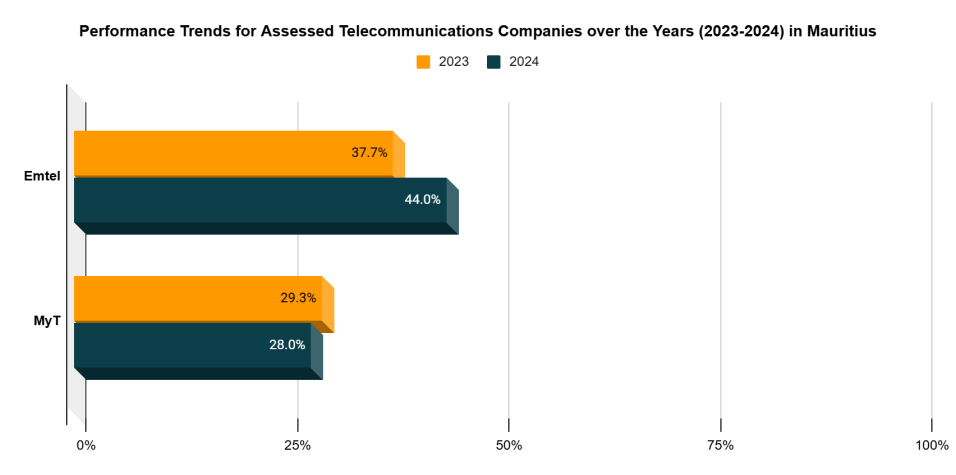
The Banks & Finance sector showed a decline from 53% in 2022 to 29% in 2024, after scoring 39.7% in 2023, signaling significant setbacks in data privacy compliance. This sharp drop could indicate increasing challenges in securing financial data, evolving regulatory landscapes, or failures in addressing consumer privacy concerns, especially in light of growing cyber risks. Online Betting, with scores of 29% in both 2024 and 2023, also struggles to improve its privacy practices, signaling that this sector, dealing with financial transactions and personal data, remains underregulated and vulnerable to data privacy issues. Government agencies continue to lag behind, with a score of just 20% in 2024, a slight improvement from 11.1% in 2023 but still far from adequate. These low scores indicate poor data handling practices and weak enforcement of data protection laws, raising concerns about citizen privacy and trust in government operations.

The Health sector showed the most concerning performance, with a score of just 19% in 2024, down from 0% in 2021, although the sector is making some progress. However, the low score still suggests serious issues with data security and compliance, particularly as health data is a prime target for cyberattacks. The Insurance sector, on the other hand, improved from 23% in 2021 to 40% in 2024, indicating a positive trend in data protection practices. However, there is still significant room for improvement, especially in securing customer data and ensuring compliance with evolving privacy regulations. Overall, while some sectors like Banks & Finance and Insurance show positive movement, many others, particularly e-commerce, Digital Loans, e-Government, and Health, face substantial challenges and must urgently address privacy and data protection shortcomings to build trust and comply with regulatory standards.

3.2.3 Performance Trends of Assessed Companies/entities Across the Years

This section provides an analysis of the performance trends of the companies/ entities assessed over the years, from 2021-2024. By examining historical data and performance metrics, this section aims to identify patterns, strengths, and areas for improvement, offering a clear picture of how these companies have evolved over time. This analysis will provide valuable insights into the factors driving compliance or challenges, contributing to informed decision-making and strategic planning for the future.

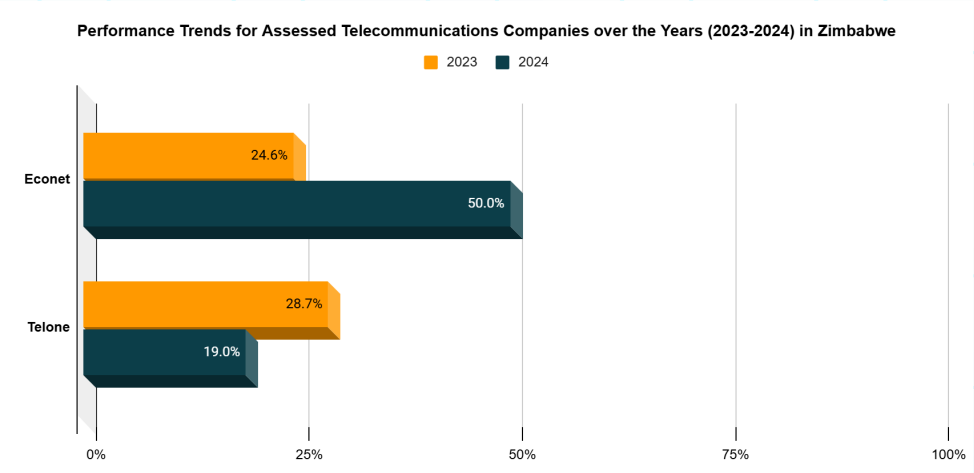
i. Trends in performance of assessed companies/entities over time in Telecommunication Sector



In 2024, Emtel scored 44.0%, showing an improvement from 37.7% in 2023. This upward trend suggests that Emtel has made progress in enhancing its data protection practices, possibly through better implementation of privacy measures, security protocols, or improvements in regulatory compliance. However, despite the improvement, there is still room for further progress to meet higher global standards for privacy and data protection.

On the other hand, MyT scored 28.0% in 2024, a slight decline from 29.3% in 2023. This decline could indicate challenges in strengthening its privacy frameworks or addressing data security concerns. The drop in performance suggests that MyT may be facing difficulties in keeping pace with evolving regulatory demands or in addressing issues such as consumer data security or compliance with data protection laws. Overall, Emtel appears to be making positive strides in improving its privacy practices, while MyT needs to address the setbacks in its performance and prioritize stronger data protection measures to avoid further declines in its compliance.

Both companies should continue to invest in enhancing their data protection strategies to safeguard user privacy and ensure compliance with evolving global standards.

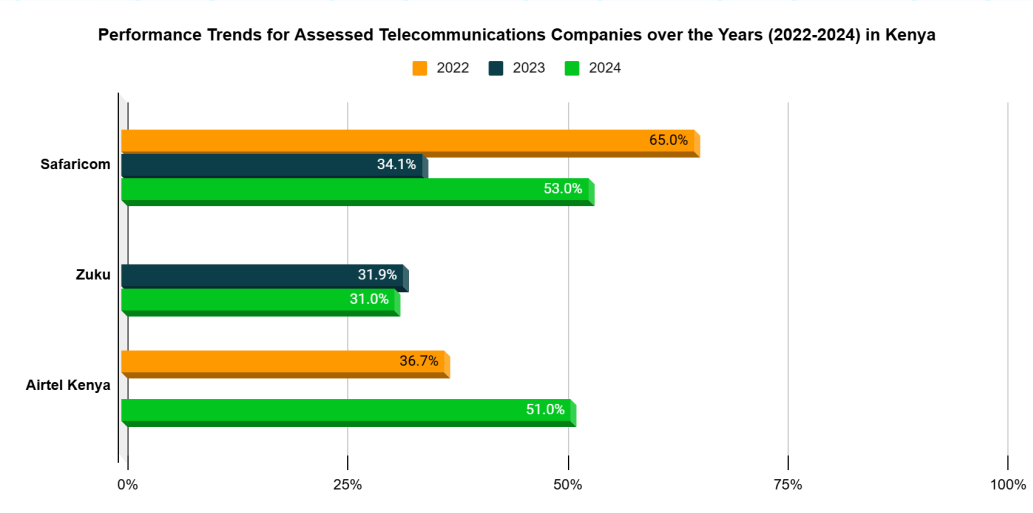


The performance of Econet and Telone over the past two years shows stark differences in their approaches and outcomes. Econet has shown significant improvement, increasing from 24.6% in 2023 to 50.0% in 2024. This upward trend suggests that the company has made notable strides in enhancing its data protection practices, possibly by improving compliance with data protection laws, implementing stronger security measures, and refining privacy policies. The 50% score in 2024

indicates a solid commitment to safeguarding customer data, though there is still room for further improvement to meet higher international privacy standards.

In contrast, Telone has experienced a decline in performance, dropping from 28.7% in 2023 to 19.0% in 2024. This significant drop signals potential challenges in maintaining or improving data protection practices. It could reflect issues such as insufficient investment in privacy frameworks, inadequate regulatory compliance, or emerging data security risks. The low score suggests that Telone needs to urgently address these gaps to protect customer data and ensure alignment with regulatory expectations.

In conclusion, Econet has made considerable progress in improving its privacy and data protection practices, while Telone faces setbacks and must take immediate action to enhance its data protection framework. Both companies must prioritize data security, compliance, and transparency to improve their privacy scores and foster greater trust among customers.

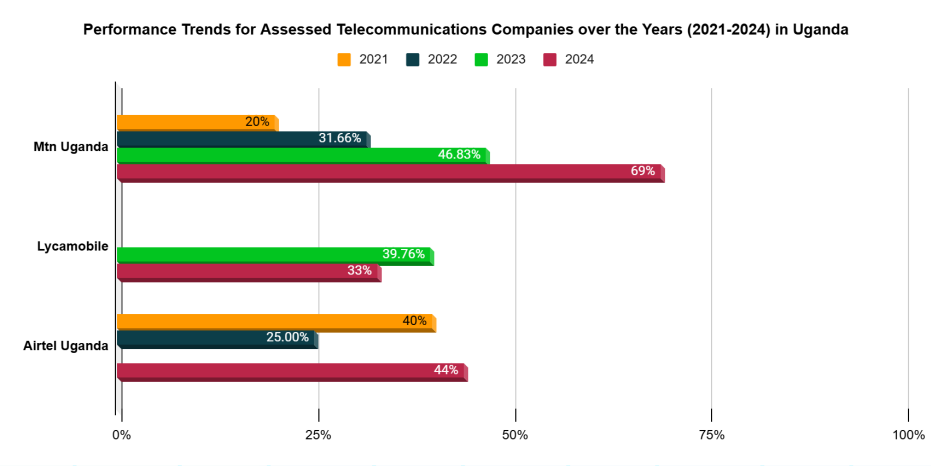


The performance of Safaricom, Zuku, and Airtel Kenya reveals significant variations in their approaches and outcomes over the past few years. Safaricom has shown notable improvement, increasing from 34.1% in 2023 to 53.0% in 2024, after a peak of 65.0% in 2022. While there is a slight dip from 2022, the company has made substantial progress since 2023, suggesting ongoing efforts to enhance its data protection frameworks. Safaricom's high score in 2022 and continued improvement in 2024 reflect a strong commitment to privacy and data security, which is crucial given the large volume of personal and financial data it handles. However, the slight decline from 2022 to 2024 might suggest some challenges or regulatory hurdles that could have affected its overall performance.

Zuku has maintained a relatively stable but low score, scoring 31.0% in 2024 and 31.9% in 2023. The score indicates that Zuku has not significantly improved its privacy practices or data protection compliance over the past two years. Despite this stability, the low score suggests that Zuku faces challenges in addressing privacy concerns, possibly due to insufficient investments in data security or compliance with evolving data protection laws. There is a clear need for the company to focus on strengthening its privacy and security measures to protect customer data and meet regulatory standards.

Airtel Kenya has made significant strides, improving from 36.7% in 2022 to 51.0% in 2024, reflecting a clear upward trend in its privacy and data protection practices. The growth in its score suggests that Airtel Kenya is addressing gaps in its data protection framework and making efforts to align with best practices. This improvement is a positive sign for the company's commitment to safeguarding user data, but continued focus on enhancing security protocols and ensuring compliance with privacy regulations will be essential to maintain and build on this progress.

In conclusion, Safaricom shows strong performance with some fluctuations, indicating ongoing efforts but also some challenges. Airtel Kenya is improving steadily, while Zuku needs to make significant improvements in its privacy practices to match the efforts of its competitors. Each company must prioritize data protection and compliance to stay competitive and ensure user trust.



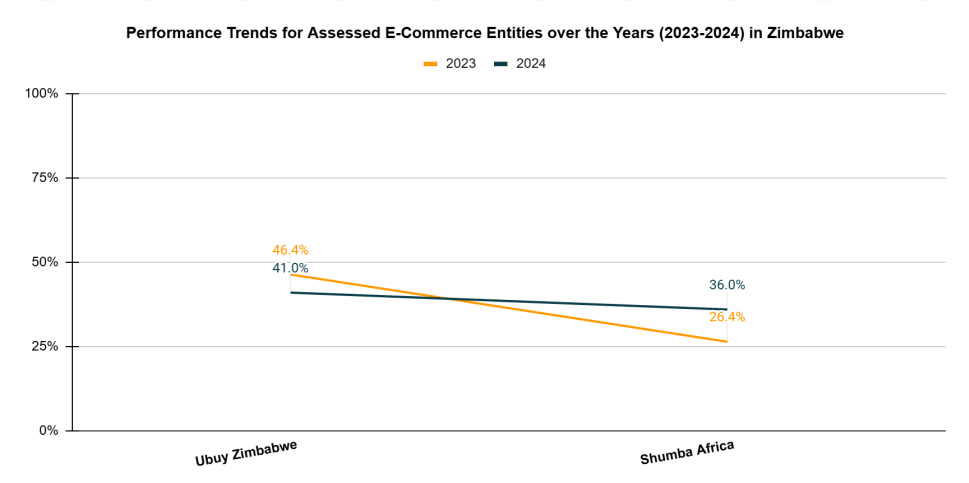
The performance of MTN Uganda, Lycamobile, and Airtel Uganda over the past few years reveals differing trends, with some companies showing significant improvement while others face challenges in enhancing their data protection frameworks. MTN Uganda has shown a marked improvement in its privacy and data protection performance, with a substantial rise from 20% in 2021 to 69% in 2024. This significant progress indicates that MTN Uganda has likely invested in strengthening its data protection policies, improving compliance with privacy regulations, and enhancing user data security. The increase from 46.83% in 2023 to 69% in 2024 suggests that MTN Uganda has focused on addressing previous shortcomings and is now better equipped to handle sensitive user information in line with regulatory requirements.

Lycamobile has experienced a decline in its score, dropping from 39.76% in 2023 to 33% in 2024. This decrease could reflect challenges in maintaining or improving its data protection practices, which might include issues such as inadequate implementation of privacy regulations, lack of security infrastructure, or ineffective compliance with local data protection laws. The decline signals that Lycamobile needs to address privacy and security concerns urgently to avoid further deterioration in compliance.

Airtel Uganda shows a positive trend, improving from 25% in 2022 to 44% in 2024. While the company's score has not reached the high levels of MTN Uganda, it demonstrates consistent progress in improving its privacy practices and data protection efforts. However, Airtel Uganda still has room for improvement to align with global standards, especially considering its competitors like MTN Uganda have made more significant strides.

Overall, MTN Uganda stands out with the most impressive progress, while Lycamobile needs to address its decline in data protection compliance. Airtel Uganda, though improving, should continue enhancing its data security measures to remain competitive and align with best practices in the industry. Each company must prioritize strengthening their data protection frameworks to ensure compliance with privacy regulations and safeguard user trust.

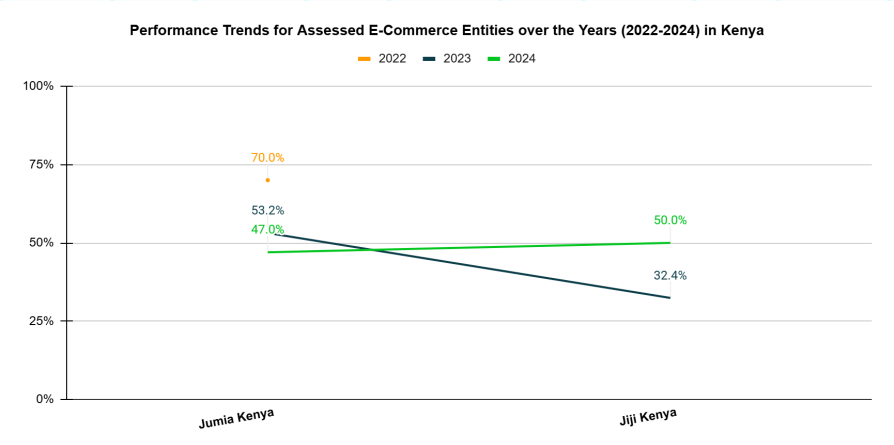
ii. Trends in performance of assessed companies/entities over time in the e-Commerce Sector



The performance of Ubuy Zimbabwe and Shumba Africa shows contrasting trends over the past two year. Ubuy Zimbabwe scored 41.0% in 2024, which reflects a slight decline from 46.4% in 2023. While this decrease suggests that Ubuy Zimbabwe may have encountered challenges in maintaining its previous improvements, it still maintains a relatively solid score in comparison to other sectors. The decline could be attributed to issues such as increased regulatory pressure, the need for stronger data security measures, or evolving privacy concerns. However, the company is still performing better than many of its peers, indicating that it has foundational data protection measures in place but may need to enhance them to stay compliant and secure.

Shumba Africa, on the other hand, saw a notable improvement, jumping from 26.4% in 2023 to 36.0% in 2024. This upward trend suggests that the company has made significant efforts to improve its data protection practices, possibly by addressing gaps in privacy policies, enhancing security protocols, and ensuring better compliance with data protection laws. However, the company still lags behind Ubuy Zimbabwe, indicating that there is further room for improvement in aligning with best practices and strengthening its data protection frameworks.

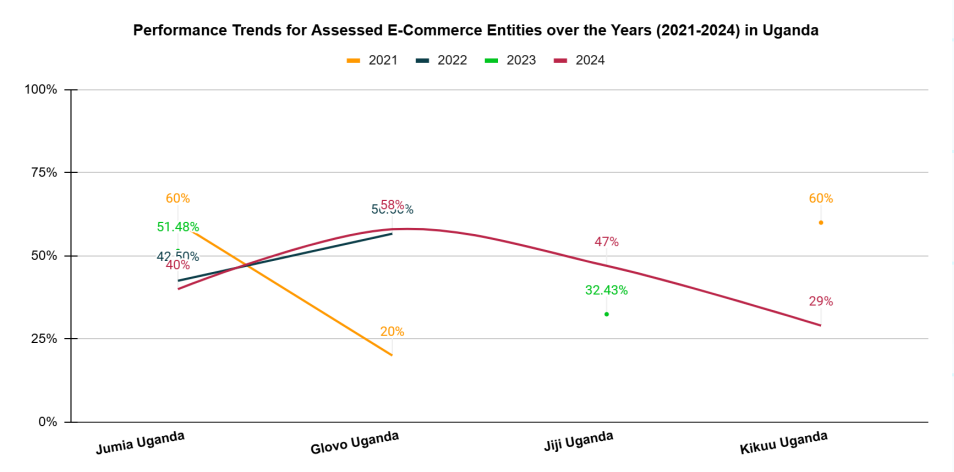
In summary, Ubuy Zimbabwe has seen a minor decline but still maintains a strong performance compared to other companies, while Shumba Africa has made substantial progress in improving its data protection practices. Both companies need to continue focusing on strengthening their privacy measures and compliance to ensure they are aligned with evolving regulatory standards and effectively protect customer data.



The performance of Jumia Kenya and Jiji Kenya over the past few years reveals important trends in their approach to safeguarding customer data. Jumia Kenya scored 47.0% in 2024, showing a decline from 53.2% in 2023 and 70.0% in 2022. This steady decrease in performance suggests that Jumia Kenya has faced challenges in maintaining its previous high standards of privacy protection. The decline could indicate issues such as evolving regulatory requirements, security breaches, or difficulties in consistently implementing strong privacy measures. Despite the decline, Jumia Kenya remains at a relatively moderate level of compliance, but it will need to address the factors contributing to the drop to restore its previous levels of performance and better protect consumer data.

In contrast, Jiji Kenya experienced a dramatic improvement, rising from 32.4% in 2023 to 50.0% in 2024. This significant increase suggests that the company has made substantial efforts to enhance its data protection practices over the past year, possibly through improved compliance measures, stronger security protocols, or better privacy policies. While Jiji Kenya still lags behind Jumia Kenya, the notable improvement in its score reflects progress in aligning with data protection regulations and improving its privacy framework.

In sum, Jumia Kenya has seen a decline in its privacy practices, signaling the need for better data security measures and more consistent compliance efforts, while Jiji Kenya has made notable progress in improving its data protection and privacy practices. Both companies should focus on addressing their respective challenges to improve their data protection measures and maintain customer trust.



The performance of Jumia Uganda, Glovo Uganda, Jiji Uganda, and Kikuu Uganda over the past few years reveals varying trends, with some companies showing improvements while others face setbacks.

Jumia Uganda scored 40% in 2024, reflecting a significant decline from 51.48% in 2023 and a slight drop from 42.50% in 2022. This downward trend suggests that Jumia Uganda has encountered challenges in maintaining its data protection measures over the years, possibly due to regulatory changes, security lapses, or insufficient investment in privacy protections. Despite the decline, Jumia Uganda remains relatively moderate in its compliance, but this trend signals the need for greater efforts to stabilize and improve its privacy practices.

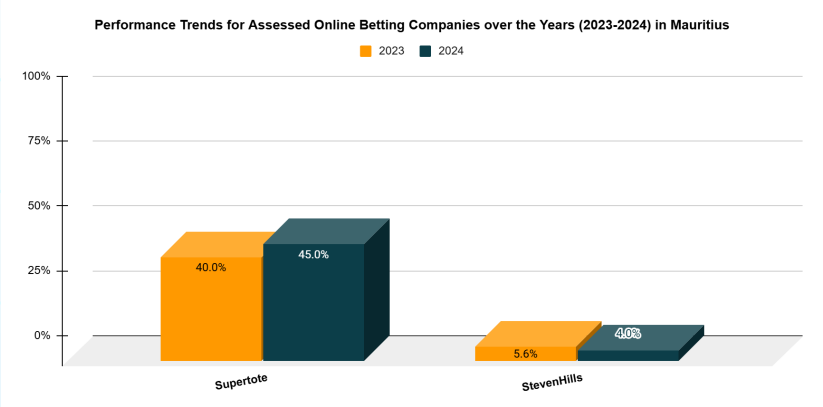
Glovo Uganda, on the other hand, shows an improvement, with a score of 58% in 2024, up from 56.66% in 2022 (no data for 2023). This positive trend indicates that Glovo Uganda has focused on strengthening its data protection measures and aligning with privacy regulations. The 58% score suggests a solid commitment to safeguarding user data, though there is still room for improvement to fully comply with international privacy standards.

Jiji Uganda shows an increase from 32.43% in 2023 to 47% in 2024, reflecting progress in improving its data protection practices. The steady improvement in its score indicates that Jiji Uganda has made efforts to address privacy gaps, enhance security measures, and comply better with regulatory requirements. While it still has work to do to reach higher levels of compliance, this upward trend is a positive sign for the company's commitment to improving data privacy.

Kikuu Uganda scored 29% in 2024, down from 60% in 2021 (no data for 2022 and 2023). This significant decline raises concerns about the company's ability to maintain effective privacy practices and data protection compliance over time. The drop in score suggests that Kikuu Uganda has faced challenges in keeping up with evolving data protection regulations or strengthening its security measures, which may put customer data at risk. Urgent action is required to improve its privacy practices and restore consumer trust.

In conclusion, Glovo Uganda has shown consistent improvement in its privacy practices, while Jiji Uganda is also progressing steadily. However, Jumia Uganda and Kikuu Uganda are facing challenges, with Jumia Uganda experiencing a decline and Kikuu Uganda showing a sharp drop in performance. These companies must focus on addressing the gaps in their data protection frameworks, investing in stronger security measures, and ensuring compliance with privacy regulations to enhance customer trust and align with global standards.

iii. Trends in performance of assessed companies/entities over time in the Online Betting Sector



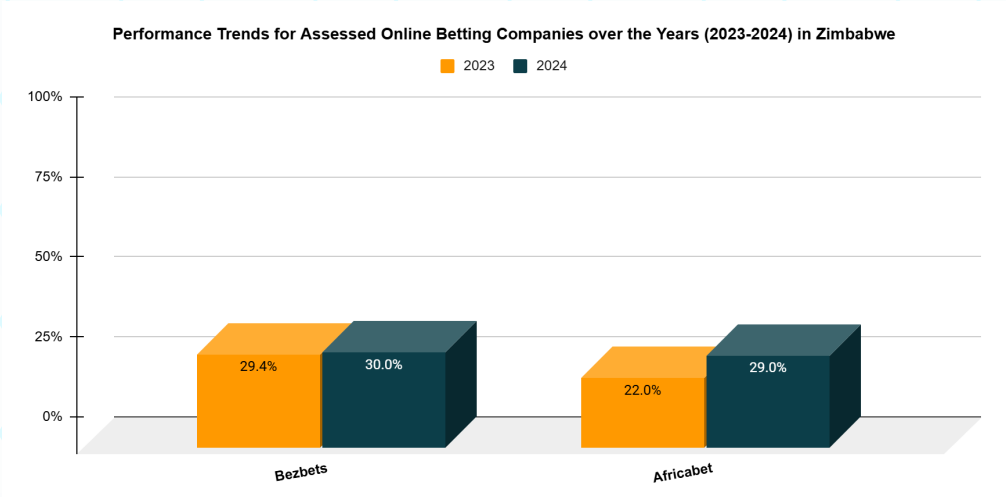
The performance of Supertote and StevenHills over the past two years presents a clear contrast in their efforts. Supertote has shown a moderate improvement, increasing from 40.0% in 2023 to 45.0% in 2024.

This upward trend suggests that the company has made some strides in enhancing its data protection measures and improving compliance with privacy regulations.

Although the increase is modest, it reflects a positive direction in strengthening privacy practices and safeguarding customer data. However, there is still room for further improvement, especially to align with best practices in the industry and meet evolving regulatory standards.

StevenHills, on the other hand, shows minimal improvement, with a score of just 4.0% in 2024, up slightly from 5.6% in 2023. This very low score indicates that StevenHills has made little to no progress in improving its privacy practices and data protection compliance. The company's performance suggests significant gaps in its data protection framework, which could expose customer data to risks and highlight the need for urgent action. It is critical for StevenHills to address these issues by implementing stronger security measures, improving its compliance with data protection laws, and ensuring better management of customer data.

In sum, while Supertote has made some progress, StevenHills is facing serious challenges in achieving even basic compliance with privacy standards. Both companies need to prioritize improvements in their data protection frameworks, but StevenHills, in particular, must urgently take steps to enhance its privacy practices and align with regulatory requirements to protect user data.

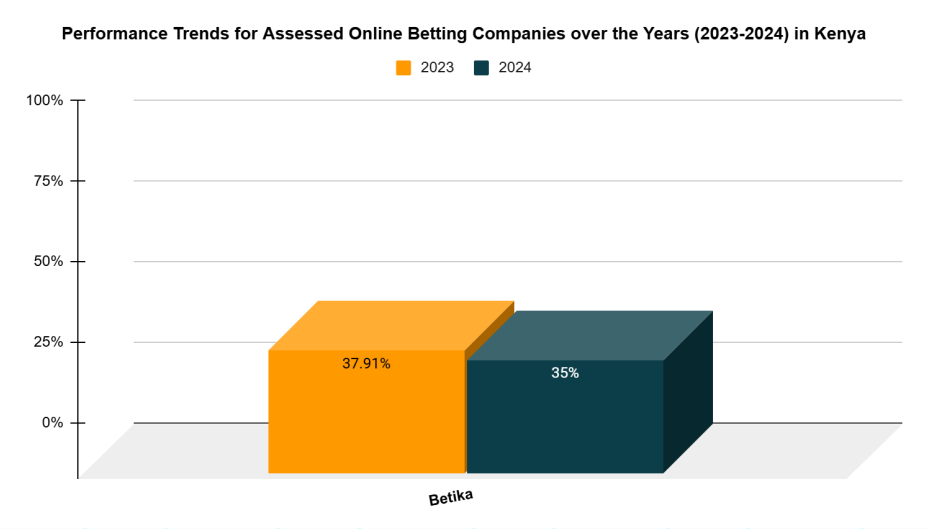


The performance of Bezbets and Africabet over the past two years shows slight improvements, though both companies still have significant room for enhancement. Bezbets scored 30.0% in 2024, which represents a small improvement from 29.4% in 2023.

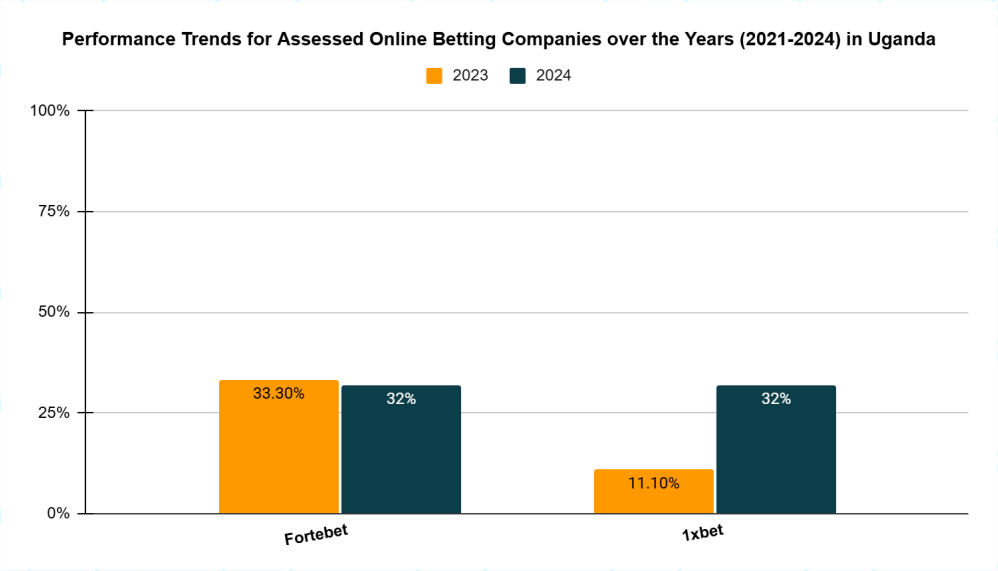
This indicates that the company has made minor progress in its data protection practices and compliance with privacy regulations. However, the overall score remains relatively low, suggesting that Bezbets still faces challenges in strengthening its data protection measures, addressing security concerns, and aligning with evolving regulatory standards. The company must invest more in privacy frameworks and security protocols to ensure better protection of customer data.

Africabet also showed progress, with a score of 29.0% in 2024, up from 22.0% in 2023. While the improvement is noticeable, Africabet still faces significant gaps in its privacy practices. The score remains low, indicating that while the company has taken steps toward improving data protection, it has not made enough advancements to bring its compliance level in line with industry best practices. Stronger measures need to be implemented to enhance security and privacy protection.

In sum, both Bezbets and Africabet show some positive movement in their data protection efforts, but their scores remain low, indicating that there is much more to be done to strengthen their privacy practices and ensure compliance with data protection laws. Both companies need to prioritize further improvements in their data security frameworks to better safeguard customer information and align with global standards.



The performance of Betika has slightly declined over the past year, from 37.91% in 2023 to 35% in 2024. This decrease, while not drastic, suggests that the company may have faced challenges in maintaining or improving its data protection measures. The decline could be due to factors such as evolving regulatory requirements, insufficient investment in privacy enhancements, or potential security concerns. Despite the drop, Betika is still operating at a moderate level of compliance, but it will need to address any weaknesses in its privacy practices to ensure better protection of customer data and to align with evolving data protection standards. Moving forward, Betika should prioritize strengthening its data security infrastructure to improve its privacy score and ensure greater regulatory compliance.

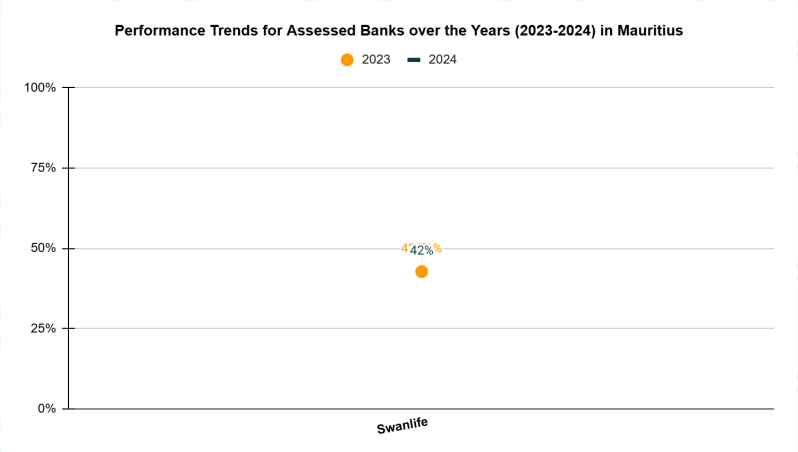


The performance of Fortebet and 1xbet reveals differing trends over the past two years. Fortebet scored 32% in 2024, showing a slight decline from 33.30% in 2023. This small drop suggests that while the company has maintained a relatively stable level of privacy compliance, it may not have made significant strides in improving its data protection measures over the past year. The company should focus on strengthening its data security protocols and compliance efforts to ensure better protection of customer data and align with evolving privacy regulations.

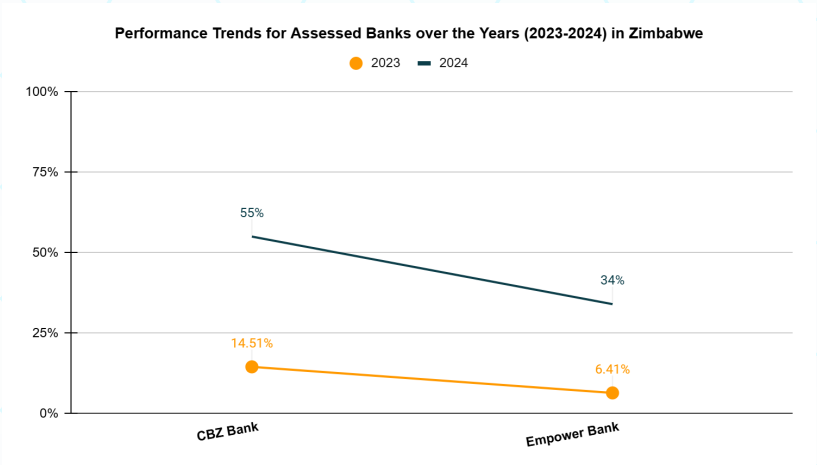
1xbet, however, saw a significant improvement, rising from 11.10% in 2023 to 32% in 2024. This notable increase indicates that 1xbet has made significant progress in addressing privacy gaps and improving its data protection practices. The rise in its score reflects efforts to enhance its compliance with data protection laws and strengthen security measures, although there is still room for improvement to align with best practices in the industry.

In sum, while Fortebet shows a minor decline, 1xbet has demonstrated substantial progress in improving its privacy practices. Both companies still have room to enhance their data protection efforts further, but 1xbet's improvement suggests that it is on the right track in prioritizing data security and regulatory compliance. Fortebet should take note of this progress and work towards similar advancements to strengthen its own data protection measures.

iv. Trends in performance of assessed companies/entities over time in the Banks and Finance Sector



The performance of Swanlife has remained relatively stable, with a score of 42% in 2024 compared to 42.71% in 2023. This slight decrease indicates that Swanlife has maintained a consistent level of compliance with data protection regulations over the past year. While the minor decline is not concerning, it also suggests that there has been no significant improvement in their privacy practices. To enhance their standing, Swanlife could focus on strengthening their data security measures, ensuring compliance with evolving privacy laws, and addressing any potential gaps in their data protection framework. Sustaining or improving this score will be essential for maintaining customer trust and regulatory compliance.

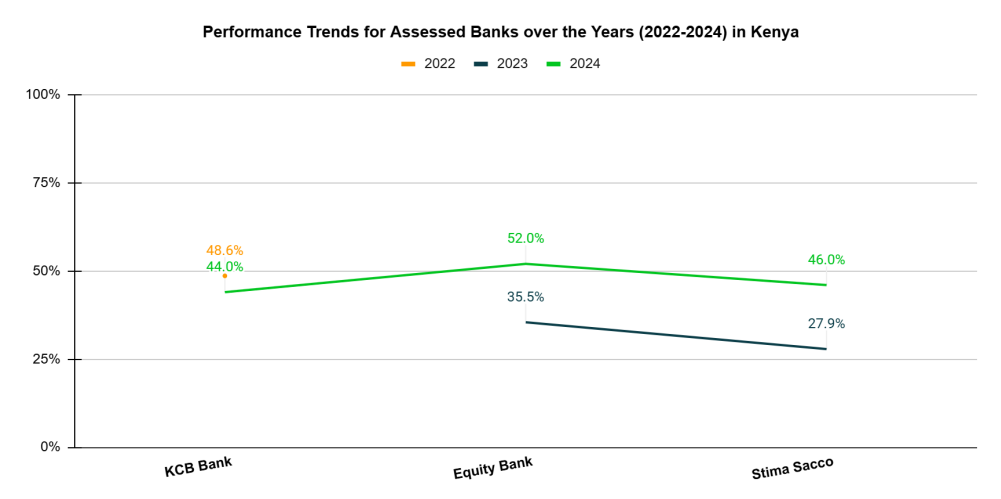


The performance of CBZ Bank and Empower Bank shows notable improvements, particularly for CBZ Bank, while Empower Bank has made some progress but remains at a relatively low level of compliance. CBZ Bank saw a substantial increase in its score, from 14.51% in 2023 to 55% in 2024.

This significant improvement suggests that the bank has made considerable efforts to enhance its data protection frameworks, comply with privacy regulations, and strengthen its security measures. The rise reflects a commitment to safeguarding customer data, but there is still room for further improvement to align with industry best practices and ensure continued compliance with evolving regulatory requirements.

Empower Bank, while showing progress, only increased slightly from 6.41% in 2023 to 34% in 2024. Although this marks an improvement, Empower Bank still faces significant challenges in meeting privacy standards and implementing strong data protection measures. The score suggests that the bank has taken some initial steps to address data privacy concerns, but there is still a significant gap between its current performance and global best practices. Continued efforts will be required to strengthen its privacy and security protocols.

In conclusion, CBZ Bank has made a strong improvement, signaling a robust commitment to data protection, while Empower Bank has made some progress but needs to accelerate its efforts to enhance privacy practices and align with regulatory standards. Both banks should continue to focus on strengthening their data protection frameworks to ensure better safeguarding of customer data and regulatory compliance.



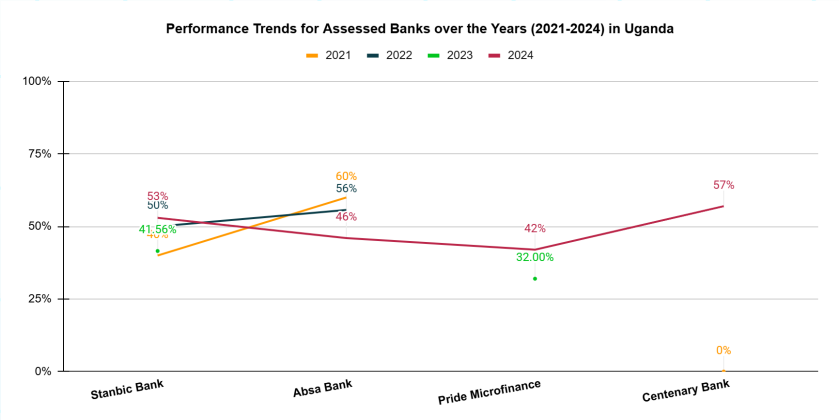
The performance of KCB Bank, Equity Bank, and Stima Sacco over the past few years reveals varying trends in their efforts to safeguard customer data.

KCB Bank scored 44.0% in 2024, indicating a slight decline from its performance in 2022, when it scored 48.6%. Although this represents a small dip, KCB Bank has still maintained a relatively strong level of data protection compliance compared to many of its peers. The drop may suggest challenges in consistently improving its data protection frameworks or responding to evolving regulatory requirements, but overall, the score remains positive, and further efforts can help the bank strengthen its privacy practices.

Equity Bank saw a significant improvement, with its score rising to 52.0% in 2024 from 35.5% in 2023. This upward trend demonstrates that Equity Bank has made considerable strides in enhancing its privacy and data protection practices. The increase suggests that the bank has taken important steps to comply with privacy regulations, implement stronger security measures, and address gaps in its data protection framework. While there is still room for further improvement, the progress is a positive sign of the bank's commitment to safeguarding customer data.

Stima Sacco also experienced an improvement, with its score rising to 46.0% in 2024 from 27.9% in 2023. This increase suggests that Stima Sacco has made meaningful efforts to strengthen its data protection measures and improve compliance with privacy laws. The score indicates that the Sacco is moving in the right direction, but like the other institutions, further improvements will be necessary to reach higher standards of data protection and align with best practices.

In conclusion, Equity Bank has shown the most significant improvement, demonstrating a strong commitment to enhancing its privacy practices. Stima Sacco has also made progress, while KCB Bank has experienced a slight decline but remains relatively stable. All three institutions should continue investing in improving their data protection frameworks to ensure compliance with evolving privacy regulations and build stronger customer trust.



The performance of Stanbic Bank, Absa Bank, Pride Microfinance, and Centenary Bank over the past few years shows both improvements and fluctuations, reflecting varied levels of commitment to safeguarding customer data. Stanbic Bank has shown a significant improvement, increasing its score from 41.56% in 2023 to 53% in 2024. This upward trend suggests that the bank has made notable strides in strengthening its privacy and data protection practices. Although it saw a decline from 50% in 2022, the increase in 2024 indicates that Stanbic Bank is actively working on enhancing its compliance with privacy regulations and security measures, moving closer to aligning with best practices.

Absa Bank scored 46% in 2024, slightly down from 55.70% in 2022 (no data for 2023). While there is a decline in performance, Absa Bank remains at a relatively moderate level of compliance with privacy and data protection standards. The decrease might reflect challenges in maintaining or improving its data protection measures, but it still demonstrates a solid commitment to safeguarding customer information.

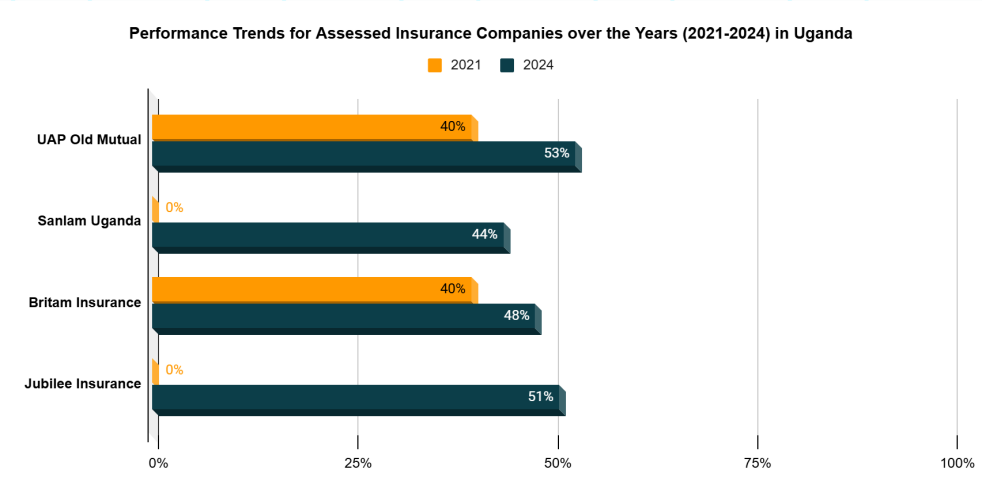
Pride Microfinance scored 42% in 2024, showing an improvement from 32% in 2023. This positive shift indicates that Pride Microfinance has taken steps to enhance its data protection framework and improve its compliance with privacy regulations. While still at a moderate level, the progress shows that the microfinance institution is focusing on strengthening its privacy measures, although further improvements are necessary to reach higher standards.

Centenary Bank scored 57% in 2024, the highest among the four institutions, reflecting a significant improvement from its previous score of 0% in 2021 (no data for 2022 and 2023). This dramatic rise indicates that Centenary Bank has made considerable progress in addressing privacy and data protection gaps, demonstrating a strong commitment to aligning with data protection laws and implementing effective security measures. However, continuous efforts are needed to ensure ongoing compliance and improve further.

In conclusion, Centenary Bank stands out with the most remarkable improvement, showing a strong commitment to data protection. Stanbic Bank has also made significant progress, while Absa Bank and Pride Microfinance show mixed results. Absa Bank needs to address the decline in performance, while Pride Microfinance is on the right track with its improvement. All institutions should continue to prioritize strengthening their data protection frameworks to ensure better customer privacy and compliance with evolving regulatory standards.

v. Trends in performance of assessed companies/entities over time in the Insurance Sector

The performance of UAP Old Mutual, Sanlam Uganda, Britam Insurance, and Jubilee Insurance shows significant improvements, with some companies making notable strides in strengthening their data protection frameworks. UAP Old Mutual scored 53% in 2024, showing a considerable improvement from 40% in 2021. This increase reflects a strong effort by the company to enhance its privacy practices and compliance with data protection regulations. The solid score indicates that UAP Old Mutual has successfully strengthened its data security measures, though there is still room to improve to align with industry best practices.



Sanlam Uganda scored 44% in 2024, a dramatic improvement from 0% in 2021. This remarkable increase demonstrates that Sanlam Uganda has made substantial progress in addressing its data protection gaps and aligning with privacy regulations. The rise in its score highlights the company's commitment to improving its privacy framework, but it should continue to focus on refining its practices to meet higher compliance standards.

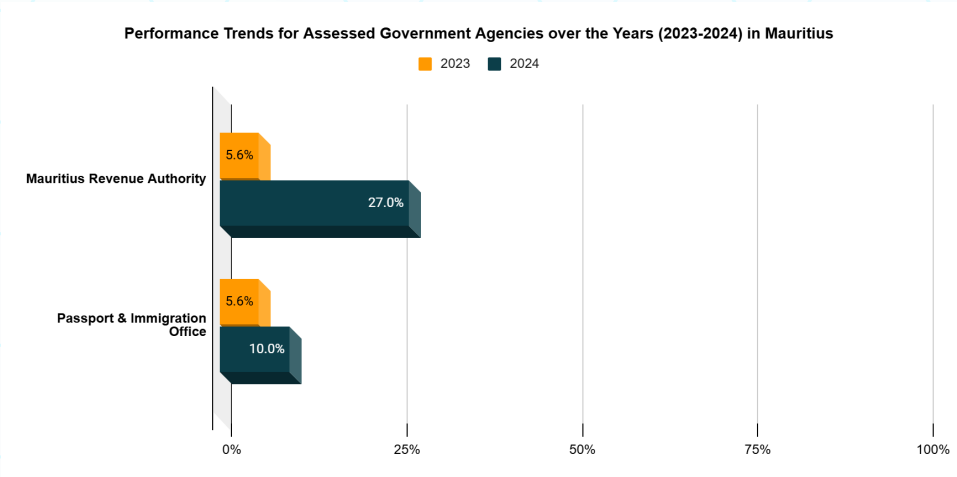
Britam Insurance scored 48% in 2024, reflecting a moderate increase from 40% in 2021. The improvement suggests that Britam Insurance has made meaningful efforts to enhance its data protection and compliance with privacy laws. While

it is performing better, the company still has room to further strengthen its security measures and privacy practices to achieve higher compliance levels. Jubilee Insurance scored 51% in 2024, a significant rise from 0% in 2021. This dramatic improvement indicates that Jubilee Insurance has taken significant steps to improve its data protection practices and comply with privacy regulations.

While the increase is impressive, the company should continue building on this progress to ensure ongoing compliance and enhance customer data security.

In conclusion, all four companies have made substantial progress in improving their data protection and privacy practices since 2021, with UAP Old Mutual and Jubilee Insurance leading in terms of compliance. Sanlam Uganda and Britam Insurance have also made impressive strides, but continued efforts will be necessary to strengthen their data protection frameworks and align with global best practices. These improvements are positive for customer trust, and further enhancement will help ensure compliance with evolving data protection regulations.

vi. Trends in performance of assessed companies/entities over time in the e-Government Sector

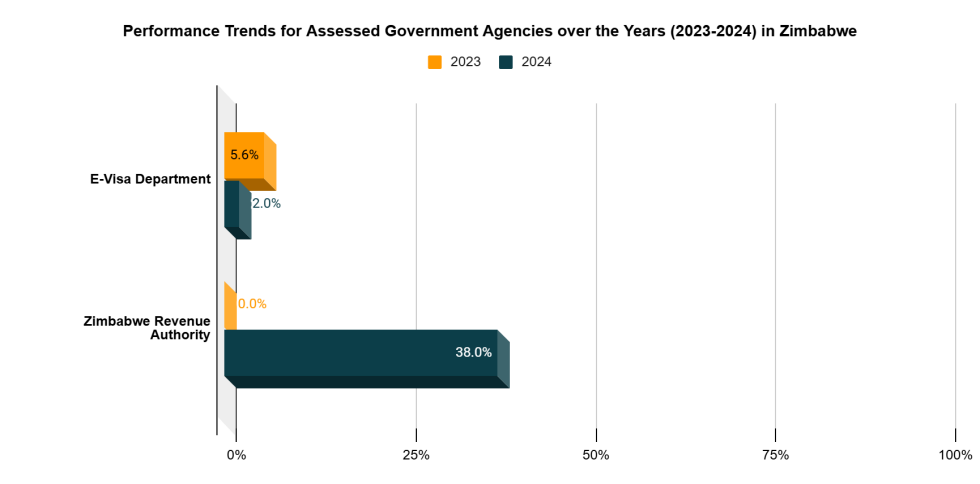


The performance of the Mauritius Revenue Authority (MRA) and the Passport & Immigration Office shows significant progress for both entities over the past year.

Mauritius Revenue Authority (MRA) scored 27.0% in 2024, a notable increase from 5.6% in 2023. This improvement indicates that the MRA has made significant strides in enhancing its data protection practices and aligning with privacy regulations. The increase in compliance suggests that the authority has taken steps to address gaps in its data privacy frameworks, potentially by strengthening security measures and improving internal policies related to the handling of personal data. While the score is still relatively low, the progress made in just one year is a positive sign, and further improvements are needed to fully comply with international privacy standards.

The Passport & Immigration Office, on the other hand, scored 10.0% in 2024, which is unchanged from its score in 2023. Although this represents a small level of compliance, the lack of improvement signals that the office may not have made significant efforts to enhance its data protection and privacy practices. The low score suggests that there are substantial gaps in the office's data security measures, and urgent action is needed to bring it in line with regulatory standards. Enhancing privacy protections will be crucial to ensuring the security of sensitive personal information, especially in an agency dealing with national identification and travel documents.

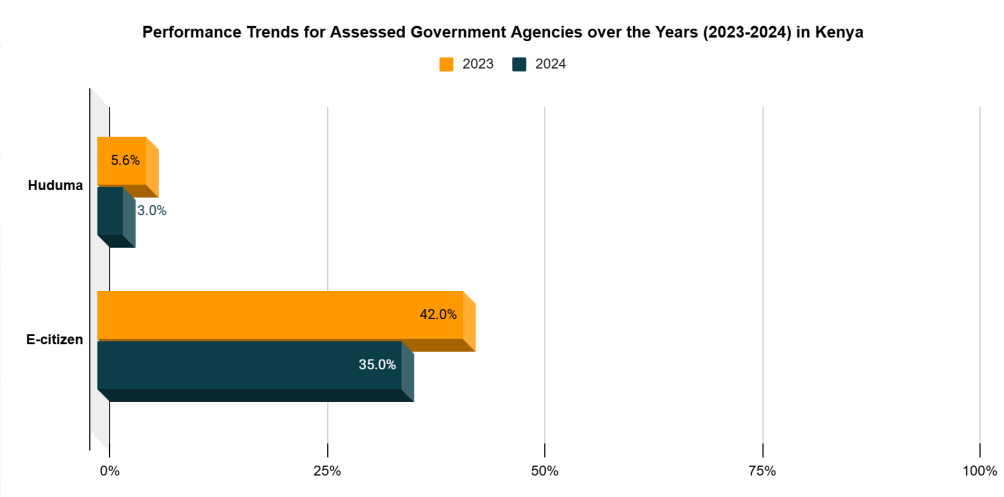
In conclusion, while both entities have shown some progress, the Mauritius Revenue Authority has made a marked improvement, reflecting efforts to strengthen data protection measures. The Passport & Immigration Office, however, remains stagnant, and significant improvements are needed to meet evolving data protection requirements and safeguard citizens' personal data effectively. Both organizations should prioritize upgrading their privacy frameworks to ensure full regulatory compliance and build public trust.



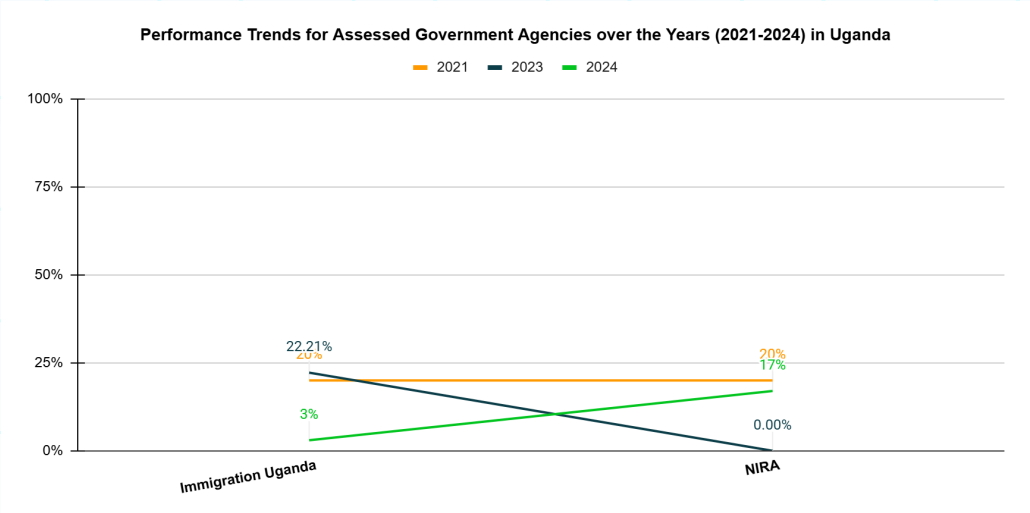
The performance of the E-Visa Department and the Zimbabwe Revenue Authority (ZIMRA) reflects differing levels of progress and challenges in their efforts to safeguard customer and citizen data. The E-Visa Department scored 2.0% in 2024, a slight improvement from 5.6% in 2023. While this increase is minimal, it still indicates some movement in the right direction. However, the overall low score highlights significant gaps in the department's data protection practices and suggests that there are major deficiencies in its privacy framework. The E-Visa Department needs to take substantial steps to strengthen its data security measures and comply with evolving privacy regulations to protect the sensitive personal information of applicants effectively.

In contrast, Zimbabwe Revenue Authority (ZIMRA) saw a significant improvement, scoring 38.0% in 2024, up from 0.0% in 2023. This dramatic rise indicates that ZIMRA has made considerable progress in enhancing its data protection practices over the past year. The increase suggests that the authority has taken meaningful actions to address privacy gaps, improve internal data handling procedures, and align with privacy regulations. While there is still considerable work to be done, the improvement marks a positive shift towards better compliance and data security.

In conclusion, while ZIMRA has made substantial progress in improving its data protection practices, E-Visa Department still faces significant challenges in meeting privacy standards. The E-Visa Department must urgently address the gaps in its data protection framework, while ZIMRA should continue its efforts to build on its improvements and further strengthen its privacy measures to ensure ongoing compliance with data protection laws.



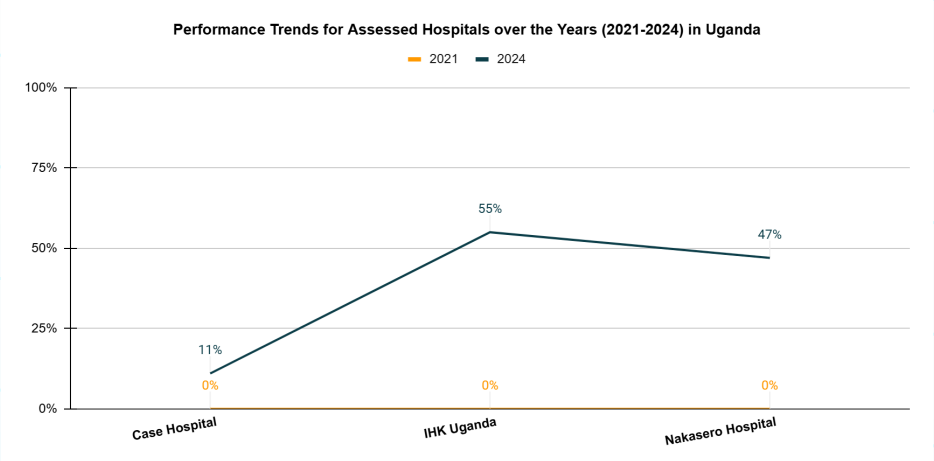
The performance for Huduma and E-citizen in the figure above, shows a decline in scores between 2023 and 2024. Huduma's score decreased from 5.6% in 2023 to 3.0% in 2024, suggesting a regression in their privacy practices. This decline may indicate reduced attention to or challenges in improving their data protection framework. On the other hand, E-citizen's score dropped from 42.0% in 2023 to 35.0% in 2024, showing a smaller decrease compared to Huduma, but still pointing to a negative trend in their privacy and data protection efforts. While both platforms experienced a decline, E-citizen's higher score indicates a more established approach to privacy compared to Huduma, though both could benefit from reevaluating and strengthening their privacy measures to avoid potential compliance and reputational risks.



The performance for Immigration Uganda and NIRA shows significant fluctuations between 2021 and 2024. Immigration Uganda's score dropped drastically from 22.21% in 2023 to 3% in 2024, following a smaller decrease from 20% in 2021. This sharp decline suggests a regression in privacy practices, potentially due to lapses in their data protection efforts or challenges in compliance. In contrast, NIRA's score increased from 0% in 2023 to 17% in 2024, marking significant progress in its privacy and data protection practices after starting from a baseline of 20% in 2021. While NIRA's 17% score indicates ongoing efforts, it still lags behind in comparison to other institutions with more robust privacy practices. Overall, both agencies show mixed results, with Immigration Uganda needing urgent attention to address its privacy shortcomings, while NIRA, although making progress, still has much work to do to enhance its data protection framework.

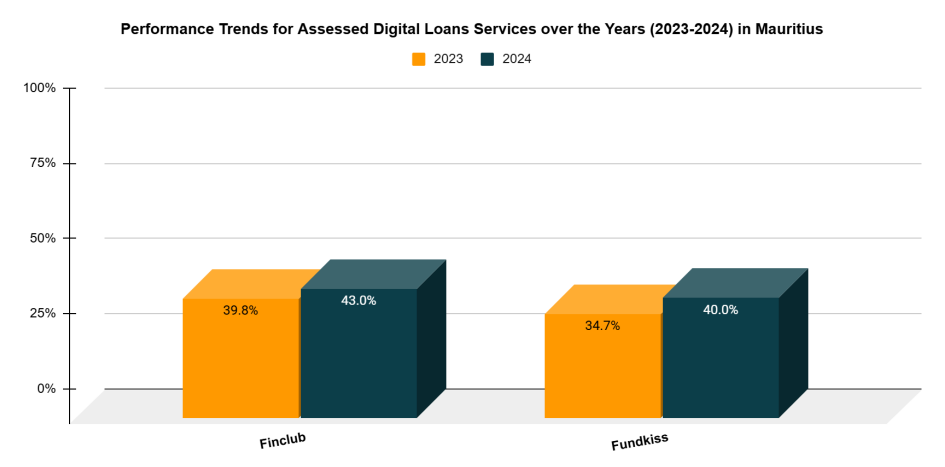
vii. Trends in performance of assessed companies/entities over time in the Health Sector

The performance of the assessed health institutions shows notable improvement from 2021 to 2024. Case Hospital's score rose from 0% in 2021 to 11% in 2024, indicating initial steps in establishing privacy measures, though significant work remains. IHK Uganda made the most substantial progress, increasing from 0% to 55%, suggesting a strong commitment to privacy and data protection practices, positioning it as a leader in the group. Nakasero Hospital, with a score of 47% in 2024 (up from 0%), demonstrates moderate progress, though it still lags behind IHK Uganda.



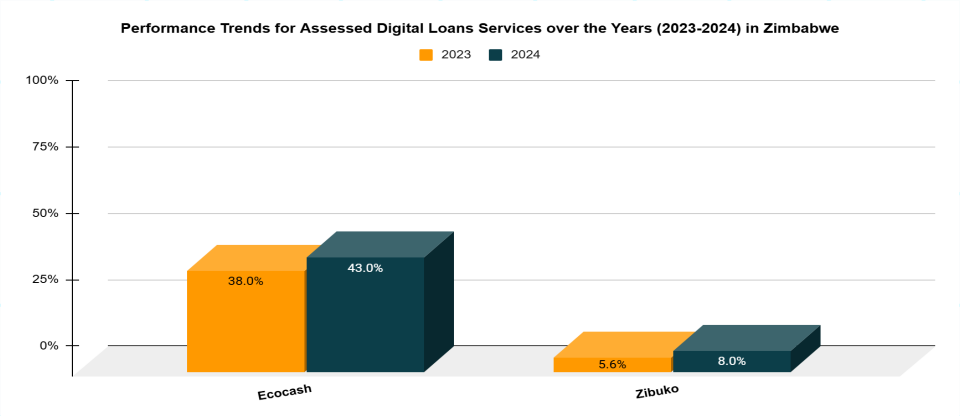
Overall, while all three hospitals have made strides, IHK Uganda's higher score reflects a more mature approach to privacy, reducing legal risks and enhancing patient trust. Case Hospital and Nakasero Hospital, however, still have considerable room for improvement to meet industry standards and mitigate regulatory and reputational risks.

viii. Trends in performance of assessed companies/entities over time in the Digital Loans Sector

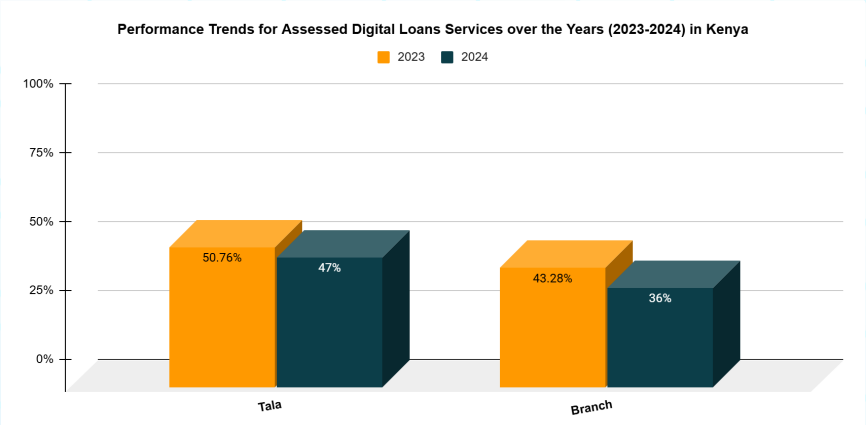


The performance for Finclub and Fundkiss in the above figure shows positive trends from 2023 to 2024. Finclub's score increased from 39.8% in 2023 to 43.0% in 2024, indicating a steady improvement in its privacy practices. Similarly, Fundkiss saw a rise from 34.7% in 2023 to 40.0% in 2024, reflecting a continued focus on enhancing data protection measures. While both platforms show progress, Finclub has outpaced Fundkiss slightly in terms of improvements.

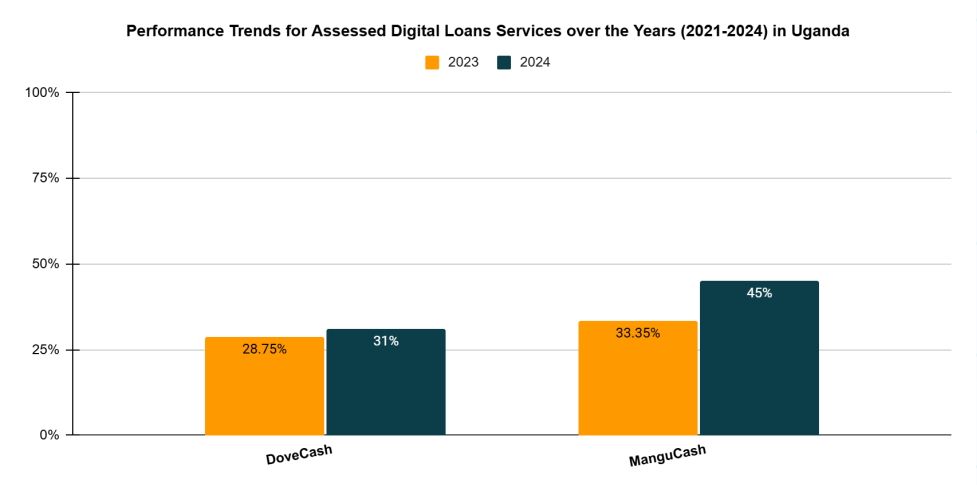
However, both scores still suggest that there is room for further enhancement in their data protection frameworks to meet higher standards and ensure full regulatory compliance.



The performance in the above figure for Ecocash and Zibuko show positive progress for both platforms from 2023 to 2024. Ecocash improved from 38.0% in 2023 to 43.0% in 2024, indicating a steady enhancement in its data protection practices. Zibuko also saw progress, rising from 5.6% in 2023 to 8.0% in 2024, although the increase is more modest. While Ecocash demonstrates a stronger and more consistent focus on privacy and data protection, Zibuko's score, though improving, remains significantly lower, highlighting a need for more substantial efforts to strengthen its privacy framework. Both platforms are on the right path, but Ecocash is currently leading in terms of privacy performance.



The performance for Tala and Branch in the above figure shows a decline from 2023 to 2024. Tala's score decreased from 50.76% in 2023 to 47% in 2024, indicating a slight regression in its privacy practices, although it still maintains a relatively strong performance. Similarly, Branch's score dropped from 43.28% in 2023 to 36% in 2024, reflecting a more significant decrease in its data protection efforts. Despite these declines, Tala still outperforms Branch in terms of privacy and data protection. Both platforms may need to reassess and strengthen their privacy frameworks to reverse these trends and continue improving their compliance with data protection standards.

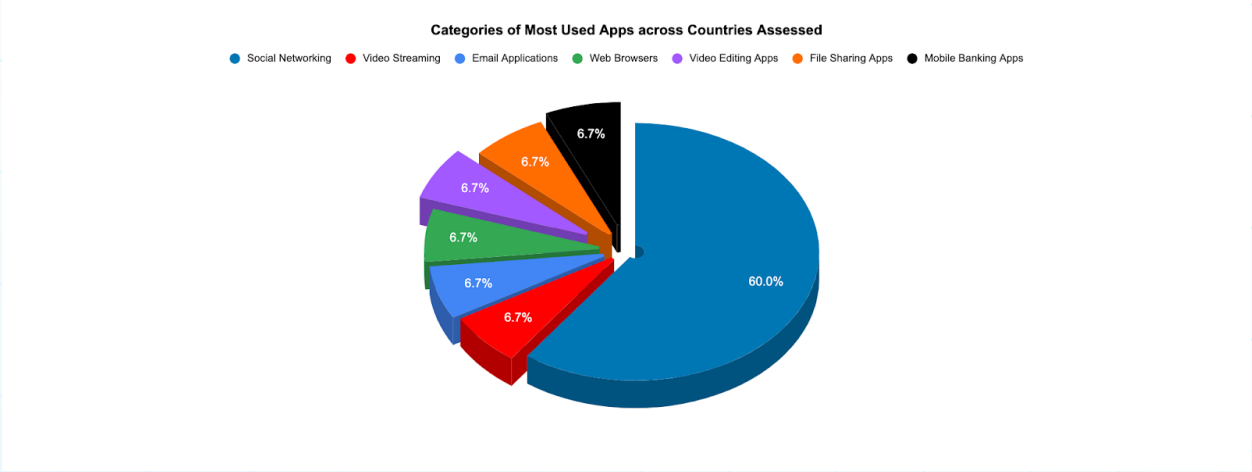


The performance in the above figure for DoveCash and ManguCash shows improvement from 2023 to 2024. DoveCash's score increased from 28.75% in 2023 to 31% in 2024, indicating a modest but positive trend in its privacy practices. ManguCash saw a more significant improvement, rising from 33.35% in 2023 to 45% in 2024, reflecting a stronger focus on enhancing data protection measures. Although both platforms have made progress, ManguCash has shown a more substantial improvement, positioning it ahead of DoveCash in terms of privacy performance. Both platforms, however, still have room to strengthen their data protection frameworks to fully align with industry standards.

3.3 Overall Assessment of the most used Apps in the countries

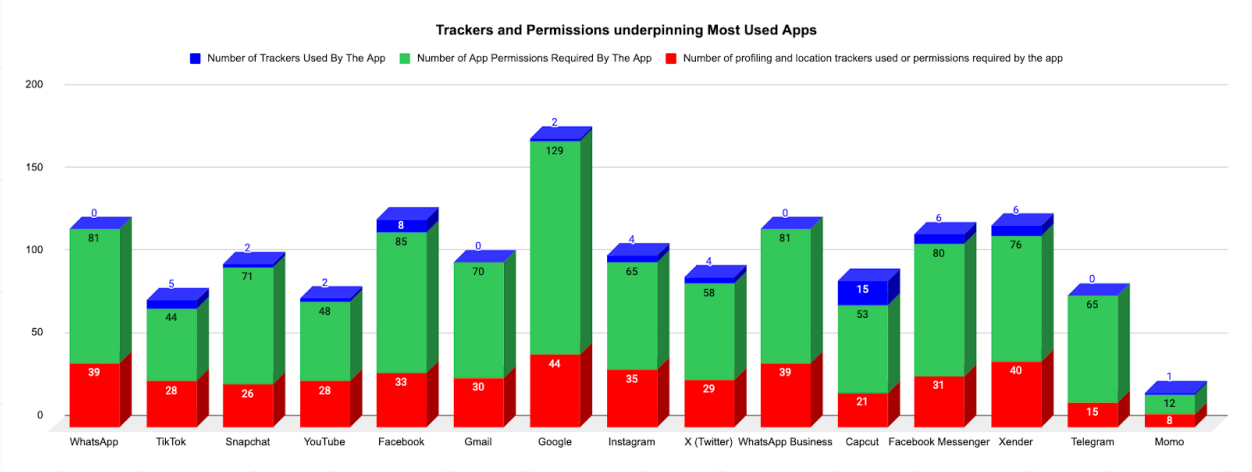
The assessment examined a total of 20 most used apps across the countries assessed in the report. Out of which, the category most used is social networking apps at 60%, while other app categories – video streaming, email applications, file sharing apps, mobile banking apps and much more, each is at 6.7%. social networking apps as the most used category suggests that these platforms face intense scrutiny regarding privacy practices and compliance with data protection laws.

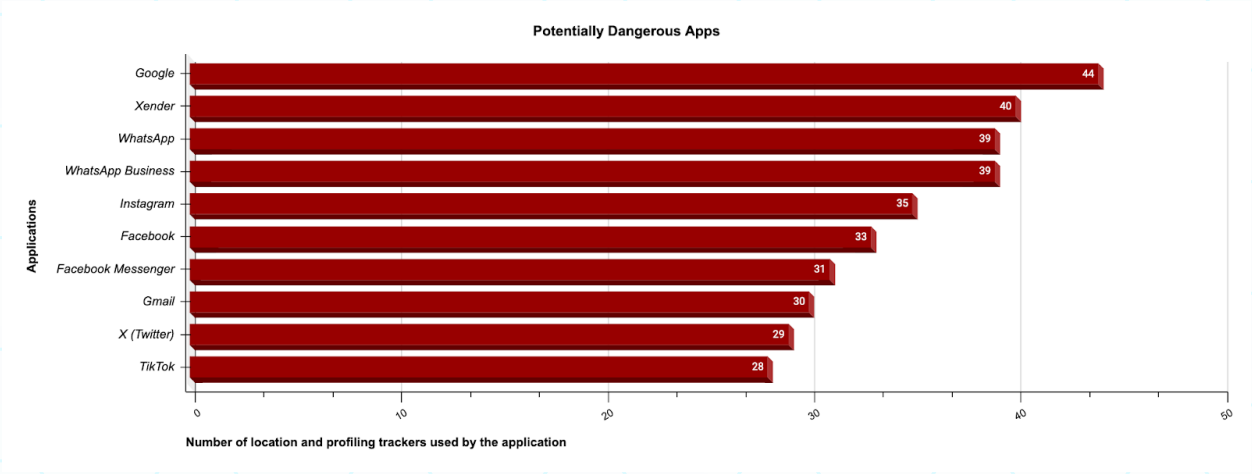
Given the vast amount of personal data they handle, including user interactions, location data, and more, a 60% privacy score indicates that there are efforts to implement some privacy controls. However, challenges remain in securing user data, managing third-party access, and ensuring full compliance with privacy regulations.



All the other categories have a 6.7% score each, indicating that the apps most used in these categories have very weak or insufficient privacy and data protection measures. These apps may not be addressing critical privacy risks adequately, exposing users to potential data breaches, misuse, and lack of informed consent.

The disparity between social networking apps and the rest of the categories, suggests that social networking platforms are under more scrutiny and are likely subject to greater regulatory pressure, which might explain their relatively better privacy efforts. While, the other categories - video streaming, email, web browser, video editing, file sharing, and mobile banking apps are significantly lagging in terms of privacy protections. There is wide spread privacy deficiencies and these apps are vulnerable to data breaches, unauthorized data sharing, and misuse of personal information. Given their reliance on user data for various functions (e.g., browsing, financial transactions, or content sharing), they need to adopt stricter privacy policies and security measures to ensure user trust and comply with data protection laws including enhancing security protocols, stronger encryption, implementation of privacy-by-design principles, user consent management, and better transparency, to safeguard user privacy and comply with global standards.





The figures above, show potentially dangerous Apps based on the number trackers and permissions. These trackers are used to collect user data, often for personalized advertising, location-based services, and profiling, raising significant privacy concerns. Google's high tracker count (44) reflects its extensive data collection practices. Google collects vast amounts of user data through its various services (Search, Maps, Gmail, YouTube, etc.), including location, browsing behavior, and personal information. This level of data collection can lead to privacy risks, including misuse of personal data for targeted advertising and profiling. Google's use of so many trackers raises concerns about user consent, data transparency, and control. Google should prioritize improving data anonymization, minimizing data retention, and providing users with clearer options to manage and limit data collection. The app might also be at risk of breaching data protection regulations if its practices are not fully compliant with GDPR or similar laws.

Xender, a file-sharing app, uses 40 trackers, which is a concerning number for an app primarily focused on transferring files. This suggests that Xender may be collecting a significant amount of personal data from users for purposes other than file sharing, such as profiling or targeted advertising. The high number of trackers in Xender could result in the collection of sensitive user data, especially if users are unaware of the data being collected. Users need clear disclosures about what data is being gathered and for what purpose. The app must implement stronger data protection measures and ensure full transparency about its data handling practices.

WhatsApp, a messaging app with a strong user base, uses 39 trackers, which is significant considering its primary function is communication. While WhatsApp's end-to-end encryption provides a degree of privacy for messages, the

app still collects metadata and other data points, such as location and device information, through its trackers. The data collected by WhatsApp, including location and metadata, can be used for profiling and targeted ads. Privacy-conscious users may find this concerning, as it could undermine the confidentiality of their communication. WhatsApp should focus on improving transparency and limiting the amount of data it collects for non-essential purposes.

Instagram's 35 trackers reflect its significant data collection practices, which are largely aimed at personalizing user experience and targeting ads. Instagram, owned by Meta, tracks user behavior across its platform and other third-party apps, collecting extensive data about user preferences, interests, and online behavior. Instagram's high tracker count raises concerns about the extent of surveillance and profiling. Users should be informed about the data being collected and should have the ability to opt out of certain tracking mechanisms. Moreover, Instagram needs to focus on enhancing data security to prevent breaches and misuse of personal information.

Facebook, also owned by Meta, uses 33 trackers. Like Instagram, Facebook collects vast amounts of personal data for targeted advertising and profiling. The app tracks user interactions, locations, and even the data of users who do not have Facebook accounts (through tools like the Facebook Pixel). The large number of trackers means Facebook has access to a considerable amount of personal data, making it a target for privacy concerns and regulatory scrutiny. Facebook needs to better address user consent, limit unnecessary data collection, and provide stronger user controls over their data.

TikTok, with 28 trackers, collects significant amounts of data about its users, including location, device data, and interaction with content. Given its wide popularity, particularly among younger users, this raises privacy concerns, especially as TikTok has been criticized for its data practices, including ties to China, raising fears about government surveillance and data misuse. TikTok's data collection practices need to be more transparent, and the company should take greater care in safeguarding user data. Privacy risks include unauthorized data sharing, potential data breaches, and misuse of personal information for profiling. TikTok should also comply with global data protection regulations to mitigate risks to user privacy.

Telegram, known for its focus on privacy and security, uses significantly fewer trackers (15), reflecting a more privacy-conscious approach compared to other apps on this list. Telegram's end-to-end encryption for secret chats and its relatively low data collection practices make it a safer option for users concerned about privacy. Despite its lower tracker count, Telegram must remain vigilant about potential data collection through its platform. It should continue to focus on minimizing its data footprint and ensuring that its encryption and data protection mechanisms remain strong to safeguard user privacy.

Momo, with only 8 trackers, has one of the lowest tracker counts on this list. While this might indicate that Momo collects less data compared to other apps, users should still be cautious and ensure they understand the specific permissions the app requests. Momo's lower tracker count is a positive sign in terms of privacy, but it still needs to maintain transparency about the data it collects and the purposes behind the trackers it uses. Users should be aware of the app's privacy policies and have control over the data they share.

In sum, Apps with a high number of trackers (Google, Xender, WhatsApp, Instagram, and Facebook) create significant privacy risks. These apps are likely collecting vast amounts of personal information, including location data, browsing habits, and behavioral profiling, which can be used for targeted advertising or, in some cases, sold to third parties. Many apps with high tracker counts lack transparency about the data being collected and the purposes behind it. Users need clear consent mechanisms, easy-to-understand privacy policies, and greater control over the data shared with these apps. Apps with excessive tracking and profiling need to prioritize robust security measures, including encryption, data minimization, and regular audits, to prevent misuse of personal data and ensure compliance with global privacy regulations like GDPR and CCPA.

Apps with a high number of trackers are likely to attract regulatory scrutiny, especially as countries around the world introduce stricter data protection laws. These platforms must take proactive steps to comply with these regulations, ensuring that user data is handled ethically and legally.

Lastly but not least, Apps with a high number of trackers, such as Google, Xender, and WhatsApp, pose significant privacy and data protection risks. These apps must improve transparency, strengthen user consent mechanisms, and ensure compliance with privacy regulations to protect user data. On the other hand, apps like Telegram and Momo, with fewer trackers, show a more privacy-conscious approach, but they must remain vigilant in protecting user data. In the context of the privacy scorecard, these findings emphasize the need for stronger privacy practices and greater user control over personal data across all app categories.

3.4 Significant gaps/ shortcomings in data protection practices

This section highlights the significant gaps and shortcomings in current data protection practices. It identifies key areas where organizations may be failing to implement adequate security measures, leaving sensitive information vulnerable to breaches or misuse. These gaps arose from several aspects including insufficient training, lack of comprehensive policies, or ineffective enforcement, all of which can compromise data privacy and security. This section aims to shed light on these critical issues and explore potential solutions to enhance data protection frameworks.

I. Transparency and Clarity of Data Practices

A recurring issue across sectors like telecommunications, e-commerce, online betting, finance, and healthcare is the lack of transparency regarding data collection, processing, and sharing. Many organizations fail to disclose the types of data they collect, its intended uses, and how long it will be retained. This lack of clarity undermines consumer trust and increases the risk of non-compliance with privacy regulations. Additionally, users are often unaware of third-party data sharing practices, which compounds privacy risks.

II. Consent Mechanisms and User Control

Consent practices are frequently inadequately implemented across sectors, leaving users with limited control over their personal data. Telecom and e-commerce platforms, for example, often present unclear or overly complex consent forms, failing to inform users adequately about data collection and its purposes. Similarly, in sectors like healthcare, digital loans, and e-government, consent is not always informed or explicit, undermining users' privacy rights and increasing regulatory risks.

III. Data Security Deficiencies

Many sectors, including telecom, finance, health, and e-commerce, exhibit significant weaknesses in their data security measures. Weak encryption, outdated security protocols, poor access control, and the absence of regular security audits expose sensitive personal information to breaches and cyberattacks. Inadequate security practices are particularly concerning in industries like online betting and financial institutions, where the risk of fraud and identity theft is high.

IV. Third-Party Data Transfers and Partnerships

Across sectors such as online betting, finance, and telecommunications, data is often shared with third-party vendors. However, these transfers frequently occur without sufficient transparency or oversight, leaving users unaware of how their data is being shared, the parties involved, or the purposes of such transfers. Third-party vendors may not adhere to the same security standards as the original data holders, heightening the risk of data misuse and breaches.

V. Data Retention and Disposal

Many organizations fail to establish clear data retention policies, resulting in the retention of personal data for longer than necessary. This lack of clarity is particularly concerning in industries like health, finance, and digital lending, where sensitive personal information is involved. Without clear retention and disposal practices, organizations expose themselves to unnecessary privacy risks and legal consequences.

VI. Regulatory Compliance and Oversight

Compliance with privacy laws such as the GDPR, CCPA, and HIPAA is often inconsistent across sectors. Many organizations fail to conduct regular audits, which can lead to non-compliance and expose them to potential fines and legal actions. Sectors like e-government face additional concerns about surveillance programs and the collection of data for national security purposes, often lacking adequate oversight or clear legal frameworks.

VII. Breach Management and Response

A common shortcoming across sectors is a lack of preparedness for handling data breaches. While many organizations have basic security measures in place, their breach response plans are often inadequate or slow. This delay in responding to breaches exacerbates the impact, damaging consumer trust and increasing the risk of regulatory penalties. Effective breach management protocols, including timely notifications to affected individuals and regulators, are necessary to mitigate these risks.

VIII. Addiction Monitoring and Ethical Data Use

Online betting platforms face unique challenges concerning the ethical use of data for addiction monitoring. While some platforms use data to promote responsible betting, there is often a lack of transparency regarding how this data is used, and in some cases, it may be exploited for targeted marketing. Ethical data practices must be established, ensuring users have control over how their data is used, including the ability to opt out.

IX. Data Minimization and Over-Collection

Several sectors, including insurance, healthcare, and digital loans, tend to over-collect personal data, increasing the risk of breaches and non-compliance. Implementing data minimization policies—only collecting the data necessary for operations—can help mitigate these risks and ensure compliance with data protection laws.

Across various sectors—telecommunications, e-commerce, online betting, finance, healthcare, insurance, and government—there are significant gaps in data protection practices. These gaps primarily revolve around transparency, data security, consent mechanisms, third-party sharing, and regulatory compliance. By addressing these shortcomings, organizations can enhance user trust, mitigate privacy risks, and ensure compliance with evolving privacy regulations. Key measures include improving transparency, implementing robust security practices, obtaining informed consent, and establishing clear data retention and breach response policies.

3.5 Sector-Wise Analysis

This section provides a comprehensive analysis of the privacy policies, security practices, and transparency measures of selected organizations. It reviews how 190 companies across eight (8) sectors—telecommunications, e-commerce, online betting, banks and finance, insurance, e-government, health and digital loans and—are addressing personal data protection based on their public disclosures. The analysis evaluates the information available on each entity's website, using key criteria aligned with seven indicators outlined in the methodology and selection criteria section above. The findings are presented in two parts: sector-specific insights for each country, an overall assessment of the performance against indicators and the most used apps and implications thereof for personal data protection and privacy rights.

3.5.1 Telecommunications Sector Analysis

3.5.1.1 Overview of the sector and data collectors evaluated

The telecommunications sector across Rwanda, Tanzania, Mauritius, Kenya, Zimbabwe, and Uganda plays a crucial role in driving economic development and digital transformation. Each country has seen significant growth in mobile services, internet connectivity, and mobile money solutions. In Rwanda, the government is heavily investing in digital infrastructure, with key players like MTN and Airtel driving mobile and broadband expansion. Tanzania has experienced rapid growth, particularly in mobile money, with operators like Vodacom and Tigo leading the way. Mauritius boasts a well-established telecom market, with high internet penetration and a focus on digital services through Mauritius Telecom and Emtel.

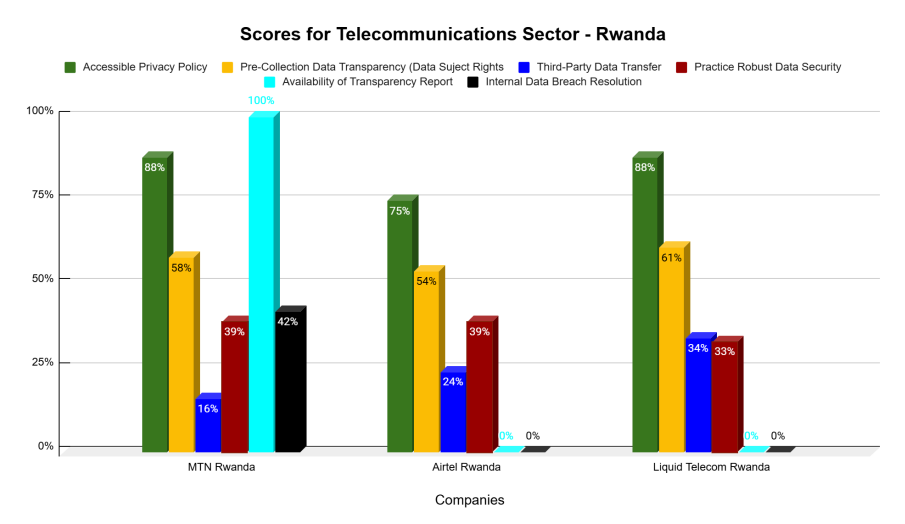
Kenya is a regional leader, with Safaricom's M-Pesa revolutionizing mobile money, while expanding 3G and 4G networks. Zimbabwe faces economic challenges but remains reliant on telecom services, with Econet and NetOne providing essential mobile and internet connectivity. Uganda has a competitive market with MTN and Airtel leading mobile services, and mobile money playing a significant role in financial inclusion. Overall, while each country presents unique challenges and opportunities, the telecommunications sectors in these nations are integral to improving digital connectivity, supporting financial inclusion, and fostering broader economic growth through continued infrastructure investment and regulatory reform.

3.5.1.2 Analysis of compliance with each criterion

In this sector, the report focused on a total of 23 data collectors. These included: MTN Rwanda, Airtel Rwanda and Liquid Telecom Rwanda from Rwanda; Vodacom, Tigo Tanzania, TTCL and Airtel Tanzania from Tanzania; Emtel, Liquid Telecom, MyT (my.t) and Atcomm from Mauritius; Econet, TelOne, NetOne and Liquid Telecom Zimbabwe from Zimbabwe; Zuku, Safaricom, Jamii Telecommunications Limited (JTL) and Airtel from Kenya; and MTN Uganda, Lycamobile, Airtel Uganda and Roke Telkom from Uganda. With the exception of Rwanda where only three (3) companies could be selected, in the rest of the countries, four (4) companies were selected in each country.

a) MTN Rwanda, Airtel Rwanda and Liquid Telecom Rwanda in Rwanda

Only MTN Rwanda was found with a transparency report and scored 100% while the rest for the lack of a transparency report registered 0%. Both MTN Rwanda and Liquid Telecom Rwanda registered 88% as the highest score for the indicator on an accessible privacy policy while Airtel Rwanda scored 75%. An average performance of 50% was registered by all companies in respect of the indicator on pre-collection data transparency (data subject rights) while very low scores where registered for compliance with indicators on practice robust data security, followed by third-party transfer and internal data breach resolution. The figure presents further details on the performance, with an in-depth discussion of the three companies provided below.



All three companies have privacy policies exceeding 200 words, with MTN's policy at 2,878 words, Airtel's at 1,235 words, and Liquid Telecom's at 1,666 words. While MTN and Liquid Telecom's policies were relatively readable, Airtel's was more difficult to comprehend.

Liquid Telecom provides details on data collection, retention, and user rights (access, correction, objection, restriction, deletion, and complaint mechanisms). It prohibits sharing data with advertisers but lacks specifics on collected data, company contact information, and third-party recipients. Personalized advertising is opt-in, but the policy does not clarify law enforcement access to user data. MTN outlines the types of data collected, reasons for collection, and user rights, including deletion and objection. It allows permanent deletion and requires opt-in for advertising. However, it only provides an email contact, permits third-party data sharing without listing recipients, and allows law enforcement access upon reasonable request. Airtel specifies company contact details and types of data collected while prohibiting data sharing with advertisers. It states reasons for collection but does not include a retention period. The policy does not clearly define user rights to access, correction, deletion, or restriction of processing. It allows complaints to the regulator and permits law enforcement access upon reasonable request.

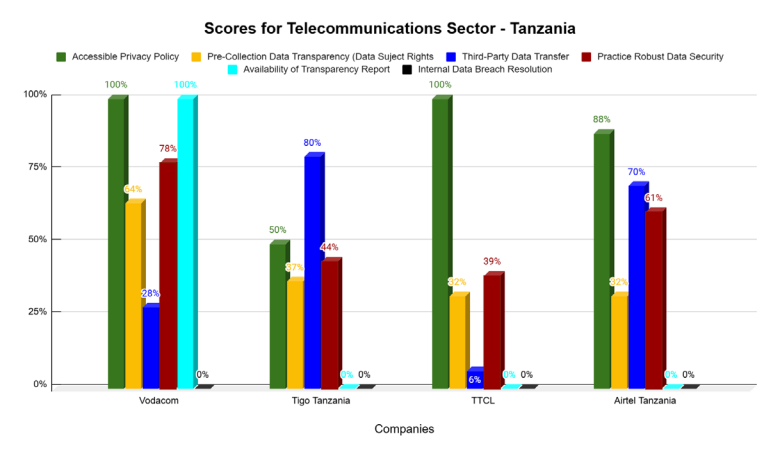
Liquid Telecom prohibits third-party access to personal data and does not share with advertisers but allows law enforcement access upon reasonable request. It does not outline data breach resolution mechanisms. MTN and Airtel allow third-party access without listing recipients or specifying shared data types. MTN permits sharing with advertisers, while Airtel does not. Neither policy provides clear breach resolution mechanisms, and both allow law enforcement access upon request. MTN acknowledges data breaches, outlines reporting procedures, and mentions resolution mechanisms but lacks clarity on rectification, does not mandate user notification, omits resolution timeframes, and does not ensure fair investigations. Airtel and Liquid Telecom do not address data breaches at all.

In terms of security sssessments, SSL Server Scored: MTN (B), Airtel (A), Liquid Telecom (B); Security Header Scored: MTN (F), Airtel (D), Liquid Telecom (D) while, MTN's policy mentioned data security but lacked specifics. On the other hand, Airtel and Liquid Telecom did not address data security at all.

b) Vodacom, Tigo Tanzania, TTCL and Airtel Tanzania from Tanzania

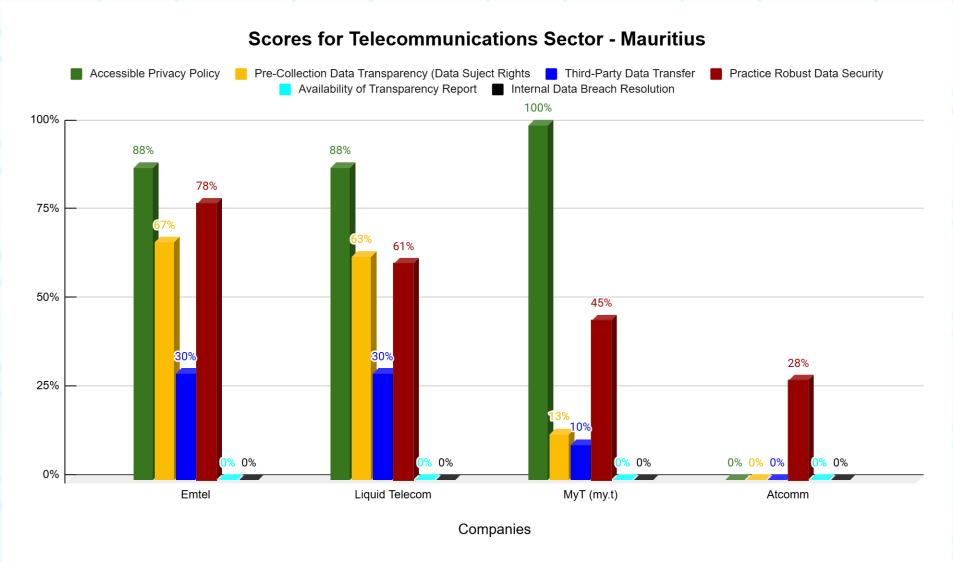
Vodacom and TTCL registered the highest score 100% in respect of the indicator on accessible privacy policy, closely followed by Airtel Tanzania with 88%. Vodacom is the only company that complied with the indicator on an available transparency report.

The performance for indicators on third-party data transfer and practice robust data security and pre-collection data transparency followed third with companies registering relative high scores. Tigo Tanzania and Airtel Tanzania scored 80% and 70% respectively, Vodacom and Air Tanzania scored 78% and 61% respectively and only Vodacom registered above 60% in respect pre-collection data transparency. On the other hand, a poor performance was observed for indicators on availability of transparency report and internal data breach resolution with very low scores registered by most of the companies assessed in the sector. The figure provides additional insights into the performance, with a more detailed discussion presented below.



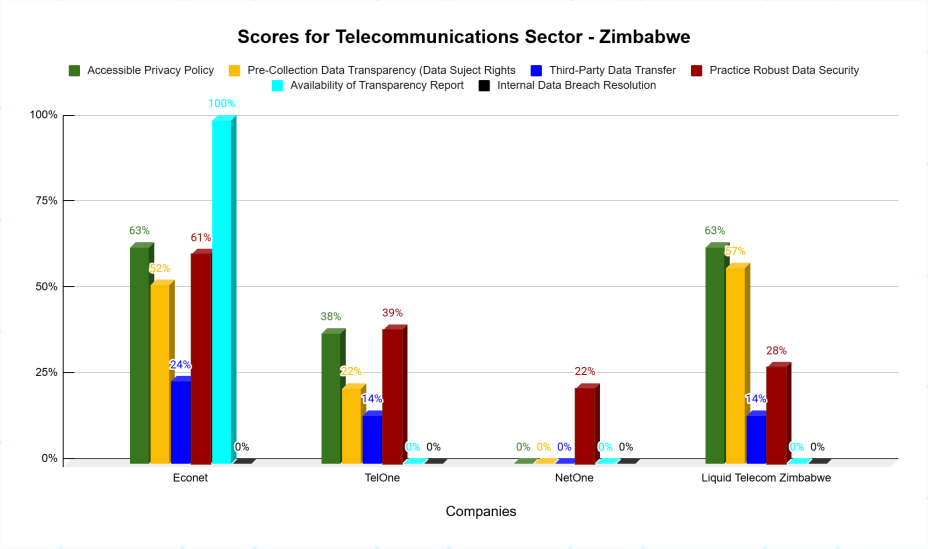
c) Emtel, Liquid Telecom, MyT (my.t) and Atcomm in Mauritius

MyT (my.t) company registered the higest score 100% in respect of the indicator on an accessible privacy policy and closely followed by Emtel and Liquid Telcom that both scored 88%. These companies also respectively registered 78% and 61% for the indicator on practice robust security as the second indicator with high compliance. Followed by the indicator on pre-collection transparency were once again both companies registered 67% and 63% respectively. On the other hand, low compliance levls were registered for the indicators on availability of transparency report, internal breach resolution with Atcomm company registering the least scores of them all. The figure below provides additional information, with a more detailed discussion on the performance following.



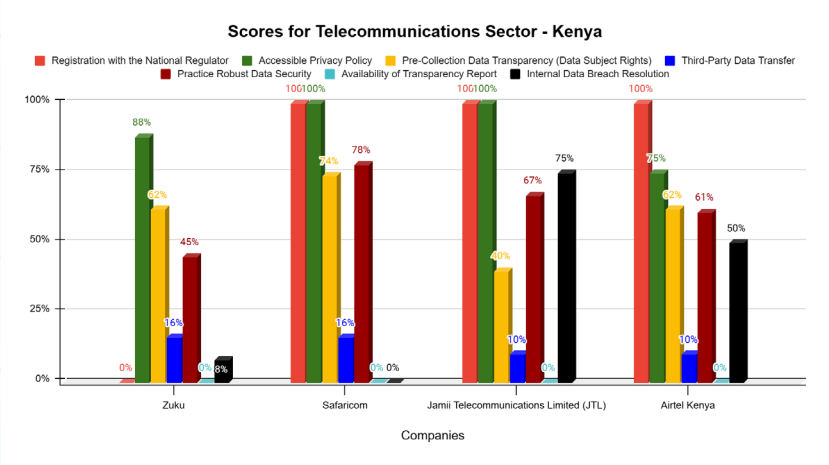
d) Econet, TelOne, NetOne and Liquid Telecom Zimbabwe in Zimbabwe

Whereas Econet registered the highest score 100% for the indicator on availability of a transparency report, the rest of the companies did not exhibit an annual transparency report. This was followed with score of 63% registered by both Econet and Liquid Telecom Zimbabwe for the indicator on accessible privacy policy. Equally, the same companies, registered 52% and 57% respectively as the highest scores for pre-collection data transparency. Though Econet scored 61% for the indicator on practice robust data security, low scores were observed for the rest of the companies and NetOne had the least scores. The figure below provides more details, followed by a further discussion on the companies' performance.



e) Zuku, Safaricom, Jamii Telecommunications Limited (JTL) and Airtel Kenya in Kenya

There was greater compliance exhibited with a good performance registered for indicators on registration with the National Regulator and accessible privacy policy were three (3) companies namely Safaricom, Jamii Telecommunications Ltd and Airtel Kenya each scored 100%. While, low compliance levels were observed for the indicators on third-party data transfer were both Zuku and Safaricom scored 16% each and JTL and Airtel Kenya scored 10%. While, the lowest score of 0% was registered for indicators on availability of transparency report, internal data breach resolution. The figure below provides additional details on the performance, followed by a further discussion.



Safaricom and Jami Telecommunications (JTL) both maintain comprehensive and accessible privacy policies. Safaricom's 3,038-word policy, effective since 2019, aligns with the Kenya Data Protection Act, outlining data collection, legal bases, usage, and users' rights. These rights include access, correction, deletion, objection, and complaint lodging. The policy also details data disclosure in Tanzania, retention conditions, and the role of a Data Protection Officer.

JTL's 2,232-word policy, prominently displayed on its website, mirrors Safaricom's in clarity and adherence to the Kenya Data Protection Act and EU GDPR. It specifies data processing principles, transfer safeguards, and users' rights. Additionally, JTL's policy emphasizes the role of Data Protection Officers in policy enforcement and dispute resolution, ensuring transparency and accountability.

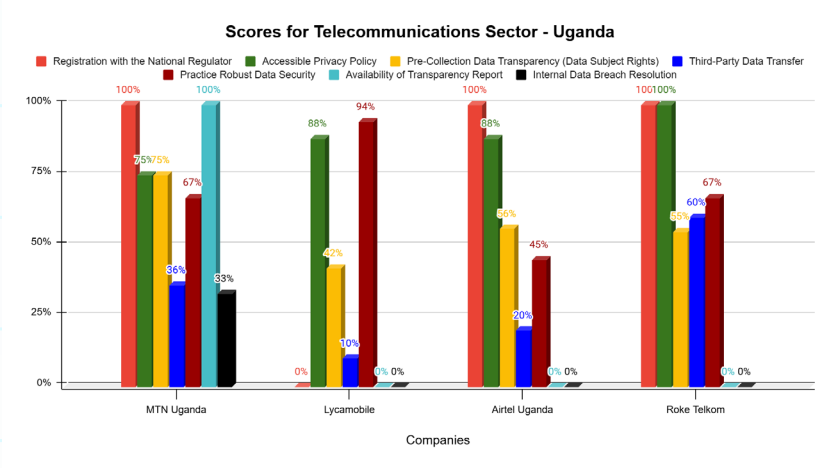
f) MTN Uganda, Lycamobile, Airtel Uganda and Roke Telkom in Uganda

MTN Uganda, Airtel Uganda, Lycamobile, and Roke Telkom are the leading telecommunications companies in Uganda. MTN dominates the market with 53% share (20 million subscribers), followed by Airtel with 35.3% (over 10 million subscribers). MTN Uganda exhibited more compliance levels across the seven (7) indicators in the sector compared to the rest.

MTN Uganda, Airtel Uganda, and Roke Telkom all scored 100% for registration with the national regulator and having publicly accessible privacy policies. However, only Roke Telkom's policy is easy to read and understand. MTN, despite its market leadership, has the least readable policy due to its complexity and excessive length.

Lycamobile remains unregistered with the national regulator due to its status as a Mobile Virtual Network Operator (MVNO)—leasing network capacity rather than owning infrastructure. This limits regulatory oversight, leading to compliance gaps. A key example is Lycamobile's unlawful practice of charging UGX 43,000 (~$12) for users to access their own personal data, directly violating Uganda's Data Protection and Privacy Act.

With the exception of MTN Uganda, the rest of the companies exhibited the least compliance levels for the indicators on availability of a transparency and internal breach resolution. This was the case for Lycamobile, Airtel Uganda and Roke Telkom. The figure offers additional insights into the performance, with a further discussion provided below.



For data collection and user rights, MTN's policy is transparent in data collection and user rights, explicitly outlining the types of data collected and granting users rights to access, correct, delete their data, and lodge complaints. While, Airtel and Lycamobile's policies fail to clearly state reasons for data collection or list third parties with access and Roke Telkom allows behavioral marketing without an opt-in/out option, unlike the other three.

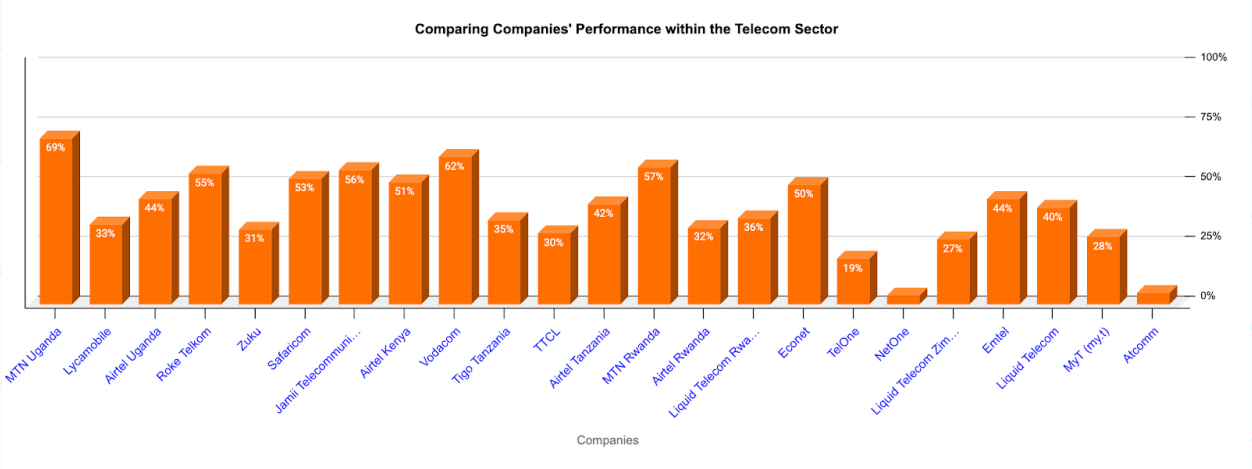
In respect of data sharing and retention, Roke Telkom's policy prohibits third-party access to personal data, though it lacks clear reporting channels for data breaches. MTN, Airtel, and Lycamobile allow third-party access, but only MTN explicitly lists these third parties. None specify the types of data shared, creating risks for users. Lycamobile lacks clarity on data retention, third-party sharing, law enforcement access and illegally charges users for data access.

Lycamobile has the strongest data security, followed by MTN and Roke Telkom, while Airtel lags behind indicating weaker protections. MTN is the only company to have published a transparency report (since 2023), while the others offer no insight into government or third-party data requests. None of the companies provide robust internal mechanisms for reporting or investigating data breaches. MTN leads though with a weak score while the rest registered low compliance levels showing a severe lack of transparency and accountability in data protection.

To this end, Lycamobile's non-compliance highlights gaps in Uganda's data protection enforcement. Other telecoms should follow MTN's lead in publishing user data request reports. Airtel, in particular, must improve security protections. Airtel and Lycamobile must explicitly list third-party recipients and specify the data shared. Companies should clearly outline data retention policies and provide free access to personal data, per Ugandan law.

3.5.1.3 Comparison of companies/entities within the sector

MTN Uganda leads the telecom sector with a strong score of 69%, demonstrating a solid commitment to user data management and regulatory compliance. Close behind, Vodacom in Tanzania scores 62%, reflecting a similar focus on securing user data. Roke Telkom in Uganda, with a score of 55%, also performs well, though there is still room for improvement compared to MTN Uganda.



Safaricom, Kenya's leading telecom operator, scored 53%, showing solid efforts in data protection, though it trails behind MTN Uganda and Vodacom. Jamii Telecommunications Limited (JTL) follows closely with 56%, indicating a good commitment to privacy. Airtel Uganda (44%) and MTN Rwanda (57%) fall in the mid-tier, with MTN Rwanda performing slightly better than Airtel Uganda, but both still have significant room for improvement in their privacy practices.

Lycamobile (33%) and Tigo Tanzania (35%) have low privacy scores, indicating significant gaps in their data protection efforts and compliance with privacy regulations. Airtel Tanzania (42%) performs slightly better but still falls below industry standards, signaling the need for improvement.

Econet in Zimbabwe scores 50%, showing moderate commitment to privacy, while Liquid Telecom, with a score of 40% in both Mauritius and Zimbabwe, demonstrates some effort but has considerable room for growth.

NetOne (4%) and TelOne (19%) in Zimbabwe are the lowest performers, with extremely low scores indicating poor privacy practices, putting user data at high risk of breaches and misuse. Atcomm in Mauritius also scores poorly at 5%, reflecting a severe lack of focus on privacy, which could expose users to significant privacy violations and cybersecurity risks.

In sum, companies with low privacy scores, such as NetOne (4%), TelOne (19%), Lycamobile (33%), and Tigo Tanzania (35%), risk failing to comply with local and international data protection regulations, which could lead to legal consequences, fines, and reputational damage. Telecoms with higher privacy scores, like MTN Uganda (69%), Vodacom (62%), and MTN Rwanda (57%), are likely to gain greater consumer trust and a competitive advantage by positioning themselves as privacy-conscious. On the other hand, companies with low scores risk losing customer trust, potentially leading to customer churn. Telecoms with low scores are also more vulnerable to data breaches and cyberattacks, which could expose sensitive data and result in financial losses. Companies with higher scores typically offer better transparency and user control over data, while lower-scoring firms may limit customer control, increasing the risk of privacy violations. Mid-tier companies, like Safaricom (53%) and Airtel Uganda (44%), have opportunities to improve by enhancing encryption, user consent processes, and transparency to better protect their customers' data.

The performance of telecom companies across the region varies significantly. Top performers like MTN Uganda and Vodacom show a strong commitment to user data protection, reducing regulatory risks and fostering consumer trust. In contrast, low performers such as NetOne, TelOne, and Lycamobile face major privacy concerns, risking legal issues and a loss of customer confidence. Mid-tier companies should focus on improving transparency, user consent, and cybersecurity to strengthen their market position. Overall, the telecom sector must improve privacy practices to meet international standards, safeguard user data, and create a safer digital environment.

3.5.1.4 Identification of sector-specific challenges and best practices

The section explores the sector-specific challenges faced by the telecommunications industry, alongside the best practices for addressing them. It delves into the unique issues, such as safeguarding customer data, ensuring compliance with privacy regulations, and managing security risks related to vast networks and personal information. By identifying these challenges and highlighting effective strategies, this section provides insights into how telecommunications companies can strengthen their privacy and data protection practices while maintaining trust and compliance in an increasingly digital world. These include the following;

I. Data Collection and Storage

Telecom companies collect vast amounts of sensitive data, including subscriber information, communication metadata, call logs, internet usage patterns, and location tracking data. This wealth of information, while crucial for delivering services, also presents significant privacy and security challenges. The storage of such data is often fragmented across multiple systems and locations, making it difficult to ensure comprehensive protection.

In many cases, insufficient encryption, outdated security measures, and a lack of robust access controls increase the risk of data breaches or unauthorized use.

The sheer volume and sensitivity of the data create an attractive target for cybercriminals, and any lapses in security can lead to severe consequences, including identity theft, financial fraud, or unauthorized surveillance. As a result, telecom companies must take urgent steps to strengthen their data protection practices, implementing modern encryption technologies, regularly auditing their security protocols, and ensuring strict compliance with privacy regulations to safeguard this invaluable information.

II. Consent Mechanisms

Consent mechanisms in telecommunications are often inadequately implemented, leaving consumers with limited understanding and control over how their personal data is collected, used, and shared. Providers frequently fail to establish clear, transparent, and accessible consent processes, relying on generic or overly complex consent forms that do not provide sufficient detail on the scope of data collection or its intended purposes. As a result, customers may unknowingly consent to the collection of sensitive data or its sharing with third parties, including advertisers, business partners, or other external entities.

This lack of informed consent undermines consumer trust and creates significant privacy risks. Moreover, in many cases, the consent obtained may not meet regulatory requirements, particularly with regards to data protection laws such as the GDPR, which mandates that consent be explicit, specific, and revocable at any time. To mitigate these issues, telecom providers must implement robust and user-friendly consent mechanisms that clearly outline the types of data being collected, the purpose of its use, and the entities with whom it may be shared, while also offering easy-to-understand options for users to manage or withdraw consent

III. Third-Party Sharing

Telecom providers frequently collaborate with third parties, including advertisers, service vendors, analytics companies, and other external partners, to enhance their offerings, improve customer experience, and generate additional revenue streams. However, these partnerships can raise significant privacy and data protection concerns, particularly when it comes to the transparency of data-sharing practices. Telecom providers often do not fully disclose the scope of data shared with these third parties, including the specific types of information exchanged and the purposes for which it will be used.

This lack of transparency can lead to consumer mistrust, as individuals may be unaware that their personal data is being shared or sold to external entities, sometimes for purposes beyond their initial expectations, such as targeted advertising, market analysis, or cross-selling of services.

Moreover, third-party vendors may not always adhere to the same stringent security measures as the telecom providers, increasing the risk of data breaches or misuse. To address these concerns, telecom providers must adopt clearer, more transparent data-sharing practices, including informing customers about the nature of these partnerships, the specific data being shared, and the steps taken to ensure the privacy and security of the information. Clear and accessible opt-in and opt-out mechanisms should also be provided, enabling consumers to make informed decisions about their participation in such data-sharing agreements.

IV. Government Interventions

Telecom companies often find themselves under legal mandates that require them to share subscriber data with government agencies, such as law enforcement, national security, and intelligence bodies. These legal obligations, while typically framed as necessary for national security or criminal investigations, can raise significant concerns regarding privacy infringements and civil liberties. In many cases, telecom providers are compelled to hand over extensive personal data, including call records, browsing history, location data, and even real-time communications, without sufficient oversight or transparency. This can lead to the potential for government overreach, with data being accessed and used in ways that extend beyond the original intent, such as surveillance or monitoring of individuals' activities without clear justification.

The lack of clear, consistent frameworks governing the scope and duration of such data requests further exacerbates these concerns, leaving consumers with little recourse or knowledge about how their personal information is being utilized by government agencies. Additionally, telecom providers may face pressure to comply with these mandates quickly, sometimes at the expense of robust data protection practices.

To mitigate privacy risks and safeguard public trust, it is essential for telecom companies to advocate for stronger safeguards around government data requests, including ensuring that data-sharing practices are narrowly defined, that there is independent oversight of such requests, and that affected consumers are notified where possible.

Furthermore, telecom companies should prioritize the implementation of strong encryption and anonymization techniques to protect subscriber data, ensuring that only the most essential information is shared in compliance with the law.

3.5.2 e -Commerce Sector Analysis

3.5.2.1 Overview of the sector and data collectors evaluated

The e-commerce sector in East and Southern Africa has experienced significant growth in recent years, fueled by rising internet penetration, smartphone usage, and the shift toward digital platforms. Countries like Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda are making notable strides in developing their e-commerce ecosystems, each with unique market dynamics. Rwanda stands out as a digital leader, with a strong focus on innovation and government-backed initiatives like the NICI plan. Tanzania, with its growing mobile internet usage, is seeing e-commerce rise, especially in urban areas, as investment in logistics and digital platforms increases. Mauritius, though smaller, has a well-established digital infrastructure and is positioning itself as a regional hub for luxury goods and tourism. Despite economic challenges, Zimbabwe's e-commerce sector is expanding, particularly in urban areas where digital solutions offer crucial support.

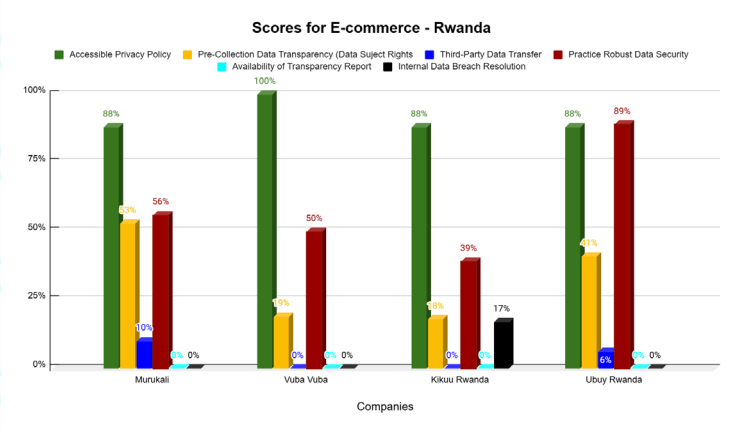
Kenya, a regional innovation leader, is driving e-commerce growth with advanced mobile payment systems like M-Pesa, while Uganda sees increasing adoption of mobile commerce and online services. Together, these countries are shaping a diverse and rapidly evolving e-commerce landscape, offering both opportunities and challenges as digital adoption continues to transform the region's economies.

3.5.2.2 Analysis of compliance with each criterion

The report in this sector covers data from a total of 24 e-commerce platform, with four (4) platforms selected from each country. These include: Murukali, Vuba Vuba, Kikuu Rwanda, and Ubuy Rwanda from Rwanda; Kikuu Tanzania, Jiji Tanzania, Inalipa, and Kupatana from Tanzania; PriceGuru, Temu Mauritius, Marideal, and Woolworths Mauritius Online from Mauritius; Ubuy Zimbabwe, Shumba Africa, Raines Africa, and Tengai Online from Zimbabwe; Jumia Kenya, Glovo Kenya, Jiji Kenya, and Kilimali from Kenya; and Jumia Uganda, Glovo Uganda, Jiji Uganda, and Kikuu Uganda from Uganda. These were assessed and their performance is highlighted below.

a) Murukali, Vuba vuba, kikuu Rwanda and Ubuy Rwanda in Rwanda

All four companies exhibited high compliance for the indicator on an accessible privacy policy with vuba vuba scoring 100%, followed by Murukali, Kikuu Rwanda and Ubuy Rwanda that all scored 88%. This was followed by the performance for the indicator on practice robust data security with Ubuy Rwanda scoring the highest score - 89%. On the other hand, very low compliance levels were exhibited by all the platforms for the indicators on third-party data transfer, internal breach resolution and availability of transparency report. The figure below gives more information with a further detailed discussion on the performance of the different platforms.



All four companies—Murukali, Vuba Vuba, Kikuu, and Ubuy—have publicly available privacy policies as noted above, exceeding 200 words, with 878, 467, 1012, and 1721 words respectively. Vuba Vuba's policy is the most readable, scoring 9 on the Hemingway Editor, while Murukali, Kikuu, and Ubuy scored 12, 10, and 11, making them fairly readable.

Murukali clearly states company details, reasons for data collection, types of data collected, and retention period. It does not list all third parties but does not share data with advertisers. However, it conducts personalized advertising without opt-in options. It conditionally allows access, correction, and deletion of data but does not mention the right to object, restrict processing, or file complaints. Data sharing with law enforcement is permitted upon reasonable request. Ubuy mentions reasons for data collection and data retention but does not provide company contact or location details. It summarizes the types of data collected and does not list all third parties. It does not allow sharing with advertisers but conducts personalized advertising with opt-in options. It conditionally allows data access, correction, restriction, and deletion but does not mention complaint mechanisms or law enforcement access.

Vuba Vuba mentions the reason for data collection but omits company details, data retention period, and user rights (access, correction, restriction, deletion, and complaints). It permits data sharing with advertisers but does not clarify law enforcement access. Kikuu briefly lists the types of data collected and conditionally allows data access, correction, restriction, and deletion. However, it does not include company contact details, data retention period, or complaint mechanisms. It permits advertiser data sharing but does not specify whether law enforcement can access data.

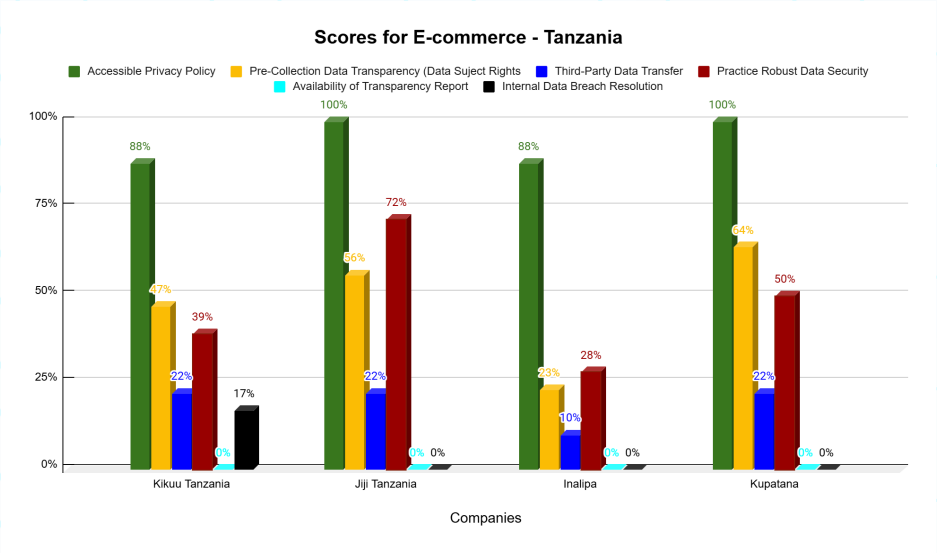
All four companies allow third-party access to personal data without specifying the type of data shared. Only Ubuy lists the third parties it shares data with. Murukali permits sharing data with law enforcement upon reasonable request, while the other policies do not specify law enforcement access. None of the policies specify how data subjects can access data breach resolution mechanisms.

Murukali and Vuba Vuba make no mention of data security. Kikuu mentions data security but lacks specifics. Ubuy details the security measures in place. SSL Server Scored: Murukali (A), Vuba Vuba (A), Kikuu (B), Ubuy (A) while Security Header Scored: Murukali (A), Vuba Vuba (B), Kikuu (Below F), Ubuy (A). None of the companies publish transparency reports, which are essential for data privacy and governance, ensuring users' rights to transparency and compliance monitoring.

Kikuu acknowledges data breaches and mandates user notification, but without a defined timeframe and no clear redress mechanisms. Murukali, Vuba Vuba, and Ubuy do not mention data breaches at all.

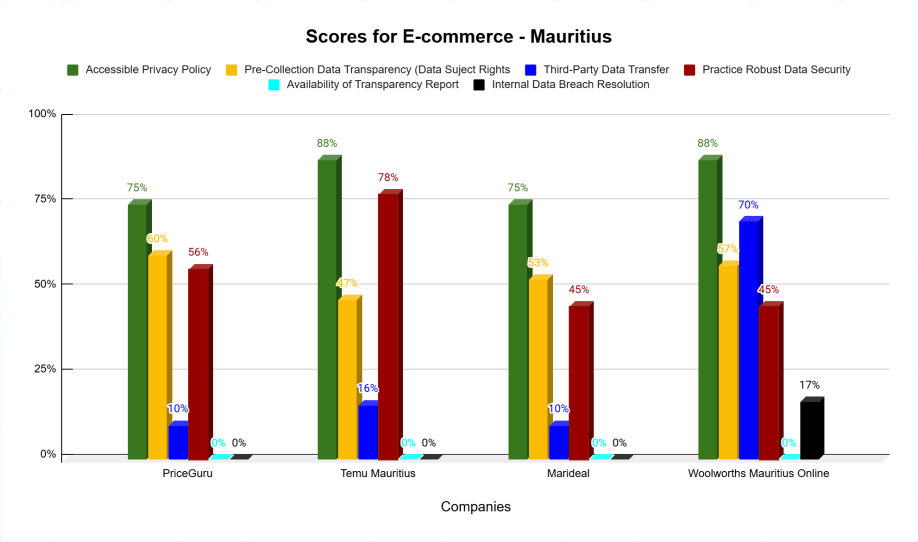
b) *Kikuu Tanzania, Jiji Tanzania, Inalipa and Kupatana in Tanzania*

All four (4) platforms exhibited high levels of compliance with the indicator on having an accessible privacy policy – both Jiji Tanzania and Kupatana scored 100% while Kikuu Tanzania and Inalipa scored 88% respectively. This was closely followed by Jiji Tanzania scoring 72% for compliance with the indictor on practice robust data security and Kupatana scored 64% as the highest mark among all the platforms for compliance with the indicator on pre-collection data transparency. More details are provided in the figure and further discussion on the performance of the platforms is below.



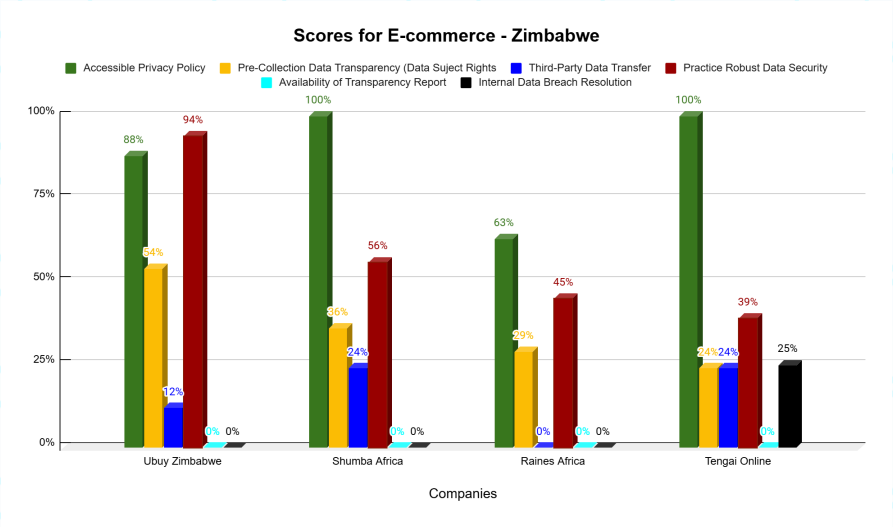
c) *PriceGuru, Temu Mauritius, Marideal and Woolworths Mauritius Online in Mauritius*

All platforms demonstrated more efforts towards compliance with indicators namely; accessible privacy policy, practice robust data security and pre-collection transparency. Temu Mauritius and Woolworths Mauritius online registered the highest mark 88% respectively for demonstrating efforts to comply with having an accessible privacy policy. On the other hand, very low compliance was observed and in some instances 0% was registed in respect of third-party data transfer, internal data breach resolution and availability of a transparency report. The figure below offers additional details and further analysis on the performance of the platforms.



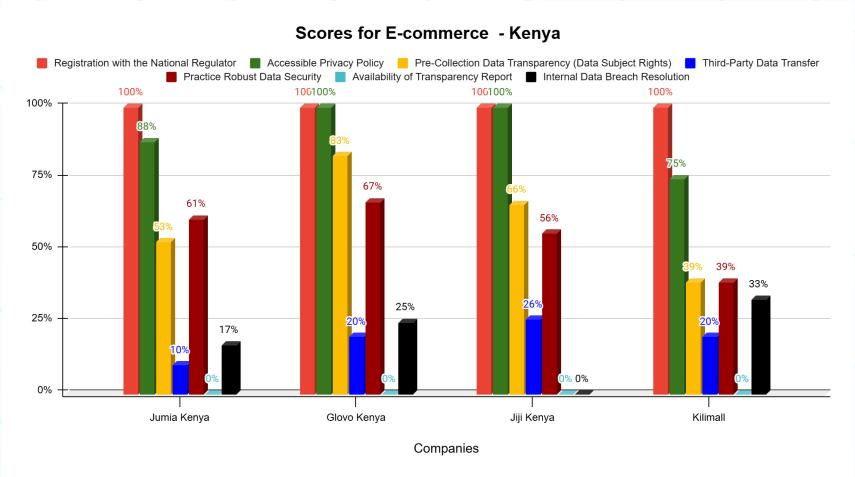
d) Ubuy Zimbabwe, Shumba Africa, Raines Africa and Tengai Online in Zimbabwe

Greater compliance was observed for the indicator on an accessible privacy policy with 63% as the least score. This was closely followed by compliance with the indicator on practice robust data security where the highest score 94% was by Ubuy Zimbabwe. The rest of the scores ranged between 40% to 57%. On the other hand, a very low compliance was observed for indicators on availability of a transparency report and internal breach resolution, with the exception of Tengai Online, the rest had 0%. The figure provides further details, followed by a more in-depth discussion of the platforms' performance below.



e) Jumia Kenya, Glovo Kenya, Jiji Kenya and Kilimali in Kenya

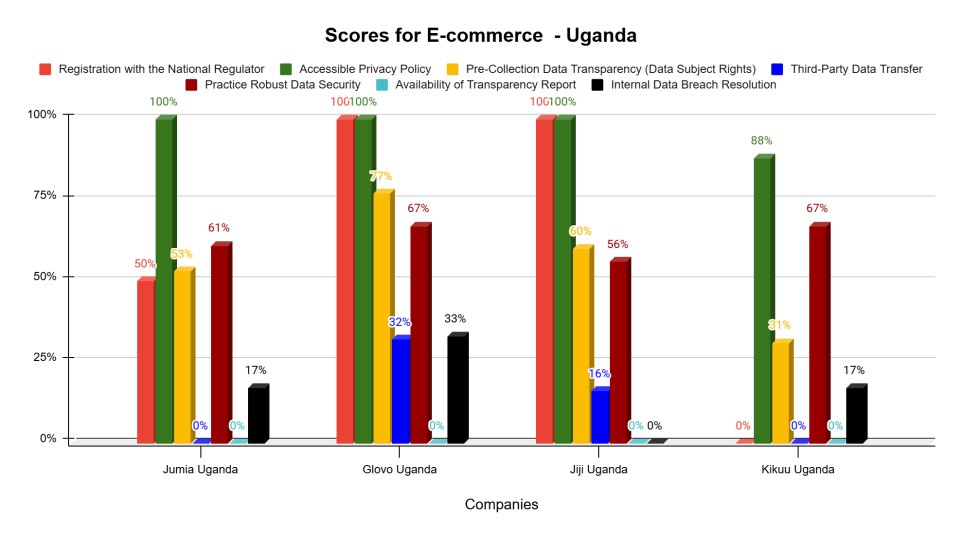
All platforms exhibited efforts to comply with the indicators on an accessible privacy policy and registration with the national regulator with scores of 100% registered. This was closely followed by indicators on pre-collection data transparency and practicing robust data security with Jumia Kenya, Glove Kenya and Jiji Kenya exhibiting some good scores. On the other hand, all platforms did not have a readily avail transparency report and had 0% for this indicator. More details are provided in the figure below, followed by a further analysis of the performance.



f) Jumia Uganda, Glove Uganda, Jiji Uganda and Kikuu Uganda

All four platforms demonstrated strong compliance with the indicator on accessible privacy policies and registration with the national regulator, earning scores as high as 100%.

They also showed notable efforts to comply with indicators on pre-collection data transparency and robust data security. However, none of the platforms had a readily available transparency report, resulting in a score of 0% for this indicator. Efforts were also noted in complying with indicators on internal data breach resolution and third-party data transfer, but these remained very low, with scores as low as 0%. The figure below provides further details, followed by an analysis of the platforms' performance.

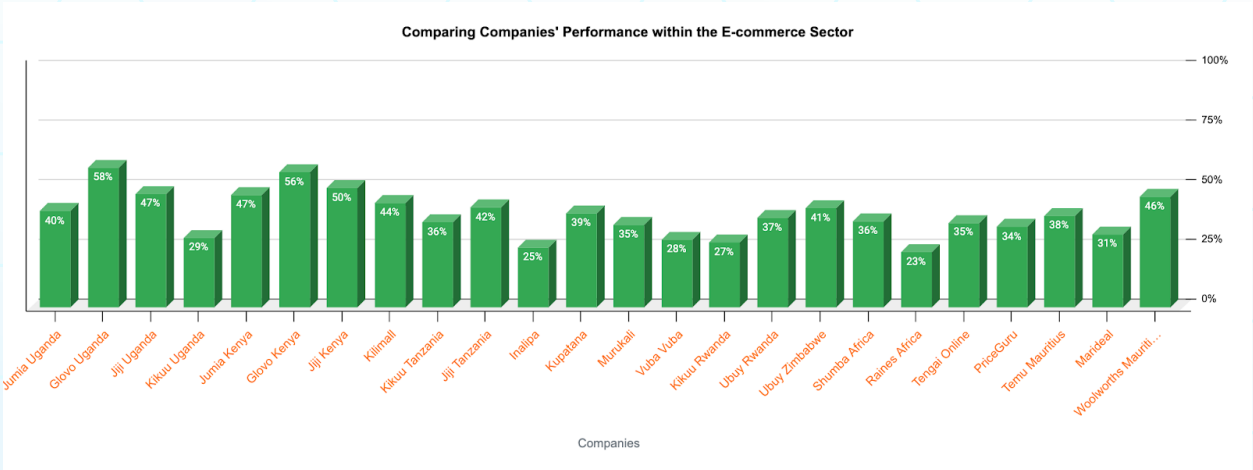


Third-Party Data Sharing is a major concern, with Jumia and Kikuu for allowing undisclosed third-party access, including advertisers, without specifying what data is shared. Even the best performer, Glovo, registered a very low score, indicating widespread non-compliance with privacy best practices. The scores for data security measures show moderate protection levels, though Jiji scores lowest for failing to mention security measures in its policy.

Transparency remains a major issue, as none of these platforms have published a transparency report since 2023, despite their high usage in Uganda. Strengthening oversight and enforcing better compliance are essential for protecting consumer data in Uganda's growing e-commerce sector.

3.5.2.3 Comparison of companies/entities within the sector

Glovo Uganda (58%) and Glovo Kenya (56%) are leading in the sector, , demonstrating robust systems for data management and transparency. Jiji Uganda (47%), Jiji Kenya (50%), and Woolworths Mauritius Online (46%) also show solid commitment to user data protection, though they still have room for improvement to reach the high standards set by Glovo.



Following closely, was Jumia Uganda (40%), Jumia Kenya (47%), and Kilimall (44%), who have made some strides in compliance, but there are still considerable gaps that require attention. These companies need to improve transparency, user consent processes, and cybersecurity to reduce privacy risks. Similarly, Jiji Tanzania (42%), Ubuy Zimbabwe (41%), and Shumba Africa (36%) show moderate efforts in data protection but continue to face difficulties in achieving higher privacy standards.

In contrast, Kikuu Uganda (29%) and Kikuu Rwanda (27%) show significant weaknesses in privacy practices and compliance, putting them at high risk for data breaches, privacy violations, and regulatory non-compliance. Similarly, companies like Inalipa (25%), Vuba Vuba (28%), Raines Africa (23%), and Marideal (31%) score poorly, reflecting a critical lack of attention to user data protection, which increases the likelihood of misuse and exploitation of personal data.

Companies with low scores, such as Inalipa (25%) and Raines Africa (23%), face significant regulatory compliance risks, potentially violating local and international regulations, which could lead to legal penalties, fines, and reputational damage. On the other hand, platforms with higher scores, like Glovo Uganda (58%) and Glovo Kenya (56%), are better able to build consumer trust, as users are more likely to engage with companies they believe protect their data. Companies with lower scores, such as Kikuu Uganda and Inalipa, risk losing customer trust, which could result in decreased user engagement and market share. Additionally, these companies are more vulnerable to data breaches and cyberattacks, which could lead to financial losses and damage to their brand reputation. Mid-tier companies like Jumia and Kilimall have the opportunity to improve by enhancing encryption, refining user consent processes, increasing transparency, and strengthening cybersecurity measures.

Overall, while Glovo leads in data protection, other companies, especially those with scores under 30%, must make significant improvements to comply with regulations, protect user data, and maintain consumer trust in an increasingly privacy-conscious digital world.

3.5.2.4 Identification of sector-specific challenges and best practices

I. Data Collection

Many platforms fail to provide clear specifications regarding the types of personal data they collect, such as names, contact information, payment details, browsing behavior, or location data. Often, users are not fully informed about what personal information is being gathered or how it will be used. This lack of transparency extends to the purpose for which the data is collected, whether it's for improving services, targeted advertising, or sharing with third parties. Without clear, upfront disclosure, users are left in the dark about the extent of their data collection, raising significant concerns about privacy and data misuse.

Additionally, platforms may not offer sufficient options for users to control or limit data collection, leaving individuals vulnerable to over-collection and exploitation of their personal information. To address these concerns, platforms must adopt transparent data collection practices, providing users with clear, easily accessible information about the types of data collected, its intended use, and offering meaningful choices to manage or opt out of data collection where possible.

II. Data Retention

Many platforms lack clear and accessible data retention policies, leaving users uncertain about how long their personal information will be stored. Without defined retention timelines, data may be kept indefinitely, increasing the risk of unauthorized access, data breaches, or misuse. Retaining data longer than necessary also raises concerns regarding privacy violations and potential exploitation of sensitive information.

Clear data retention policies are crucial to ensure that data is only stored for as long as needed to fulfill its intended purpose, after which it should be securely deleted or anonymized. To enhance transparency and protect user privacy, platforms must establish and communicate clear data retention timelines, outlining specific periods for retaining different types of data and ensuring compliance with relevant data protection regulations.

III. Third-Party Transfers

E-commerce platforms frequently collaborate with third-party entities such as logistics providers, payment processors, and marketing agencies to enhance service delivery and streamline operations. However, many platforms fail to disclose these third-party relationships or provide clear information on what data is shared with them. This lack of transparency is concerning, as consumers are often unaware of how their personal information is being accessed, used, or potentially shared beyond the platform.

Such third-party transfers can expose sensitive data to additional risks, especially if these partners do not adhere to the same security standards or privacy practices. To build trust and ensure privacy, e-commerce platforms must be transparent about their third-party relationships, clearly informing users of the data being shared, the purpose of such transfers, and the measures taken to safeguard their information.

IV. Security Measures

Ensuring robust encryption of payment information and user data is a fundamental expectation for any platform handling sensitive information. Without proper encryption, personal and financial data are vulnerable to breaches, theft, and misuse. Implementing end-to-end encryption for transactions and securely storing user data helps protect against unauthorized access, ensuring that sensitive information remains confidential.

In addition to encryption, platforms must employ other security measures, such as multi-factor authentication, secure communication protocols, and regular security audits, to further mitigate risks and enhance data protection. By prioritizing encryption and comprehensive security practices, platforms can foster trust with users, protect their sensitive data, and comply with privacy regulations.

3.5.3 Online Betting Sector Analysis

3.5.3.1 Overview of the sector and data collectors evaluated

The online betting sector in East and Southern Africa has seen rapid growth in recent years, with countries like Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda emerging as key players in the industry. This growth is driven by increasing internet penetration, mobile phone usage, and a growing interest in sports betting and casino games.

While online betting is relatively new, Rwanda has embraced the sector with several licensed operators offering sports betting and casino games. The government has regulated the industry, ensuring compliance with tax and licensing laws. In Tanzania online betting is well-established, with a mix of local and international operators. Football betting is particularly popular, and the sector is regulated by the Gaming Board of Tanzania, which ensures proper oversight and compliance with gaming laws.

As a more mature market, Mauritius has a well-regulated online betting sector, with a strong focus on sports betting. The Gambling Regulatory Authority oversees the industry, ensuring operators comply with strict legal and ethical standards. In Zimbabwe, the online betting market is growing rapidly, especially with the rise of mobile betting. Zimbabwe has implemented a regulatory framework to monitor the sector, with the country's Lotteries and Gaming Board overseeing licensing and compliance.

Kenya is one of the leading markets for online betting in Africa. With a robust mobile payment infrastructure like M-Pesa, betting on sports, especially football, has become a major pastime. The Betting Control and Licensing Board (BCLB) regulates the industry. Online betting is becoming increasingly popular in Uganda, with many local and international operators offering platforms for sports and casino betting. The Uganda Gaming Board is responsible for overseeing the sector and ensuring operators follow legal guidelines.

In all these countries, the online betting industry faces challenges such as addiction, underage gambling, and regulatory issues, but continues to thrive due to the growing demand for accessible, digital gaming experiences.

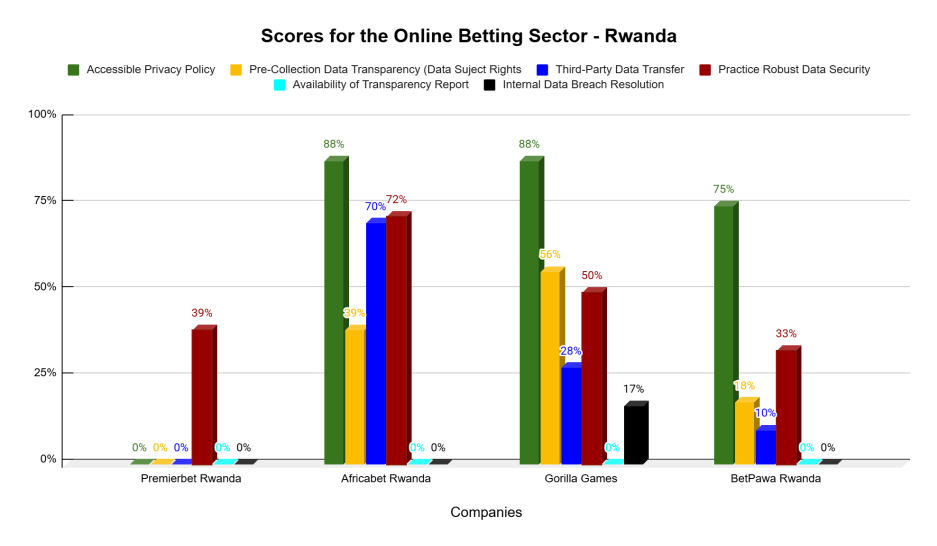
3.5.3.2 Analysis of compliance with each criterion

The report in this sector includes data from 24 companies in total, with four (4) companies chosen from each country.

These consisted of: Premierbet Rwanda, Africabet Rwanda, Gorilla Games and BetPawa Rwanda from Rwanda; SportPesa Tanzania, Betika Tanzania, Bikosports and SportyBet from Tanzania; Supertote, Stevenhills Mauritius, Totelepep Ltd and William Hill from Mauritius; Bezbets, Africabet, Mrbet and Pinnacle Sports from Zimbabwe; Ixbet Kenya, Betika Kenya, BetPawa Kenya and SportPesa Kenya from Kenya and; Ixbet Uganda, Forbet, BetPawa Uganda and 22bet Uganda from Uganda.

a) Premierbet Rwanda, Africabet Rwanda, Gorilla Games and BetPawa Rwanda in Rwanda

With the exception of Premierbet Rwanda, which showed minimal effort in ensuring compliance, the other companies evaluated demonstrated a higher level of adherence. Notably, Africabet Rwanda and Gorilla Games both scored 88% on the accessibility of their privacy policies, while BetPawa Rwanda scored 75%. However, all companies were found lacking a transparency report, resulting in a 0% score for this indicator. Further details on the companies' performance are provided in the figure below, followed by an in-depth analysis.



Among the four companies assessed, PremierBet Rwanda lacks a privacy policy, while Africabet Rwanda, Gorilla Games, and BetPawa have publicly available policies. However, only Africabet and Gorilla Games have policies that are clearly noticeable on their websites. BetPawa's policy is the most readable, scoring 7 on the Hemingway Editor, with 369 words. Gorilla Games and Africabet have fair readability, scoring 11 and 13 respectively, with word counts of 4812 and 664.

Gorilla Games provides contact details, clearly states data collection reasons, types of data collected, and retention periods as required by law. It allows third-party and advertiser data sharing, with personalized ads subject to an opt-out mechanism. It conditionally grants rights to access, correction, deletion, and restriction of processing, but does not mention the right to complain. Law enforcement agencies have access to data. Africabet lacks contact details but states data collection purposes without detailing the specific data collected or retention period. It does not allow third-party sharing and requires opt-in consent for personalized ads. Data subjects can conditionally access, correct, or delete their data, but the policy does not mention the right to complain. Law enforcement has access to data. BetPawa only mentions data collection purposes, data categories, and law enforcement access but does not provide other essential privacy details.

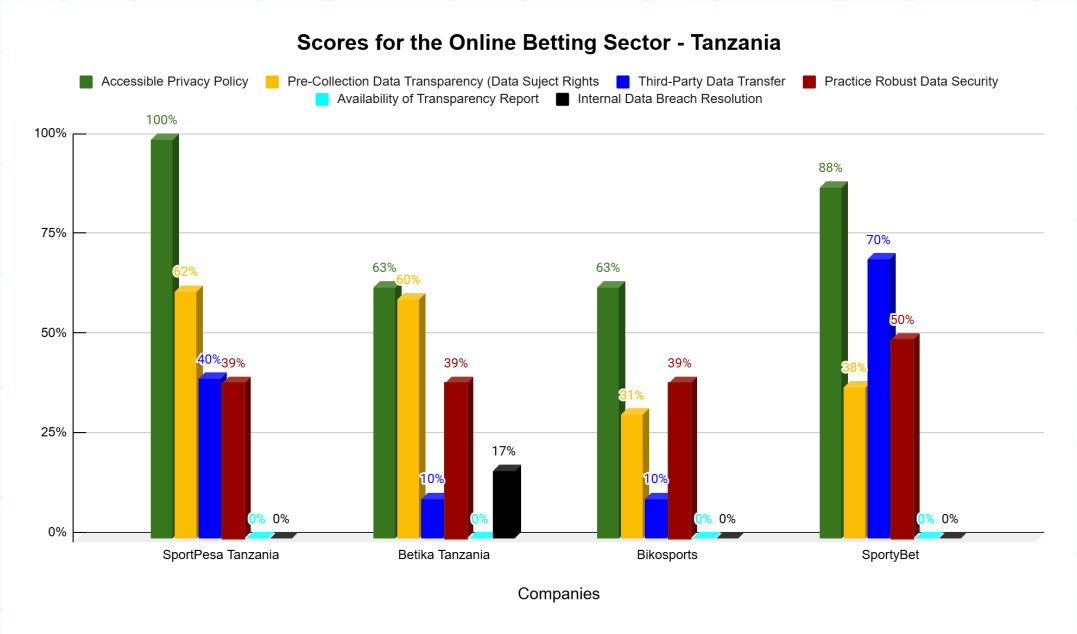
Africabet does not share data with third parties or advertisers, though it allows law enforcement access upon reasonable request. However, it does not specify data breach resolution mechanisms. Gorilla Games lists third parties it shares data with, identifies specific data shared, and allows law enforcement access. PremierBet and BetPawa make no mention of data security, while Gorilla Games and Africabet reference security but without specifics.

An outlook on security and transparency scores shows that SSL Server Scored: Africabet (A), Gorilla Games (A+), BetPawa (B), PremierBet (B) while, Security Header Scored: Africabet (D), Gorilla Games (B), BetPawa (D) and PremierBet (D). None of the companies publish transparency reports.

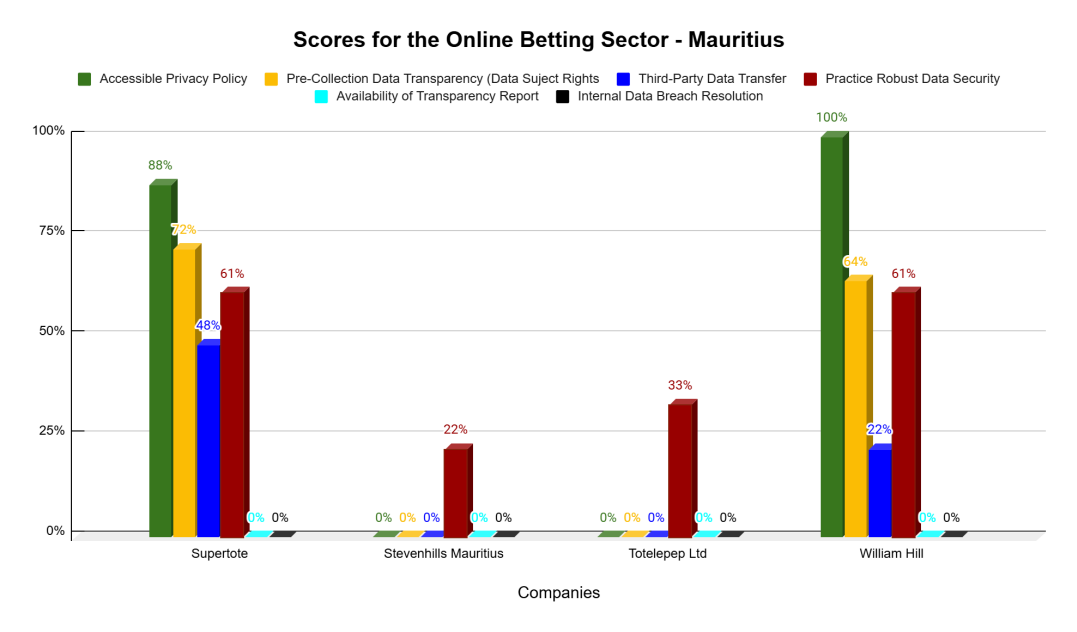
Gorilla Games acknowledges data breaches and requires user notification, but without a specified timeframe or redress mechanism. Africabet, BetPawa, and PremierBet do not mention data breaches or their resolution.

b) *SportPesa Tanzania, Betika Tanzania, Bikosports and SportyBet in Tanzania*

All four companies scored well for having accessible privacy policies, with SportPesa Tanzania and SportyBet leading, followed by Betika Tanzania and Bikosports, both scoring 63%. However, they all performed poorly in other critical areas, scoring as low as 0% for the availability of a transparency report and internal data breach resolution. This indicates that while these companies are taking steps to make their privacy policies accessible, they are lacking in crucial practices including for transparency and handling data breaches, which could leave user data vulnerable and impact their overall data protection efforts.



c) *Supertote, Stevenhills Mauritius, Totelepep Ltd and William Hill in Mauritius*

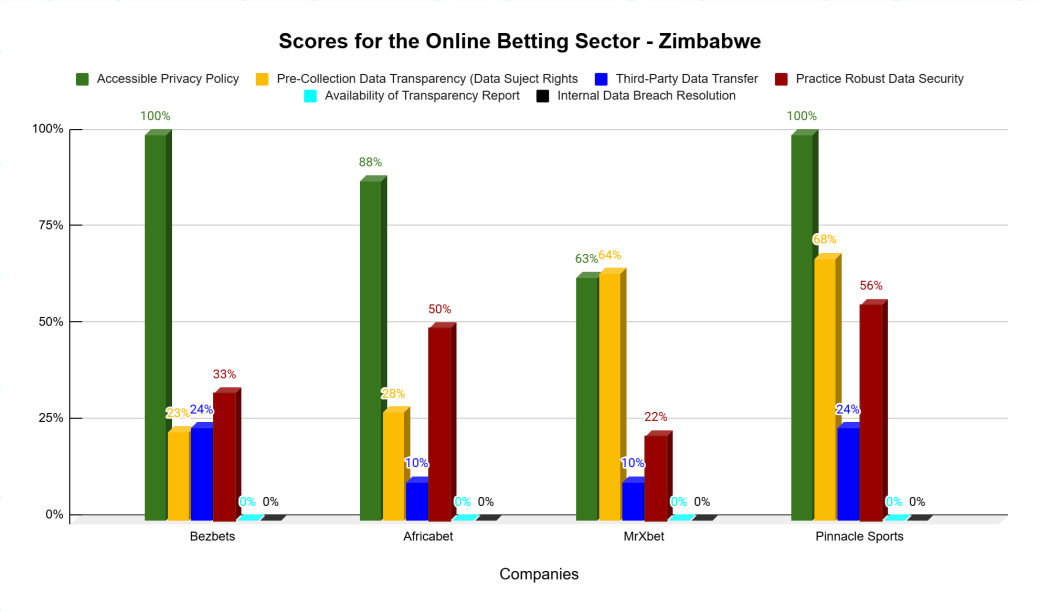


Of the four companies, two showed strong performance in having accessible privacy policies, with William Hill achieving the highest score and Supertote scoring 80%. However, Stevenhills Mauritius and Totelepep Ltd performed poorly, scoring just 22% and 33% respectively in data security practices. Still, both companies also scored 0% in other critical areas, including the availability of a transparency report, internal data breach resolution, accessible privacy policies, and pre-collection data transparency, indicating significant gaps in their overall data protection practices.

Having in place accessible privacy policies, is an important step in informing users about how their data is handled. However, Stevenhills Mauritius and Totelepep Ltd show serious gaps in their privacy practices. Their low scores in data

security (22% and 33%) suggest they may not be adequately protecting user information from breaches or cyberattacks. Moreover, their failure to provide transparency reports, implement internal data breach resolution mechanisms, or be transparent about data collection processes (scoring 0% in these areas) indicates a lack of commitment to key privacy principles, which could expose users to data risks and legal vulnerabilities. Overall, this suggests that while some companies are taking positive steps toward privacy, others need significant improvements to meet basic data protection standards and ensure user trust.

d) Bezbets, Africabet, Mrbet and Pinnacle Sports in Zimbabwe



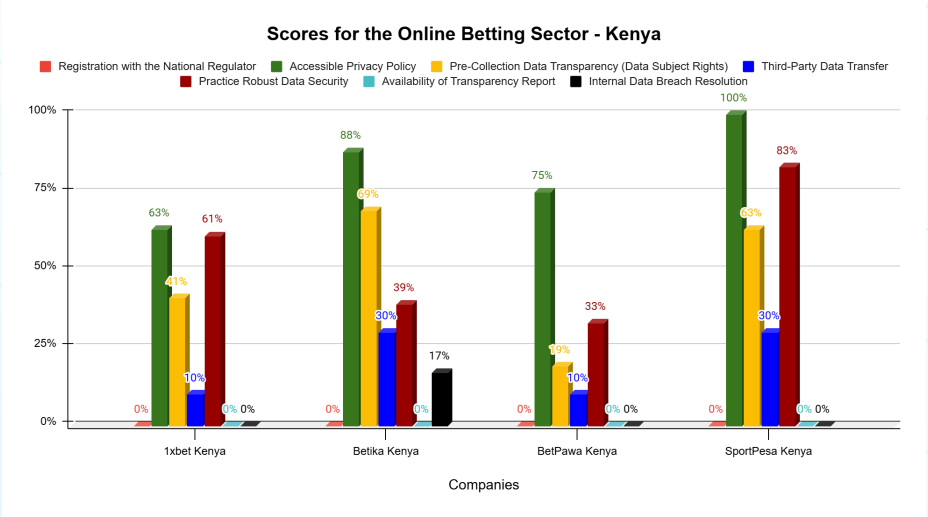
The performance of the four companies in the above figure shows varying levels of compliance and transparency. Bezbets and Pinnacle Sports lead with perfect scores (100%) for accessible privacy policies, demonstrating strong transparency. Africabet follows closely with 88%, while MrXbet trails at 63%.

Regarding pre-collection data transparency, Pinnacle Sports leads at 68%, closely followed by MrXbet at 64%. However, in terms of data security, Pinnacle Sports scores the highest at 56%, with Africabet at 50%.

All four companies performed poorly in areas like transparency reports and internal data breach resolution, as none of them scored above 0% in these categories, indicating a significant gap in these critical privacy practices.

e) Ixbet Kenya, Betika Kenya, BetPawa Kenya and SportPesa Kenya in Kenya

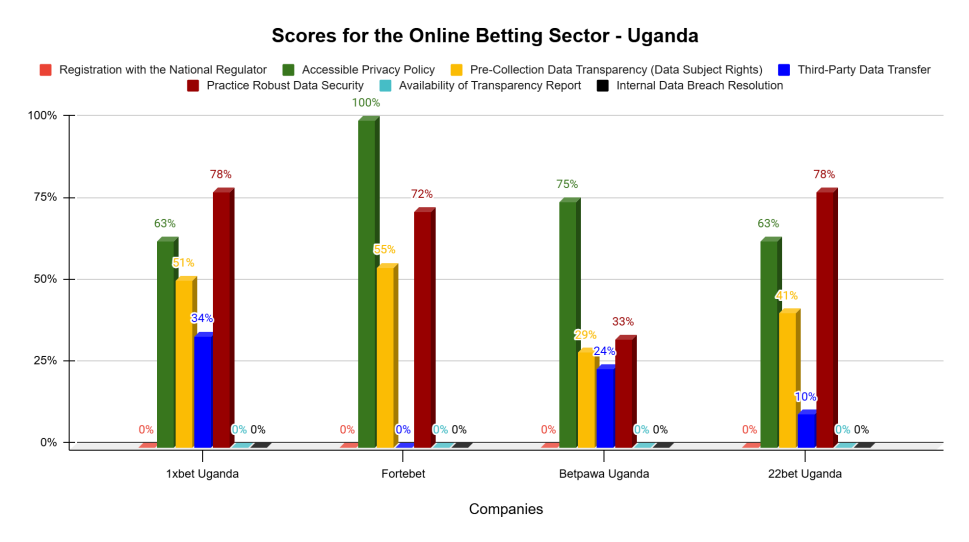
The performance of the four companies in the figure below shows some variation. SportPesa Kenya leads with a perfect score of 100% for accessible privacy policies, followed by Betika Kenya at 88%, BetPawa Kenya at 75%, and 1xbet Kenya at 63%. In terms of data security, SportPesa Kenya scored the highest at 83%, while 1xbet Kenya scored 61%. Betika Kenya led in pre-collection data transparency with 69%, while SportPesa Kenya followed closely at 63%.



However, all four companies performed poorly in key areas such as non-registration with national regulators, lack of transparency reports, and internal data breach resolution, receiving a 0% score in these categories. Additionally, they all scored below 50% for third-party data transfer, indicating significant gaps in their overall privacy practices and compliance with their respective data protection laws.

f) Ixbet Uganda, Forbet, BetPawa Uganda and 22bet Uganda in Uganda

All companies were recognized for having accessible privacy policies, with Fortebet leading at 100%, followed by Betpawa Uganda at 75%, and 1xBet Uganda and 22bet Uganda tied at 63%. In terms of data security, 1xBet Uganda and 22bet Uganda scored the highest at 78%, with Fortebet close behind at 72%.



While these scores suggest strong privacy and data protection practices, the companies' low scores in areas such as non-registration with the national regulator, lack of transparency reports, and inadequate internal data breach resolution reveal significant compliance gaps.

Although 1xBet Uganda and 22bet Uganda demonstrated strong data security, they need to improve transparency and regulatory compliance. The low scores in pre-collection data transparency (50%) for 1xBet Uganda and Fortebet, and the 0% scores for all companies in non-registration with the national regulator, lack of transparency reports, and internal data breach resolution, further emphasize the need for clearer data handling practices and better adherence to regulatory standards.

None of the four leading platforms—1xbet, Fortebet, Betpawa, and 22bet—are registered with Uganda's national data privacy regulator. While Fortebet leads in privacy policy accessibility, the other platforms do not prominently display their policies, making it harder for users to find and understand them. Data Subject Rights compliance is weak across the sector, with Betpawa performing worst due to its failure to acknowledge key user rights like data deletion and complaint mechanisms. Even Fortebet lacks transparency on third-party data sharing and law enforcement access.

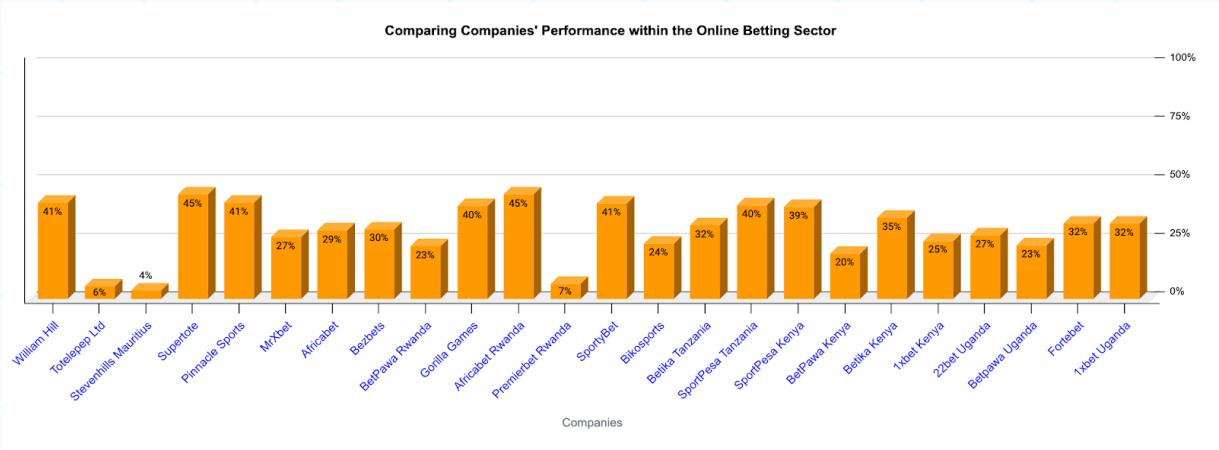
Third-party data transfer is a major concern, as all four companies allow sharing of personal data with advertisers and other entities without specifying what data is shared. Fortebet registered low compliance levels, offering users no protection against unauthorized data sharing. Data security scores are generally fair, except for Betpawa, which does not mention security measures and has a poor security rating (D) for its website.

None of the companies have published a transparency report since 2023, and all registered poor performance in internal data breach resolution, highlighting a lack of commitment to addressing data security incidents. Stricter regulations and enforcement are needed to protect users in this expanding sector.

3.5.3.3 Comparison of companies/entities within the sector

The performance of various online betting platforms shows significant variability in their compliance and privacy practices. In Uganda, 1xBet Uganda and Fortebet both score 32%, while Betpawa Uganda and 22bet Uganda scored lower at 23% and 27%, respectively. This suggests that while some companies are making efforts, there are notable gaps in their overall privacy and data protection practices.

In Kenya, Betika Kenya leads with 35%, followed by SportPesa Kenya at 39%, but 1xBet Kenya and BetPawa Kenya trail with 25% and 20%, respectively, indicating room for improvement, especially in transparency and regulatory adherence.



In Tanzania, SportPesa Tanzania and SportyBet lead with 40% and 41%, while Bikosports (24%) and Betika Tanzania (32%) have weaker scores, suggesting that companies in Tanzania may need to enhance their data security measures and regulatory compliance. Rwanda shows mixed performance, with Africabet Rwanda (45%) ranking highest, followed by Gorilla Games at 40%.

Premierbet Rwanda, with just 7%, highlights significant deficiencies in privacy and data protection practices. Zimbabwe's Pinnacle Sports and Bezbets lead with 41% and 30%, respectively, while Africabet (29%) and MrXbet (27%) perform poorly in comparison, signaling the need for stronger privacy measures.

Mauritius demonstrates a stark contrast with most companies performing poorly: Stevenhills Mauritius and Totelepep Ltd score just 4% and 6%, respectively, while Supertote and William Hill Mauritius score 45% and 41%, respectively. The generally low scores in Mauritius, alongside lower scores in countries like Uganda, Kenya, and Zimbabwe, indicate serious concerns regarding the privacy and data protection practices of many platforms, particularly in transparency, registration with national regulators, and internal data breach resolution.

Overall, the low overall percentages across many platforms point to significant gaps in privacy and data protection practices, with many companies failing to meet basic standards of transparency and regulatory compliance. These results highlight the urgent need for these platforms to enhance their privacy policies, strengthen data security, and improve their adherence to national data protection regulations to build trust and ensure the protection of user data.

3.5.3.4 Identification of sector-specific challenges and best practices

I. Transparency

Betting platforms often fail to provide sufficient transparency regarding how they collect, process, and store user data. Many users are unaware of the types of personal and financial information being gathered, the purposes for which it is used, or how long it is retained. This lack of clarity can lead to concerns about data misuse, unauthorized access, and compliance with privacy regulations. For platforms to build trust with users, it is essential to clearly disclose their data collection practices, outline how user data will be processed, and provide information on data retention policies. Transparency around these processes empowers users to make informed decisions about their participation, ensuring that their data is handled securely and in compliance with applicable privacy laws.

II. Third-Party Partnerships

Many platforms rely on third-party software providers for various services, such as payment processing, analytics, and customer support. While these partnerships can enhance functionality, they also raise significant concerns about data access and protection.

Third-party vendors may have access to sensitive user information, increasing the risk of data breaches, unauthorized use, or inadequate security practices if these providers do not adhere to the same privacy standards as the platform itself. To mitigate these risks, platforms must ensure that third-party partnerships are governed by strict data protection agreements, conduct thorough security assessments, and regularly audit third-party practices to ensure compliance with privacy regulations and maintain the integrity of user data. Transparency about these partnerships is also essential, as users should be aware of which third parties have access to their information and for what purposes.

III. Financial Data Security

Many platforms fail to implement robust security measures to adequately protect sensitive financial data, such as credit card details, banking information, and transaction history, from potential breaches. Without strong encryption, secure payment gateways, and proper data access controls, financial information becomes vulnerable to cyberattacks, fraud, and identity theft. Additionally, platforms may not regularly update or audit their security systems, further exposing users to risks. To safeguard financial data, platforms must adopt advanced security protocols, such as end-to-end encryption, tokenization, and multi-factor authentication, alongside continuous monitoring and vulnerability assessments. Ensuring these security measures are in place is essential not only for protecting users but also for maintaining trust and complying with financial regulations.

IV. Addiction Monitoring

Platforms often monitor user behavior to promote responsible betting and prevent gambling addiction. However, many of these platforms lack clear, transparent policies outlining how the data collected through monitoring is used. This absence of clarity raises concerns about potential exploitation, such as using behavioral insights for targeted marketing or manipulating vulnerable users.

To address these issues, platforms must implement transparent policies that specify how monitoring data is handled, ensure it is used solely for responsible gambling practices, and limit its use to protect user privacy. Additionally, they should provide users with the ability to access, control, and opt-out of certain forms of monitoring, fostering a safer and more ethical betting environment.

3.5.4 Banks and Finance Sector Analysis

3.5.4.1 Overview of the sector and data collectors evaluated

The banking and finance sector in east and southern Africa plays a crucial role in the economic landscape of each country being assessed, serving as a key facilitator of financial services, including savings, loans, and investments. As financial institutions handle sensitive customer information, including personal and financial data, their compliance with privacy and data proctection laws and data security measures is critical. This sector plays a pivotal role in ensuring that individuals' financial data is securely managed and protected from breaches or unauthorized access.

In Uganda, Kenya, and Tanzania, the sector is relatively well-developed, with a mix of local and international banks offering a wide range of financial products. Kenya, in particular, stands out for its innovative mobile banking services like M-Pesa, which have revolutionized financial inclusion. Mauritius, with its well-established financial sector, is a regional financial hub in the Indian Ocean, attracting international investments. Rwanda's banking sector has seen rapid growth, driven by government reforms aimed at improving financial services and digital banking.

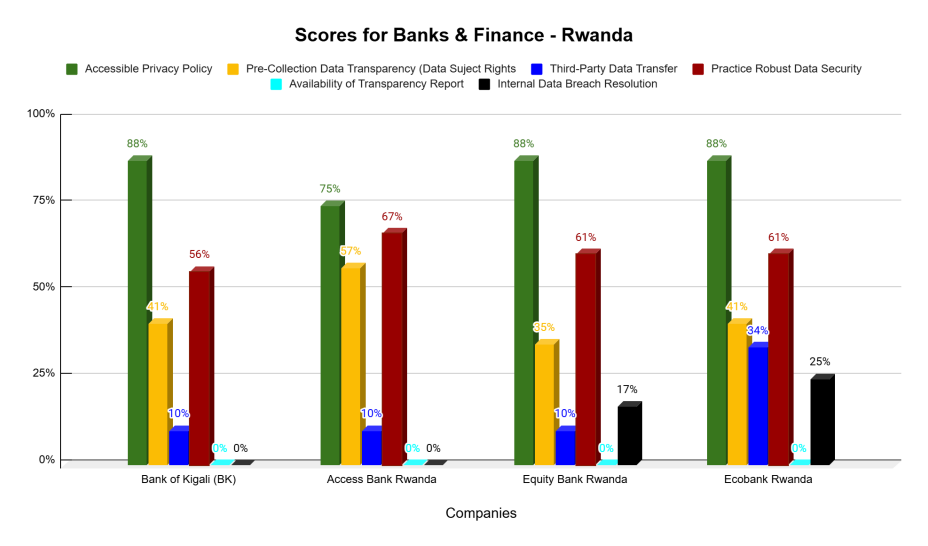
In Zimbabwe, the sector has faced challenges due to economic instability and currency issues, but remains essential for both local and international transactions. Overall, while each country has made strides in financial services, the sector across these nations is increasingly focused on improving digital banking services, regulatory frameworks, and data protection measures to build consumer trust and ensure the secure handling of financial data.

The evaluation covers a range of banks and financial institutions, examining their transparency, adherence to regulatory requirements, and the effectiveness of their privacy practices. Given the importance of financial data in today's digital economy, the findings in this report shed light on how well these companies are safeguarding their customers' privacy and the areas where improvements are necessary to ensure robust protection in line with global standards.

3.5.4.2 Analysis of compliance with each criterion

a) Bank of Kigali, Access Bank Rwanda, Equity Bank Rwanda and Ecobank Rwanda in Rwanda

The four financial institutions evaluated were recognized for having accessible privacy policies, with Bank of Kigali, Equity Bank Rwanda, and Ecobank Rwanda leading at 88%, followed by Access Bank Rwanda at 75%. These institutions also demonstrated compliance in data security, with Access Bank Rwanda scoring the highest at 67%, closely followed by Equity Bank Rwanda and Ecobank Rwanda at 61%, and Bank of Kigali at 56%.



However, their performance in other areas was notably weaker. Access Bank Rwanda led in pre-collection data transparency with a score of 57%, while Bank of Kigali and Ecobank Rwanda scored 41% each, and Equity Bank Rwanda scored 35%. In terms of third-party data transfers, Ecobank Rwanda was the leader at 34%, while the other banks scored just 10%. Despite some strengths in specific areas, all institutions performed poorly in areas such as transparency reports and internal data breach resolution, with each scoring 0%. These results indicate that while these banks have made strides in privacy policies and data security, significant improvements are needed in transparency, third-party data handling, and breach management to strengthen their overall privacy practices.

All four banks—Bank of Kigali, Access Bank Rwanda, Equity Bank Rwanda, and Ecobank as already observed had publicly available data policies, but with varying levels of readability and comprehensiveness. Access Bank Rwanda's policy is the least readable, scoring 14 on the Hemingway Editor. Bank of Kigali's policy scored 13, while Equity Bank and Ecobank were slightly more readable at 12. Equity Bank's policy is the longest (5877 words), while Access Bank's is the shortest (1675 words).

Access Bank and Bank of Kigali do not provide contact details but outline data collection purposes and types of data collected. Both permit third-party and advertiser data sharing, allowing opt-out for personalized ads.

They mention rights to access, correction, restriction of processing, and deletion, with Access Bank granting unconditional rights and Bank of Kigali making deletion unconditional. Neither mentions the right to complain. Law enforcement has access upon reasonable request. Ecobank also lacks contact details but specifies data retention periods while omitting reasons for collection. It does not permit third-party or advertiser data sharing but references personalized ads without opt-in or opt-out options. It mentions conditional access rights and the right to complain, with law enforcement access upon reasonable request. Equity Bank does not provide contact details or retention periods but states data collection reasons and types of data collected. It allows third-party and advertiser data sharing, with an opt-out for personalized ads. It includes rights to deletion, correction, and restriction of processing (conditionally) but omits rights to access and to complain. Law enforcement access is unspecified.

Ecobank does not share data with advertisers, allows law enforcement access, and provides a limited method for reporting data breaches. Bank of Kigali, Access Bank, and Equity Bank scored 10% for privacy protection, as their policies only mention law enforcement access upon reasonable requests. Bank of Kigali, Access Bank, and Ecobank reference data security but lack specifics, while Ecobank specifies some security measures.

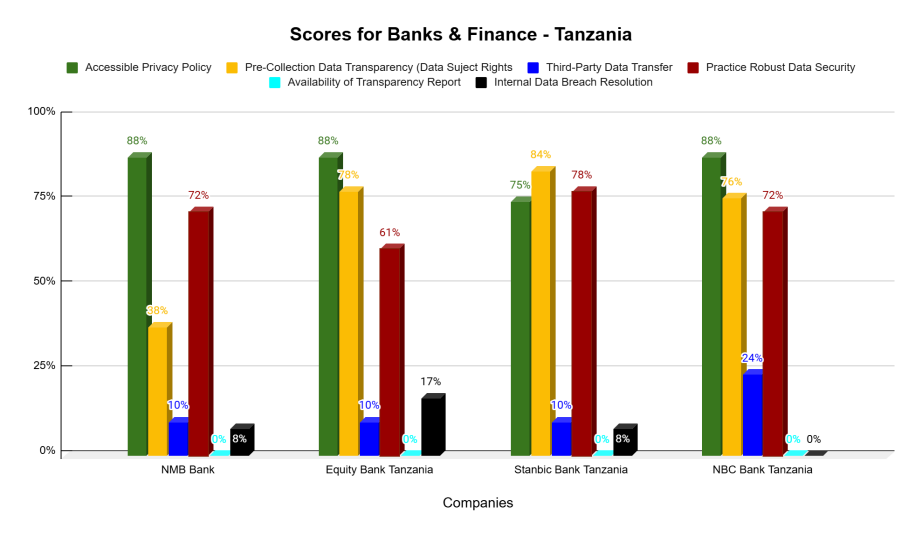
Security and transparency scores revealed that the SSL Server Scored: Bank of Kigali (A), Access Bank (A), Ecobank (A+), Equity Bank (F). while, the Security Header Scored: Bank of Kigali (D), Access Bank (B), Ecobank (D), Equity Bank (A). None of the banks publish transparency reports.

Ecobank provides clear instructions on reporting suspected data breaches, allowing reports via email. Equity Bank mentions data breaches and requires user notification but does not provide specific redress mechanisms or a resolution timeframe. Bank of Kigali and Access Bank do not mention data breaches or redress mechanisms.

b) *NMB Bank, Equity Bank Tanzania, Stanbic Bank Tanzania and NBC Bank Tanzania in Tanzania*

The figure below highlights the performance of various Tanzanian banks in relation to their privacy practices. Three institutions—NMB Bank, Equity Bank Tanzania, and NBC Bank Tanzania—earned high marks for having accessible privacy policies, each scoring 88%. Stanbic Bank Tanzania followed with a score of 75%. In terms of pre-collection data transparency, Stanbic Bank Tanzania excelled with 84%, while Equity Bank Tanzania and NBC Bank Tanzania scored 78% and 76%, respectively.

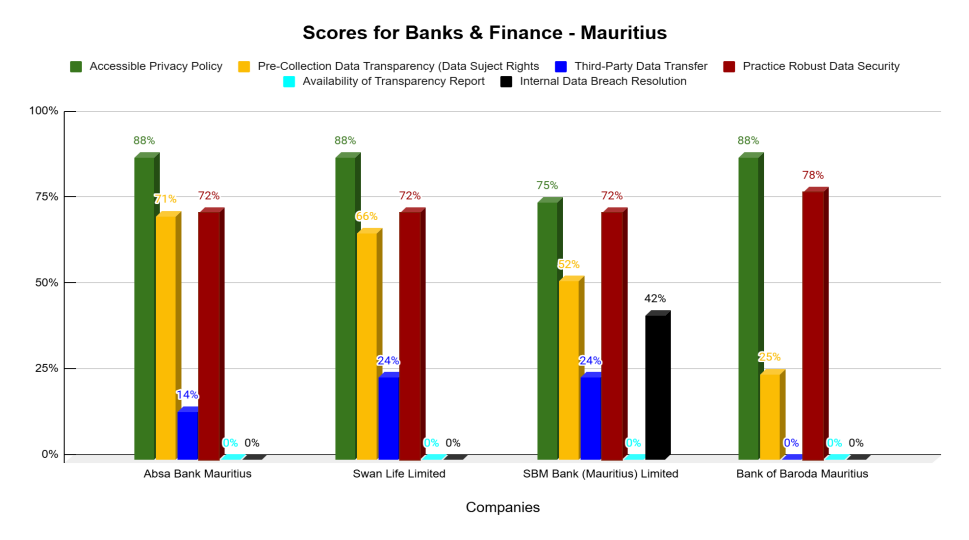
All institutions demonstrated compliance with data security, with Stanbic Bank leading at 78%, followed by NMB Bank and NBC Bank Tanzania at 72%, and Equity Bank Tanzania at 61%.



However, the report also pointed out significant weaknesses, particularly in the area of third-party data transfers, where NMB Bank, Equity Bank Tanzania, and Stanbic Bank Tanzania scored a mere 10% each. Additionally, all banks showed inadequate practices regarding transparency reports and internal data breach resolution, suggesting potential vulnerabilities in their overall data protection frameworks. These performance scores indicate that while some institutions are advancing in privacy and data protection, there is considerable room for improvement, especially in transparency and third-party data handling.

c) *ABSA Bank Mauritius, Swan Life Limited, SBM Bank (Mauritius) Limited and Bank of Baroda Mauritius in Mauritius*

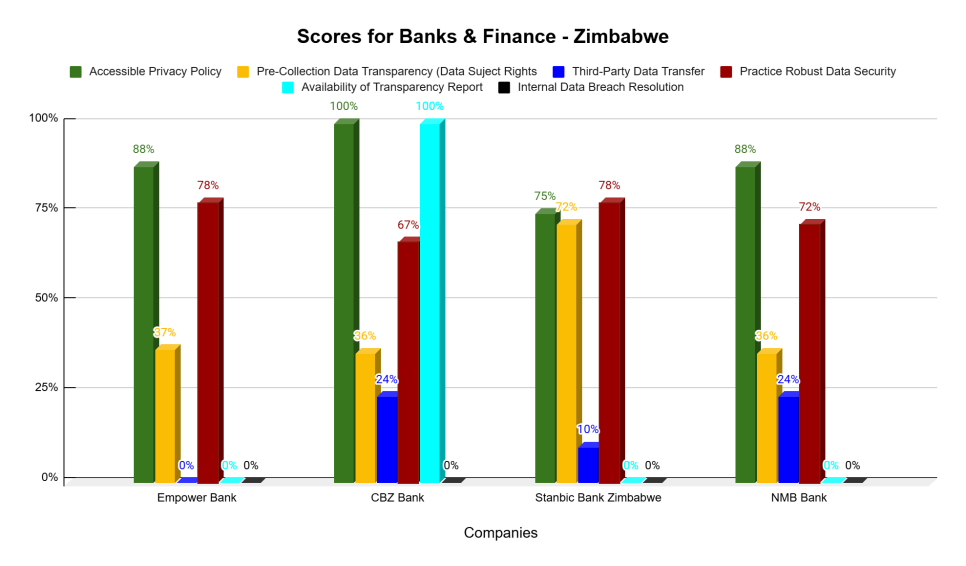
The figure highlights the privacy practices of various banks and institutions, revealing key areas of strength and weakness. All institutions were commended for having accessible privacy policies, with ABSA Bank, Swan Life Limited, and Bank of Baroda leading at 88%, followed by SBM Bank at 75%. In terms of data security, Bank of Baroda scored the highest at 78%, while ABSA Bank, Swan Life Limited, and SBM Bank scored 72% each. ABSA Bank also led in pre-collection data transparency with a score of 71%, followed by Swan Life Limited and SBM Bank at 66% and 52%, respectively.



However, the institutions showed significant weaknesses in compliance with third-party data transfers, transparency reports, and internal data breach resolution. Notably, Swan Life Limited and SBM Bank scored only 24% each in this area, ABSA Bank scored 14%, and the remaining institutions scored 0%. These weaknesses indicate a considerable gap in their privacy practices, particularly in critical aspects of data handling and breach management, which could have serious implications for customer trust and regulatory compliance.

d) Empower Bank, CBZ Bank, Stanbic Bank Zimbabwe and NMB Bank in Zimbabwe

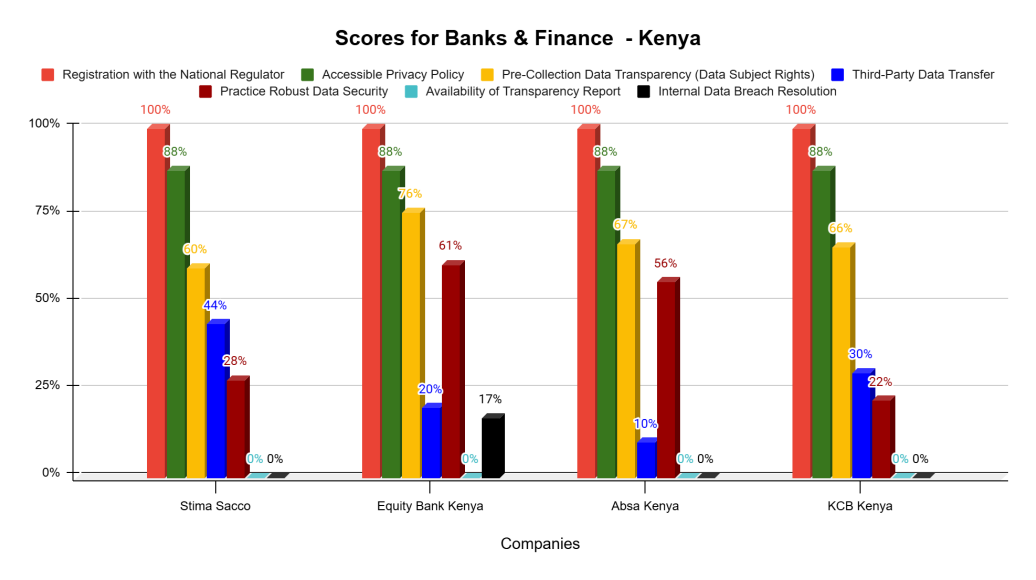
The figure reveals several strengths and areas of concern on the privacy practices of assessed banking institutions in Zimbabwe. All institutions were recognized for having accessible privacy policies, with CBZ Bank leading with a perfect score of 100%, followed by Empower Bank and NMB Bank at 88% each, and Stanbic Bank at 75%. In terms of data security, Empower Bank and Stanbic Bank stood out with strong performances, both scoring 78%, while NMB Bank and CBZ Bank followed with scores of 72% and 67%, respectively. Stanbic Bank excelled in pre-collection data transparency, scoring 72%, while other banks scored below 50%. However, significant weaknesses were observed in compliance with third-party data transfers.



CBZ Bank and NMB Bank scored 24% each, Stanbic Bank scored 10%, and the remaining institutions scored 0%. Additionally, all banks displayed poor performance in transparency reports and internal data breach resolution. Notably, CBZ Bank was the only institution with a transparency report, earning a perfect score of 100%. These performance gaps suggest that while some banks demonstrate solid privacy practices in certain areas, overall improvements are needed, particularly in third-party data transfers, transparency, and breach resolution, to ensure better data protection and compliance with privacy regulations.

e) Stima Sacco, Equity Bank Kenya, ABSA Kenya and KCB Bank in Kenya

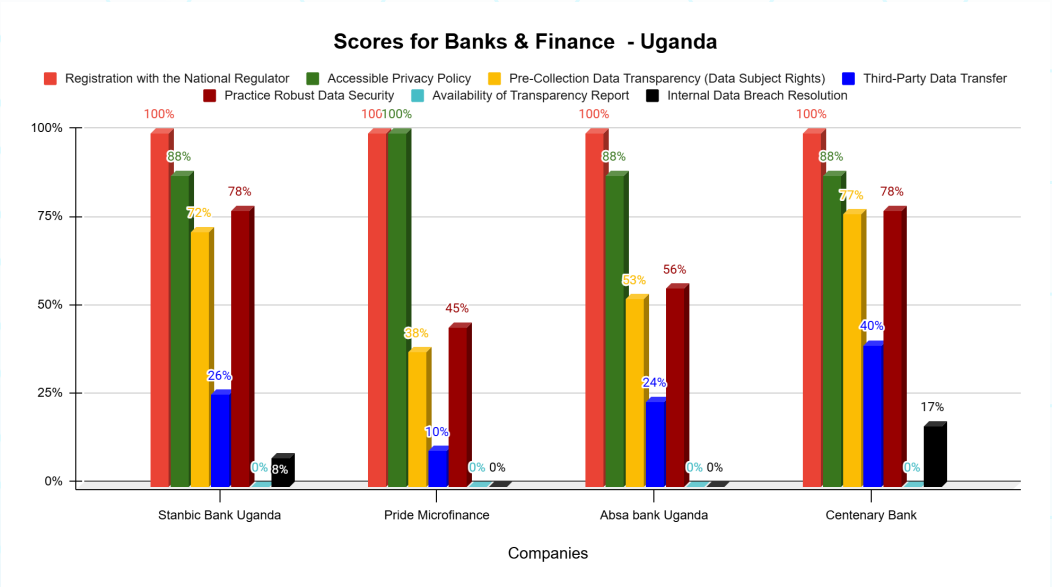
The figure below on the privacy practices of banking institutions in Kenya highlights both strengths and notable gaps in compliance. All assessed institutions received a perfect score of 100% for registering with the national regulator, marking an important first step toward privacy compliance. Similarly, each bank scored 88% for having accessible privacy policies. In terms of pre-collection transparency, Equity Bank led the sector with a score of 76%, followed by ABSA Kenya at 67%, KCB Kenya at 66%, and Stima Sacco at 60%.



However, the performance in data security was less impressive, with only Equity Bank and ABSA Bank scoring 61% and 56%, respectively, while the other institutions had scores below 50%. A similar trend was observed in the area of third-party data transfers, where most banks performed poorly. Furthermore, all institutions displayed significant weaknesses in adhering to transparency reports and internal data breach resolution, receiving a score of 0% in these critical areas. The poor performance in data security, third-party transfers, and breach resolution suggests that while the banks have made progress in some areas, there is a pressing need for improvement in safeguarding customer data, ensuring transparency, and addressing data breaches effectively to enhance overall privacy practices.

f) Stanbic Bank Uganda, Pride microfinance, ABSA Bank Uganda and Centenary Bank in Uganda

The figure highlights the performance of various banking institutions in terms of their privacy practices. The assessment of Stanbic Bank, Pride Microfinance, ABSA, and Centenary Bank highlights both strengths and critical gaps in data protection practices. All four banks achieved a 100% score for registration with Uganda's National Regulator (NITA-U), ensuring regulatory oversight. They also have accessible privacy policies, with Pride Microfinance leading at 100% and the rest scoring 88%, though clarity and conciseness remain areas for improvement. Centenary Bank (77%) and Stanbic Bank (72%) lead in pre-collection data transparency, being the only banks to explicitly list their contact details.



Centenary also ranks highest in data subject rights, offering provisions for access, correction, deletion, and complaint lodging. Stanbic follows closely but imposes some conditions, while ABSA (53%) and Pride Microfinance (38%) impose even stricter limitations. Notably, ABSA does not provide for the right to permanently delete personal data.

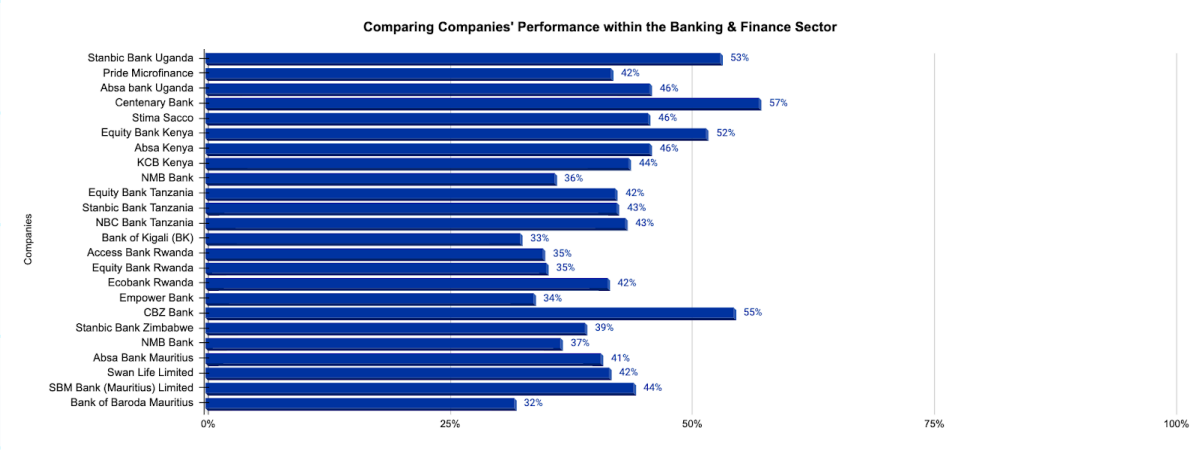
Third-party data transfer practices are weak, with none of the banks scoring above 50%. Pride Microfinance performs worst (10%), allowing unrestricted third-party access without listing recipients or specifying data types shared.

Data security scores vary, with Stanbic and Centenary leading at 78%, followed by ABSA (56%), while Pride Microfinance performs worst due to a poor website security rating (F).

Despite the high level of banking activity in Uganda, none of the banks have published a transparency report since 2023, and internal data breach resolution remains severely lacking, with the highest score at only 17%. These gaps highlight an urgent need for improved enforcement, transparency, and stronger consumer data protection measures.

3.5.4.3 Comparison of companies/entities within the sector

The figure reveals a varied performance among banks in the sector across different countries in East and Southern Africa, with notable differences in their overall privacy practices. The financial institutions' overall percentage scores reflect the varying degrees of commitment to implementing privacy and data protection measures, which are critical for compliance with data protection laws. In Uganda, Centenary Bank led the local group with an overall score of 57%, followed by Stanbic Bank Uganda at 53%, Absa Bank Uganda at 46%, and Pride Microfinance at 42%. These scores suggest that while these banks are taking steps to address privacy practices, there is significant room for improvement. The fact that none of these banks scored above 60% highlights the challenges they face in aligning with stringent data protection standards and complying with privacy regulations.



In Kenya, Equity Bank Kenya performed relatively better with an overall score of 52%, closely followed by Stima Sacco, Absa Kenya, and KCB Kenya, all at 46%. These scores indicate a moderate commitment to data protection and privacy practices, although like their counterparts in Uganda, these institutions are still far from demonstrating robust compliance with data protection requirements.

The banks in Tanzania showed generally lower performance, with NMB Bank Tanzania scoring the lowest at 36%, followed by Equity Bank Tanzania at 42%, and Stanbic Bank Tanzania and NBC Bank Tanzania at 43%. These relatively low scores indicate significant weaknesses in the privacy practices of these institutions, potentially exposing them to higher risks related to non-compliance with privacy laws.

In Rwanda, the performance was similarly weak, with Bank of Kigali (BK) scoring the lowest at 33%, followed by Access Bank Rwanda and Equity Bank Rwanda both at 35%, and Ecobank Rwanda at 42%. These low scores suggest that Rwandan banks face substantial challenges in implementing effective privacy and data protection measures, which could impact their ability to fully comply with national data protection laws.

Zimbabwe's banks showed more variability, with CBZ Bank leading at 55%, followed by Empower Bank at 34%, Stanbic Bank Zimbabwe at 39%, and NMB Bank at 37%. While CBZ Bank's relatively higher score may suggest better adherence to privacy regulations, the performance of the other banks highlights critical gaps in their compliance efforts.

In Mauritius, the scores were relatively closer to the middle range, with SBM Bank Mauritius at 44%, Swan Life Limited at 42%, and Absa Bank Mauritius at 41%. These scores reflect a moderate level of commitment to privacy and data protection practices, though they still indicate room for improvement to meet global standards.

In sum, the performance of these banks across different countries shows that while some have made strides in privacy and data protection, there is a general trend of underperformance in meeting the requirements of national and international data protection laws. Many banks, particularly in Tanzania, Rwanda, and Zimbabwe, have scores well below the 50% mark, which implies significant deficiencies in areas like third-party data transfers, internal data breach resolutions, and transparency reports. These gaps suggest that enhanced efforts are needed to strengthen data privacy practices and ensure compliance with evolving data protection regulations in these regions.

3.5.4.4 Identification of sector-specific challenges and best practices

In this sector, the challenges related to privacy and data protection are significant, especially given the sensitive nature of the information these institutions handle. Banks collect, store, and process vast amounts of personal, financial, and transactional data, which makes them prime targets for cyberattacks and data breaches. Moreover, regulatory frameworks governing data privacy are becoming increasingly stringent, creating pressure for institutions to comply with national privacy and data protection laws in the respective, GDPR in the EU, and other jurisdictional equivalents. Let's explore the key challenges in more detail and how financial institutions can address them through best practices:

I. Data Protection Measures

Banks as noted above are custodians of a vast amount of sensitive customer data, including financial transactions, personal identifiers, and even biometric information. Without adequate data protection measures, this data is vulnerable to unauthorized access, cyberattacks, and breaches. Weak encryption, insecure transmission protocols, and poor access control can leave data exposed. A failure to protect this sensitive data can lead to financial losses, legal penalties, and damage to the bank's reputation.

The consequences of a breach also extend to customers, who may suffer from identity theft, financial fraud, or privacy violations. Financial institutions to address some of the listed challenges, can encrypt data both in transit and at rest to ensure that even if data is intercepted, it cannot be read or exploited. AES (Advanced Encryption Standard) is widely regarded as a robust encryption algorithm. Banks must use secure transmission protocols like HTTPS, TLS, and SSL to protect data during online transactions and communications. These protocols prevent man-in-the-middle attacks and ensure secure data exchange between servers and users.

Implementation of strict access controls based on the principle of least privilege, ensuring that only authorized personnel have access to sensitive data. Multi-factor authentication (MFA) should be used to secure access to systems storing sensitive data.

II. Transparency

Many financial institutions struggle to provide customers with clear and transparent information regarding how their data is collected, processed, stored, and shared. Lack of transparency can lead to a breakdown of trust between the institution and its customers, especially if customers are unaware of how their data is being used or shared with third parties. Poor transparency practices can lead to non-compliance with data protection regulations, as customers may not have given informed consent for their data to be used in certain ways. Additionally, failure to disclose third-party data sharing practices can expose the institution to liability, particularly if shared data is mishandled or misused by third-party vendors.

Financial institutions must clearly disclose how they collect, process, and store personal data. This includes outlining what data is collected, why it is collected, how long it is retained, and the legal basis for processing the data. Banks should establish and communicate clear data retention policies. They must specify how long data will be stored and ensure it is securely deleted or anonymized once it is no longer needed. Banks should inform customers about the third parties with whom their data is shared, the purposes for which data is shared, and the safeguards in place to protect data when it is shared. This helps customers make informed decisions about their consent.

III. Compliance with Regulatory Frameworks

Financial institutions must comply with numerous jurisdictional privacy and data protection laws and regulations, which often vary by country and region. Regulatory frameworks like the Data Protection and Privacy Act 2021 of Uganda, GDPR in Europe, and CCPA in California, impose strict requirements on how customer data is handled. Compliance with these regulations requires ongoing attention, resources, and adjustments to internal practices. Non-compliance with data protection regulations can lead to significant financial penalties, legal action, and reputational harm. For example, the GDPR imposes heavy fines of up to 4% of global revenue for violations, while data protection laws in the assessed countries carry penalties for breach of their privacy requirements.

Financial institutions should regularly audit their data protection practices to ensure compliance with local and international privacy laws. These audits should evaluate data handling practices, security measures, and the effectiveness of internal policies. Designating a dedicated DPO or a privacy team responsible for monitoring compliance with privacy laws and regulations is essential. The DPO can oversee training, audits, and ensure that data protection processes are followed. Institutions should adopt a comprehensive framework for privacy and data protection, such as the GDPR or the ISO/IEC 27001 standard for information security management. This will help ensure that data protection measures are aligned with legal requirements.

IV. Breach Response Mechanisms

Despite robust data protection measures, no system is entirely immune from breaches. Data breaches can happen due to external attacks, internal mistakes, or lapses in security. A lack of preparedness in handling breaches can exacerbate the impact, causing further harm to customers and the institution. A slow or inadequate response to a breach can result in legal consequences, loss of customer trust, and damage to the institution's reputation. Regulatory bodies require timely breach notifications (e.g., within 72 hours for GDPR), and failing to meet these requirements can result in fines.

Financial institutions must have a clearly defined breach response plan that includes immediate actions for containment, communication with affected parties, and coordination with relevant authorities. The plan should include procedures for notifying customers and regulators in the event of a breach. The breach response plan should be regularly tested and updated to account for new threats, changing regulations, and lessons learned from past incidents. Staff should be trained in how to handle breaches quickly and efficiently. After a breach, financial institutions should conduct a thorough investigation to understand its causes and implement corrective actions to prevent future incidents. A post-breach analysis also helps in complying with legal obligations to assess and report the breach's impact.

In sum, the challenges faced by financial institutions in terms of privacy and data protection are complex and multifaceted. However, by implementing strong data protection measures, ensuring transparency, adhering to regulatory frameworks, and establishing effective breach response mechanisms, banks can significantly improve their compliance with data protection laws and enhance customer trust. These best practices not only help financial institutions safeguard sensitive data but also contribute to creating a culture of privacy and security within the organization.

3.5.5 Insurance Sector Analysis

3.5.5.1 Overview of the sector and data collectors evaluated

The insurance sector in East and Southern Africa has experienced significant growth over recent years, driven by increasing awareness of the importance of insurance, rising middle-class populations, and the expansion of digital services. Countries like Kenya, South Africa, Tanzania, Uganda, and Zimbabwe have seen the development of both traditional insurance companies and innovative insurtech startups, which leverage technology to provide more accessible and affordable insurance solutions.

Despite the growth, insurance penetration remains relatively low compared to global standards. However, rising economic development, a growing middle class, and increasing financial literacy are contributing to an uptick in both life and non-life insurance products across the region. Many insurers are embracing digital transformation, utilizing mobile platforms, apps, and digital payment systems to expand their reach and simplify customer interactions. Insurtech startups have emerged, offering innovative products such as microinsurance and pay-as-you-go insurance. Countries in the region have been improving their regulatory frameworks to better protect consumers, with some jurisdictions (such as South Africa) having well-established and robust regulatory environments, while others are in the process of enhancing regulatory measures to address emerging risks, including cyber threats.

Despite the expansion of services, many regions in East and Southern Africa still face challenges in convincing consumers of the value of insurance, which is often seen as an unnecessary expense. Consumers may lack trust in the sector due to perceptions of fraud, lack of transparency, and poor service delivery. This can affect willingness to share personal data or engage with insurers. The insurance sector collects vast amounts of sensitive personal and financial data, including identity details, health records, financial status, and claims history. This data is crucial for underwriting, pricing, and claims processing. Given the sensitive nature of this information, privacy and data protection practices are of paramount importance. However, the handling of such data varies across different countries in East and Southern Africa, with varying degrees of adherence to data protection laws.

Insurance companies typically collect personal information such as name, age, address, employment status, and contact details. They may also collect more sensitive data, such as health records, medical history, and financial status, which are necessary for risk assessment and pricing.

With the rise of digitalization, many insurers in the region now collect data through mobile apps, websites, and social media channels. This includes using mobile phones to collect biometric data, such as fingerprints or facial recognition, for identity verification, particularly in the case of mobile-based insurance solutions. Insurers often share customer data with third-party providers, such as reinsurers, claims processors, and healthcare service providers, for purposes related to claims processing, risk assessment, or product development. However, without proper data handling protocols, this can create risks regarding data security and privacy breaches.

While some countries in East and Southern Africa have made strides in enacting privacy regulations (such as the Data Protection Act of Uganda and the Protection of Personal Information Act in South Africa), the enforcement of these regulations varies widely. Some countries may lack comprehensive data protection laws, leaving insurance companies with limited accountability for mishandling personal data. Many customers in the region may not be fully aware of their rights related to data protection, leading to insufficient demand for transparency or accountability from insurance providers. Customers may not understand how their data is being used, who it is shared with, or how long it is retained. Insurers in the region face significant challenges in securing sensitive data from cyberattacks or internal breaches. With many insurers adopting digital platforms, the risk of data breaches, hacking, or misuse of personal data is growing. Moreover, smaller insurance companies or startups may lack the resources to implement robust data protection measures.

The insurance sector in East and Southern Africa is evolving rapidly, with increasing digitalization, new products, and growing market penetration. However, the sector faces challenges in maintaining robust privacy practices and complying with data protection laws. As insurers collect vast amounts of personal and sensitive data, they must prioritize strong data protection measures, transparency, and customer awareness to build trust and avoid regulatory penalties.

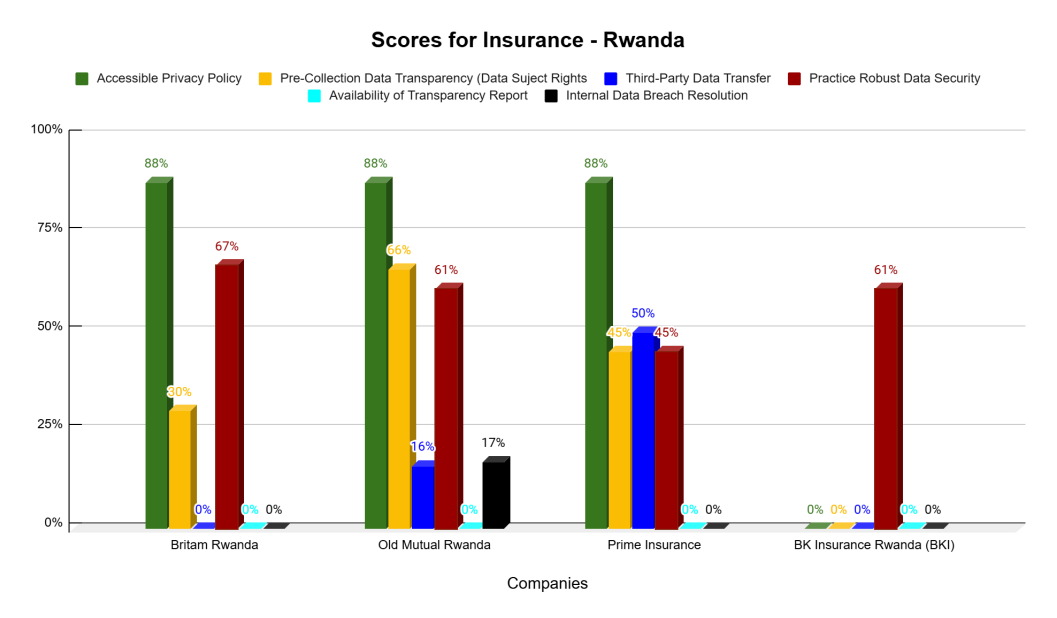
By implementing best practices for data security, compliance with local privacy laws, and clear communication with customers, insurance companies can improve privacy practices, protect their clients' data, and foster a more trustworthy and sustainable insurance market.

3.5.5.2 Analysis of compliance with each criterion

a) Britam Rwanda, Old Mutual Rwanda, Prime Insurance and BK Insurance Rwanda in Rwanda

The figure highlights varying levels of privacy practices and compliance with data protection laws among several companies. Only three companies—Britam Rwanda, Old Mutual Rwanda, and Prime Insurance—were credited for having accessible privacy policies, each scoring 88%, while BK Insurance scored a concerning 0%.

In terms of data security compliance, all companies performed reasonably well, with Britam Rwanda leading at 67%, followed by Old Mutual Rwanda and BK Insurance at 61%.



However, the performance was weaker in other areas: Old Mutual led in pre-collection data transparency with a score of 66%, while Prime Insurance was in the lead for compliance with third-party data transfers at 50%, but still faced significant shortcomings, with Old Mutual scoring only 16% and BK Insurance an alarming 0% in this area. Furthermore,

all companies displayed poor compliance with the availability of transparency reports and internal data breach resolution, with some scoring as low as 0%.

While BK Insurance achieved a decent score of 61% in data security, it exhibited alarmingly low compliance across the other categories, scoring 0% in each, highlighting critical weaknesses in its overall data protection practices. This uneven performance signals substantial risks in data protection and privacy compliance, with some companies failing to meet basic regulatory standards.

All three insurance companies—Britam Rwanda, Old Mutual Insurance, and Prime Insurance—have publicly posted data policies on their websites, which are noticeable and fairly readable. Their policies have word counts of 2969, 3609, and 1695, respectively, and were scored 12, 12, and 13 by the Hemingway editor.

Britam Rwanda: The policy mentions the contact details and purpose for data collection, but does not specify the type of data or duration of control. No third-party data sharing is allowed, and personalized ads can be opted out of. It mentions data correction rights but lacks information on access, deletion, or restriction of processing rights. Law enforcement access is unspecified.

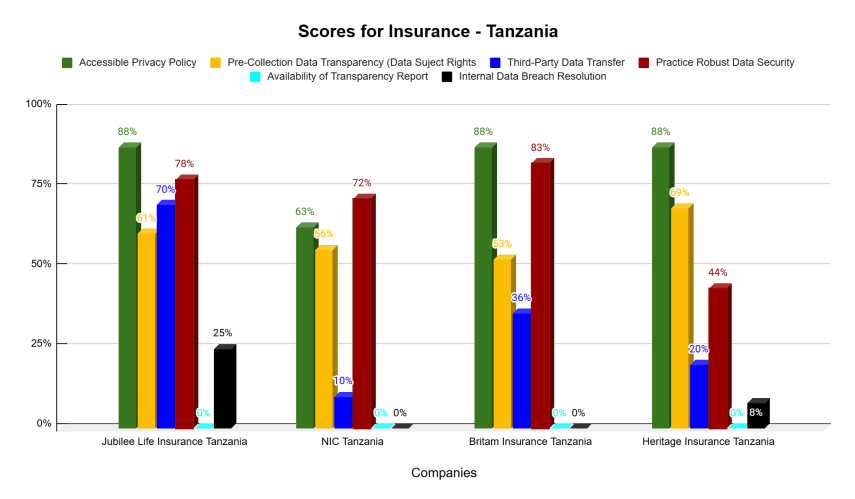
Old Mutual Insurance policy includes contact information, data collection reasons, type of data, and duration of control. No third-party data sharing is allowed, and personalized ads can be opted out of. It mentions data rights to deletion and restriction of processing unconditionally, but access and correction rights are conditional. Law enforcement access is allowed.

Prime Insurance policy does not list the contact information but mentions the reason for data collection and type of data. It does not specify the duration of control. No third-party data sharing is allowed, but personalized ads are permitted without opt-in or opt-out options. It mentions access and correction rights unconditionally and permanent deletion conditionally. Restriction of processing is not allowed, and law enforcement access is granted.

Observations in respect of security and transparency revealed that Britam, Old Mutual, and Prime mention data security but provide no specifics. BK Insurance does not mention security at all; SSL Scores were: Britam (B), Old Mutual (B), Prime (A), BK Insurance (A+) while, Security Header Scores were: Britam (A), Old Mutual (B), Prime (F), BK Insurance (A). None of the companies had a transparency report available.

Old Mutual privacy policy mentioned data breaches and provided notification to data subjects, though it lacked specifics on how breaches will be redressed or the timeframe for resolution. Britam and Prime did not address data breaches in their policies.

b) Jubilee Life Insurance Tanzania, NIC Tanzania, Britam Insurance Tanzania and Heritage Insurance Tanzania in Tanzania



All four companies have publicly accessible privacy policies, demonstrating a commitment to transparency. Jubilee, Britam, and Heritage lead with 88%, while NIC lags at 63%, suggesting potential difficulty for users in locating or understanding its policy, which may impact customer trust. Jubilee Life Insurance Privacy Policy was observed as clear and readable with1478 words and a Hemingway score of 14). A secure website (A grade) with three trackers on the website and two trackers on the app. The policy does not specify third parties, does not allow data sharing with advertisers. It provides rights to access, correct, object to, and restrict data processing, but subject to conditions. Also it mentions

breach procedures but lacks specifics on investigation timelines, reporting methods, and fairness in investigations. Users are notified of breaches within an unspecified period. Mentions data security but without specifics.

Britam Insurance privacy policy was more detailed with 7252 words and a Hemingway score of 23. A secure website (A grade) and three trackers on both app and website. The policy does not specify third parties nor allow data sharing with advertisers. Similar to Jubilee, it provides rights to access, correct, object to, and restrict data processing, but subject to conditions. Mentions breaches but lacks specifics on investigation timelines, user notification, and reporting channels. It provides more specifics on security, outlining technical, physical, and organizational safeguards.

Equally, the companies were credited for implementing security measures to protect user data, though performance varied with Britam as the top performer at 83%, followed by Jubilee and NIC exhibiting as well strong compliance at 78% and 72% respectively.

While, Heritage Insurance was observed with the weakest performance at 44%. Whereas Britam and Jubilee demonstrated robust security, Heritage's low score suggests potential vulnerabilities that could expose user data to breaches or cyber threats.

The level of transparency in informing users about data collection varied with Heritage observed as the most transparent at 69% while moderate transparency was exhibited by Jubilee (61%), NIC (56%) and Britam (53%). The lower scores indicate that some companies may not clearly communicate what data is collected and why, potentially leading to compliance risks and customer dissatisfaction.

Companies differed significantly in how they manage third-party data sharing with Jubilee topping the sector at 70% and lower compliance was observed with Britam (36%), Heritage (20%) and NIC (10%). While Jubilee provides more transparency, the other companies lacked clarity, raising concerns over potential non-compliance with best data protection practices.

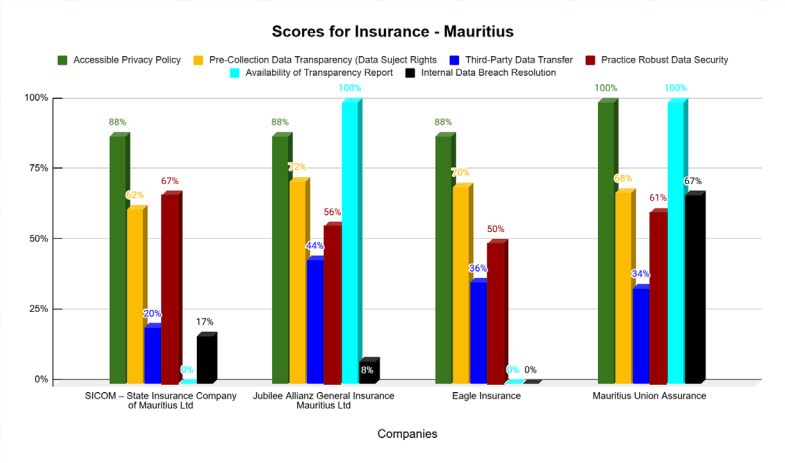
All four companies performed poorly in these areas, failing to provide transparency reports or robust internal data breach resolution mechanisms.

The lack of transparency reports limits public awareness of how these companies handle personal data. Weak data breach resolution measures mean customers may not have clear procedures to follow in case of a data breach, exposing companies to reputational and legal risks.

Heritage should strengthen security protocols to meet industry standards. All companies should publish transparency reports to increase accountability. Clear, structured policies on data breach investigation, reporting mechanisms, and resolution timelines are needed. NIC and Britam should enhance how they communicate data collection practices to users. Companies with low compliance (NIC, Heritage and Britam) should be more transparent about third-party data transfers. By addressing these gaps, Tanzanian insurance companies can enhance trust, regulatory compliance, and overall data protection standards.

c) Sicom – State Insurance Company of Mauritus Ltd, Jubilee Allianz General Insurance Mauritius Ltd, Eagle Insurance and Mauritius Union Assurance in Mauritius

All companies were credited for having in place accessible privacy policies. Whereas Mauritius Union Assurance was in the lead with 100%, SICOM, Jubilee Allianz and Eagle Insurance followed closely at 88% each. Furthermore, Jubilee Allianz and Mauritius Union Assurance were in the lead on available transparency reports with 100% each while the rest of the companies had low compliance levels at 0% each.

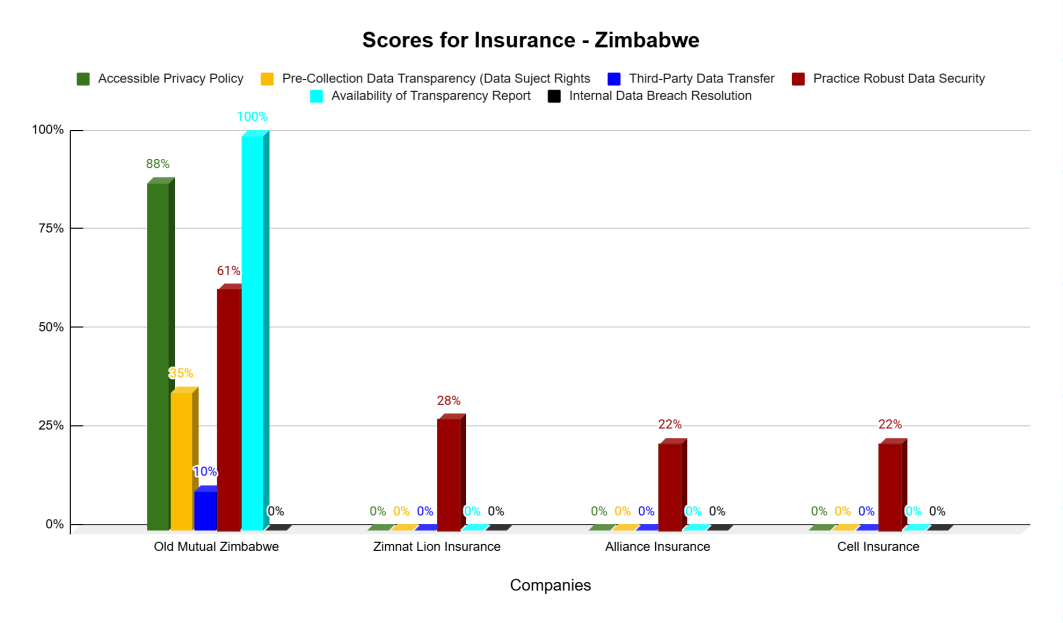


Jubilee Allianz led thee sector on pre-collection data transparency with 72%, followed by Eagle Insurance at 70%, Mauritius Union Asssurance at 68% and SICOM at 62%. Although all companies exhibited compliance with data security, the highest was only 67% placing SICOM in the lead, followed by Mauritius Union Assurance at 61% while Jubilee Allianz and Eagle Insurance were just at 56% and 50% respectively.

d) Old Mutual Zimbabwe, Zimnat Lion Insurance, Alliance Insurance and Cell Insurance in Zimbabwe

The figure below reveals significant disparities in privacy practices and compliance with data protection laws across several companies. Old Mutual Zimbabwe emerged as the leader in the sector, scoring 100% for having a transparency report in place and 88% for an accessible privacy policy. All companies were credited for compliance with data security measures, with Old Mutual Zimbabwe again leading at 61%, followed by Zimnat Lion Insurance at 28%, and Alliance Insurance and Cell Insurance, both scoring 22%.

However, Old Mutual Zimbabwe's performance in other areas, such as pre-collection data transparency and third-party data transfers, was less impressive, with scores of only 35% and 10%, respectively.

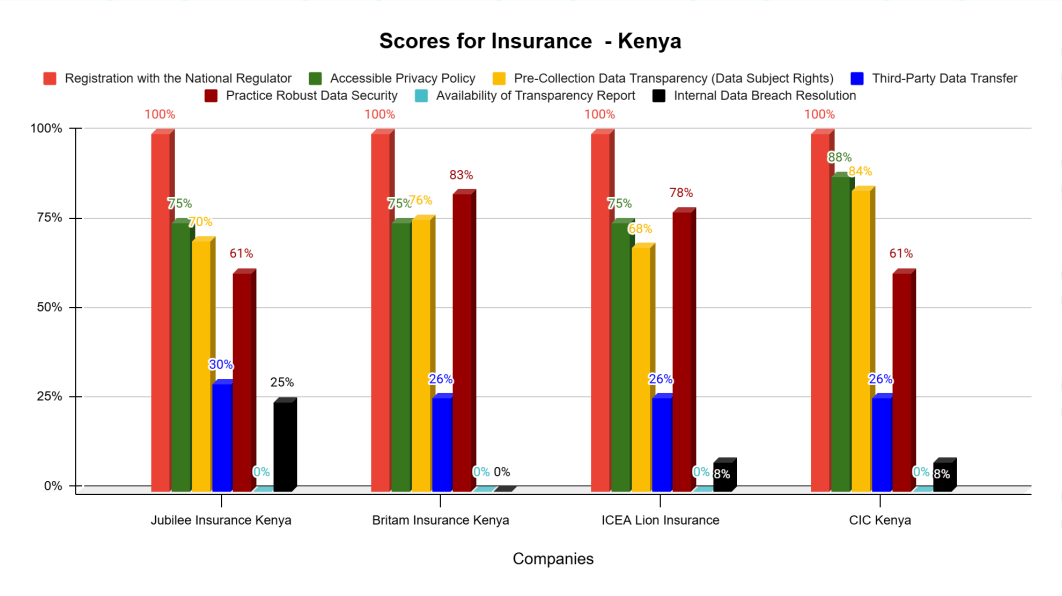


Meanwhile, the other three companies performed poorly across most areas, scoring as low as 0% for accessible privacy policies, pre-collection data transparency, third-party data transfers, transparency reports, and internal data breach resolution. These low scores suggest significant gaps in compliance, highlighting potential risks in data protection and privacy practices, with some companies failing to meet fundamental regulatory standards.

e) Jubilee Insurance kenya, Britam Insurance Kenya, ICEA Lion Insurance and CIC Kenya in Kenya

The figure below indicates that all companies were credited with registering with the national regulator, each achieving a perfect score of 100% as the first step toward compliance. Additionally, they were all recognized for having accessible privacy policies, with CIC Kenya leading the sector at 88%, followed by Jubilee Insurance Kenya, Britam Insurance Kenya, and ICEA Lion Insurance, all scoring 75%. CIC Kenya also topped the sector in pre-collection data transparency with a score of 84%, followed by Britam Insurance at 76%, Jubilee Insurance Kenya at 70%, and ICEA Lion Insurance at 68%.

In terms of data security compliance, all companies performed reasonably well, with Britam Insurance Kenya leading at 83%, followed by ICEA Lion Insurance at 78%, while CIC Kenya and Jubilee Insurance Kenya each scored 61%. However, all companies displayed weak performance in the areas of third-party data transfers, internal data breach resolution, and transparency reports, with scores as low as 0%.



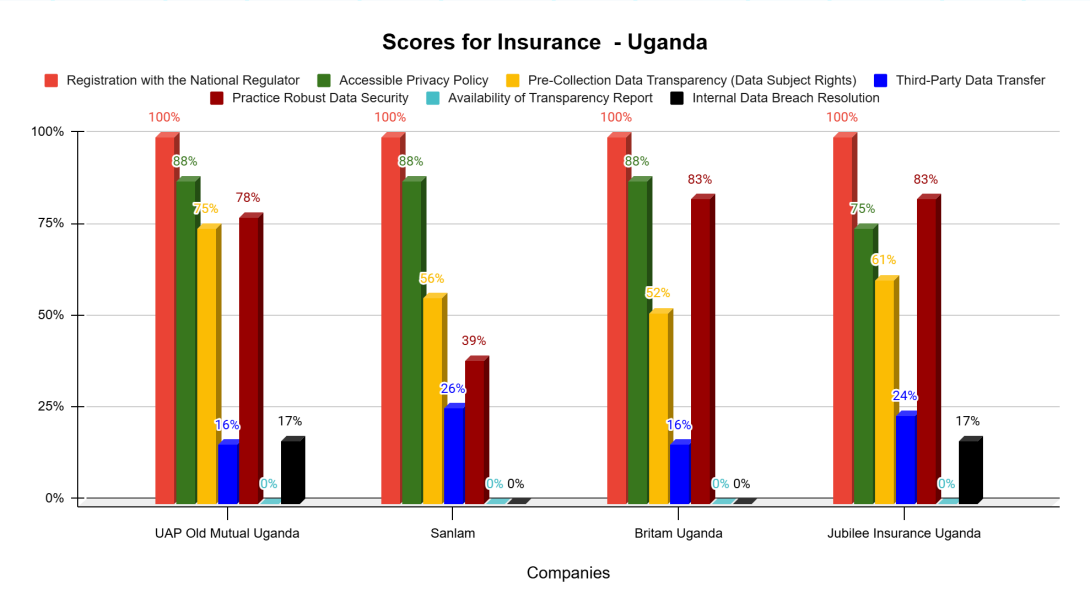
These low scores in critical areas of data protection suggest that while companies have made some progress in initial compliance steps, there are substantial gaps in their overall privacy practices and compliance with data protection laws, particularly in more complex areas like data transfers and breach resolution.

f) UAP Old Mutual Uganda, Sanlam, Britam Uganda and Jubilee Insurance Uganda in Uganda

The assessment of UAP, Sanlam, Britam, and Jubilee highlights both progress and challenges in data protection compliance. All four companies are registered with Uganda's National Data Privacy Regulator (100%), ensuring regulatory oversight. UAP, Sanlam, and Britam lead in privacy policy accessibility (88%), with Jubilee slightly lower (75%) due to less user-friendly language.

UAP scores highest in Data Subject Rights (75%), appointing a Data Protection Officer and clearly outlining privacy rights and restrictions on law enforcement access. Jubilee follows with 61%, lacking a right to lodge complaints. Sanlam and Britam score lowest, with Sanlam failing to recognize key rights such as access, correction, or permanent deletion.

Third-party data transfer compliance is weak across all companies. Their policies permit third-party access without specifying data types shared or providing clear breach resolution mechanisms. In data security, Britam and Jubilee rank highest (83%), earning A security header scores and detailing security measures.



UAP follows (78%), while Sanlam lags behind (39%). All four maintain a B SSL server score.

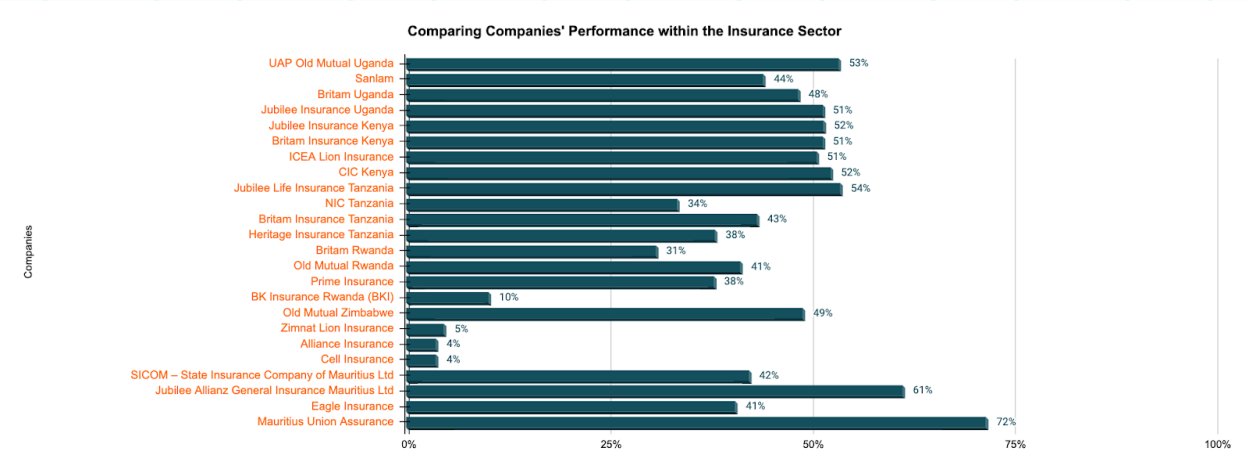
However, critical weaknesses persist as none of the companies have published a transparency report since 2023. Internal data breach resolution is severely lacking, with UAP and Jubilee scoring highest at only 17% and the rest at 0%. Their policies fail to ensure fair investigations, resolution timeframes, or clear reporting channels. These deficiencies in third-party data transfers, breach resolution, and transparency undermine customer privacy protections, highlighting an urgent need for stronger compliance measures.

3.5.5.3 Comparison of companies/entities within the sector

The figure below highlights significant variations in the performance of insurance companies across different countries, reflecting their level of compliance with data protection laws and privacy practices.

In Uganda, the companies' overall scores range from 44% to 53%, with UAP Old Mutual Uganda leading at 53%, followed by Jubilee Insurance Uganda at 51%. However, Sanlam and Britam Uganda scored lower at 44% and 48%, respectively. While these scores indicate some level of compliance, they also suggest room for improvement in privacy policies, data security, and other key areas such as transparency and internal data breach resolution.

Kenya's insurance companies had somewhat stronger overall performance, with scores ranging from 51% to 52%. Jubilee Insurance Kenya, CIC Kenya, and Britam Insurance Kenya all scored 52%, while ICEA Lion Insurance scored 51%.



These companies performed relatively well in terms of data security and privacy policies, but there are still weaknesses in areas like pre-collection data transparency and third-party data transfers, which are critical for full compliance with data protection laws.

Tanzania saw a broader range of performance, with Jubilee Life Insurance Tanzania leading at 54%, followed by NIC Tanzania at 34%, and the remaining companies—Britam Insurance Tanzania, Heritage Insurance Tanzania, and the rest—scoring much lower, between 4% and 43%. These low scores highlight substantial gaps in privacy practices, especially in data transparency, third-party transfers, and breach resolution, raising concerns about compliance with data protection regulations.

Rwanda's companies generally scored lower, with Britam Rwanda scoring 31%, Old Mutual Rwanda at 41%, Prime Insurance at 38%, and BK Insurance Rwanda (BKI) at a particularly low 10%. These poor scores suggest that many companies in Rwanda are not meeting essential privacy standards, particularly in areas like accessible privacy policies and transparency reports, which are fundamental for ensuring data protection compliance.

In Zimbabwe, the performance was notably poor across the board. Old Mutual Zimbabwe scored 49%, which was the highest in the sector, but Zimnat Lion Insurance, Alliance Insurance, and Cell Insurance all scored extremely low, ranging from 4% to 5%. These companies are at significant risk of non-compliance with data protection laws, as they are failing to meet basic requirements for transparency, data security, and breach resolution.

Mauritius had mixed results, with Mauritius Union Assurance scoring the highest at 72%, followed by Jubilee Allianz General Insurance Mauritius Ltd at 61%. SICOM and Eagle Insurance scored 42% and 41%, respectively, suggesting that while there is some adherence to data security practices, further improvements are necessary to strengthen compliance in areas such as pre-collection data transparency and third-party data transfers.

Overall, the companies' performance in the insurance sector reveals widespread weaknesses in key areas of privacy practices and data protection compliance, especially in countries like Zimbabwe, Rwanda, and Tanzania. While some companies in Kenya, Mauritius, and Uganda show relatively stronger adherence to privacy policies and data security measures, many still face critical challenges in fully complying with data protection laws, particularly concerning third-party data transfers, transparency reports, and internal data breach resolution. This inconsistent performance poses significant risks to consumer data security and privacy, and suggests that many companies need to urgently address gaps in their data protection frameworks to meet regulatory standards.

3.5.5.4 Identification of sector-specific challenges and best practices

This section highlights several key areas of concern in the insurance sector, each carrying risks that can impact both compliance with data protection laws and consumer trust.

I. Transparency in Data Processing is a key issue

Insurance companies collect sensitive data, such as medical and financial information, to assess risks and process claims.

However, without clear communication, customers may not understand why their data is being collected or how it will be used. This lack of transparency poses a risk of non-compliance with data protection laws and erodes consumer trust. To address this, insurers should ensure they provide clear, accessible privacy notices that outline their data collection practices, including the specific purposes and access details, so customers can make informed decisions.

II. Third-Party Relationships further complicate data protection

Insurance companies often rely on external vendors like medical examiners and claim processors, making data sharing a critical concern. If not properly managed, these third-party relationships can expose sensitive customer data to additional privacy risks. To mitigate this risk, insurers must establish robust data-sharing agreements with third-party vendors, ensuring they adhere to the same privacy standards. Companies should also be transparent with customers about when and why their data is shared with third parties.

III. Data Minimization is another critical issue

Insurance companies sometimes collect more personal information than is necessary for underwriting or claims processing, increasing the risk of data breaches and non-compliance with regulations. To address this, insurers should implement a data minimization policy, collecting only the data essential for their operations and ensuring that any excess data is securely deleted or anonymized.

IV. Security Measures

Finally, Security Measures are paramount to protect sensitive information such as medical and financial records. Inadequate data protection increases the risk of unauthorized access and breaches, which can lead to severe reputational

damage and legal consequences. Insurers must invest in strong security infrastructure, including encryption, secure storage, and access controls. Additionally, regular security audits and employee training are essential to ensure continuous improvement in safeguarding sensitive data from emerging threats.

In sum, by prioritizing key areas such as transparency, third-party relationships, data minimization, and security, insurance companies can strengthen their privacy practices, mitigate compliance risks, and build greater consumer trust in how personal information is managed. Achieving this requires a dedicated commitment to embedding privacy and data protection into the core of their operations.

Through investments in clearer transparency, robust security measures, and well-defined internal protocols, these companies can significantly improve their compliance with data protection laws, ultimately ensuring the safeguarding of customer privacy.

3.5.6 e – Government Sector Analysis

3.5.6.1 Overview of the sector and data collectors evaluated

The e-government sector in East and Southern Africa is undergoing rapid development, driven by the increasing adoption of digital technologies to enhance public service delivery, improve efficiency, and foster greater transparency. Governments across the region are implementing digital platforms for essential services such as taxation, public health, voting, social welfare programs, and land registration, with the aim of providing more accessible and responsive services to citizens.

However, these advancements also present significant challenges, particularly concerning privacy and data protection. As e-government platforms collect vast amounts of sensitive personal data, concerns have arisen regarding how this information is handled, stored, and shared. The scorecard report highlights that privacy practices across the region are inconsistent, with notable gaps in data protection compliance. This inconsistency is particularly evident in countries like Uganda, Kenya, Mauritius, Zimbabwe, Rwanda, and Tanzania, where varying levels of privacy practices and regulations create challenges in ensuring comprehensive data protection.

Uganda faces significant transparency challenges, with many e-government platforms lacking clear communication about the data being collected, its purpose, and who has access to it. Citizens are often unaware of how their personal data is being used, undermining trust. The report indicates that while Uganda has made strides in implementing digital government services, improvements in transparency are needed to meet data protection standards.

Kenya, on the other hand, has made notable progress with the implementation of its digital platforms. However, concerns around third-party relationships persist, as many e-government services involve partnerships with external vendors. These relationships introduce risks of data misuse, especially when proper safeguards and disclosures are not in place. Kenya must strengthen oversight of third-party vendors to ensure they meet data protection standards and increase transparency with citizens about how their data is shared.

In Mauritius, although the government has developed relatively robust e-government services, concerns around data security remain. Despite having a data protection law in place, gaps still exist in the secure storage and transmission of sensitive personal information. The report highlights the need for more investment in infrastructure, regular security audits, and stronger encryption practices to prevent data breaches or unauthorized access to personal data.

Zimbabwe has faced significant challenges in adopting and securing its e-government services. Many of its platforms are still underdeveloped, and security measures are insufficient to protect citizens' personal data. Zimbabwe's data protection laws are also outdated, which complicates the enforcement of privacy standards. The scorecard report points to the need for modernization of these laws and substantial investment in digital security infrastructure.

Rwanda has made notable progress in digital governance, but issues around data transparency and security persist. The report indicates that, while Rwanda has strong policies in place for some areas, there are still gaps in clearly informing citizens about how their data is collected and used. Data security remains a concern, particularly regarding how personal information is stored and protected from breaches. Strengthening security protocols and enhancing transparency about data collection practices are key recommendations for improvement.

In Tanzania, the e-government sector is still developing, with many platforms in their early stages. The country struggles with data protection gaps, especially in ensuring the secure transmission and storage of personal data. Limited infrastructure and outdated regulatory frameworks pose significant risks to privacy, and the lack of clarity around compliance requirements exacerbates the problem. The scorecard report emphasizes the urgent need for stronger data protection laws and increased investment in digital security measures.

Across the region, a common theme emerges, the need for stronger and more consistent data protection frameworks. Some countries, such as Kenya and Mauritius, have begun to implement data protection regulations, but these laws are often either not comprehensive or inconsistently enforced. Many countries, including Zimbabwe and Tanzania, are still in the early stages of developing effective data protection laws, which leaves citizens' data vulnerable. To address these concerns, it is crucial that governments invest in robust data security infrastructures, such as encryption and secure storage systems, and establish clear regulations governing the collection, use, and sharing of personal data.

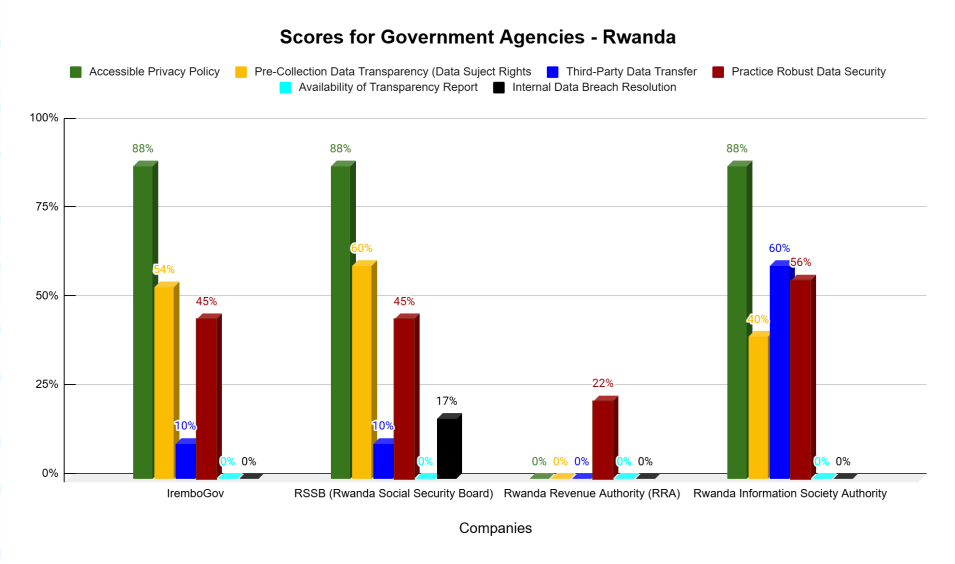
Furthermore, increased transparency is essential. Governments must provide clear privacy policies that inform citizens about what data is collected, how it is used, and who has access to it. This can help build trust and ensure compliance with international data protection standards. Enhanced oversight of third-party vendors is also necessary to mitigate the risks of data misuse when personal information is shared externally.

In sum, while e-government initiatives in East and Southern Africa offer substantial potential for improving public service delivery, addressing privacy and data protection concerns must be a top priority. By implementing stronger regulatory frameworks, enhancing transparency, securing data storage, and improving third-party relationships, governments in the region can mitigate risks, protect citizen privacy, and foster greater trust in their digital governance efforts.

3.5.6.2 Analysis of compliance with each criterion

a) IremboGov, RSSB(Rwanda Social Security Board), Rwanda Revenue Authority(RRA) and Rwanda Information Society Authority in Rwanda

In the figure below, three out of four Rwandan government agencies—IremboGov, RSSB, and the Rwanda Information Society Authority (RISA)—were recognized for having accessible privacy policies, each scoring 88%. However, the Rwanda Revenue Authority (RRA) scored 0% in this area, indicating a significant gap in privacy practices. RSSB led in pre-collection data transparency with a score of 60%, followed by IremboGov at 54%. RISA scored 40%, and RRA again scored 0%, reflecting inadequate transparency in data collection practices.



While all agencies received credit for data security efforts, the highest score was a modest 56% by RISA, followed by IremboGov and RSSB, both at 45%. RRA scored the lowest at 22%, indicating insufficient security measures. On third-party data transfers, RISA was in the lead with a score of 60%, but the other agencies, including IremboGov and RSSB (both at 10%), and RRA (0%), showed poor performance.

Furthermore, all agencies demonstrated weak performance in areas like transparency reports and internal data breach resolution, scoring as low as 0%. These low scores highlight significant gaps in the agencies' compliance with data protection laws, particularly in areas such as data transparency, security, third-party data sharing, and breach management. Without improvement in these critical areas, the agencies risk undermining public trust and falling short of data protection standards.

With the exception of Rwanda Revenue Authority that has no policy, Irembo Gov, Rwanda Social Security Board (RSSB), Rwanda Information Society Authority (RISA), have publicly posted data policies, all noticeable to data subjects. Their word counts are 2094, 3040, 620 and the Hemingway editor scored their readability at 10, 12, and 10, respectively.

Irembo Gov Policy; does not provide contact details, states the reason for data collection, type of data, and duration (lawful), does not list third parties or allow sharing with advertisers; personalized ads have no opt-in/out; grants data rights -access, correction, and permanent deletion are unconditional; no right to restrict processing and law enforcement access.

RSSB Policy does not provide contact details but mentions the reason for collection, data types, and duration (lawful), does not list third parties, allows sharing with advertisers, and offers opt-out for personalized ads. Data rights- access, correction, and deletion are unconditional; restriction is conditional. Grants law enforcement access with a reasonable request.

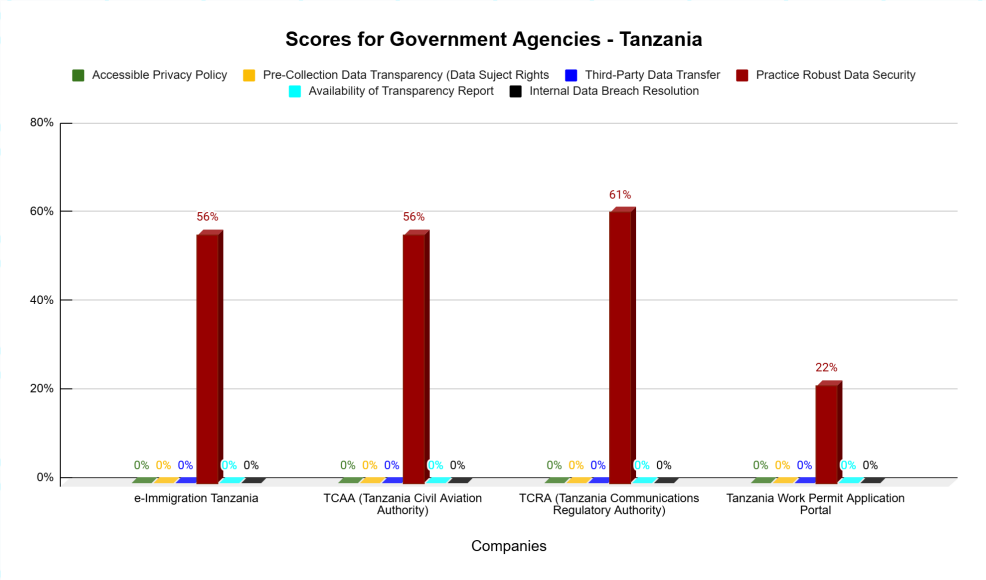
RISA Policy provides contact details and mentions reason for collection, data types, and duration (lawful), does not allow third-party access or advertisers; no personalized ads with opt-in/out, does not mention data rights (access, correction, deletion), restriction, or complaints nor is law enforcement access specified. RRA Policy does not provide specific details on data collection or third-party sharing nor is law enforcement access specified.

Irembo Gov, RSSB, and RISA mention data security without specifics, while RRA provides no security details. SSL Scores were A, A, B, and B respectively. Security Header Scores were F, F, F, and D respectively and none of the agencies had a transparency report available.

RSSB mentions data breaches but does not specify how to address them. It provides notification to data subjects, but the timeframe is unspecified. Other agencies did not mention data breaches or resolution mechanisms.

b) e-Immigration Tanzania, TCAA (Tanzania Civil Aviation Authority), TCRA (Tanzania Communications Regulatory Authority) and Tanzania Work Permit Application Portal in Tanzania

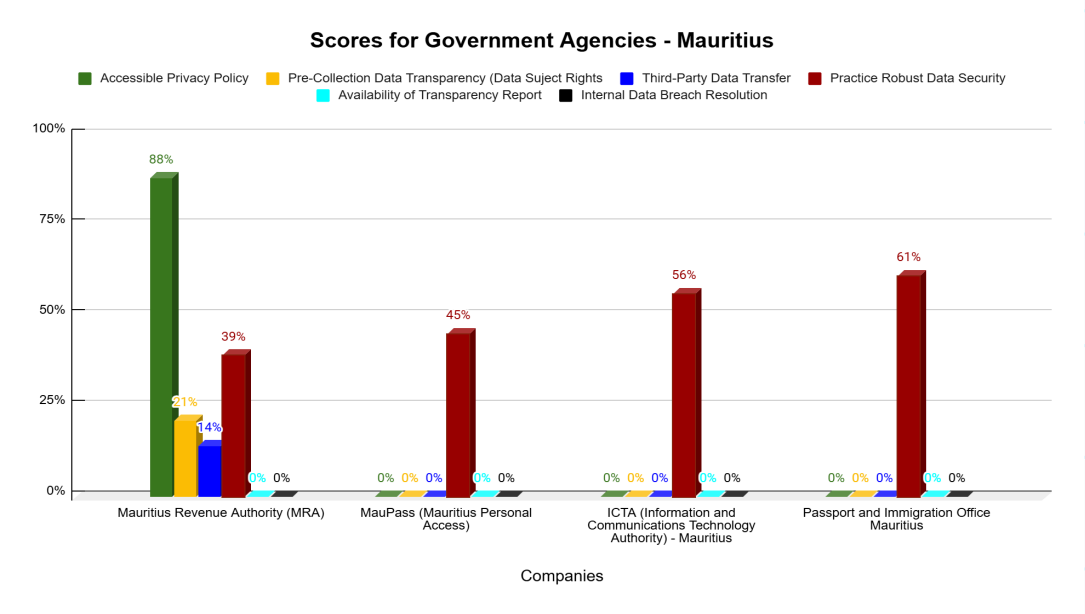
In the figure below, all the agencies in Tanzania were acknowledged for their efforts to improve data security, with TCRA leading the sector at 61%, followed by e-Immigration Tanzania and TCAA, each scoring 56%.



However, Tanzania Work Permit Application Portal scored significantly lower at 22%. Despite these efforts in data security, the agencies exhibited weak compliance in several other critical areas. In terms of accessible privacy policies, pre-collection data transparency, third-party data transfers, transparency reports, and internal data breach resolution, all the agencies scored as low as 0%, highlighting major gaps in their privacy practices. These poor scores suggest that while some progress has been made in securing data, there is a pressing need for improvement in transparency, accountability, and the protection of citizens' rights. Without addressing these deficiencies, the agencies risk violating data protection laws and eroding public trust.

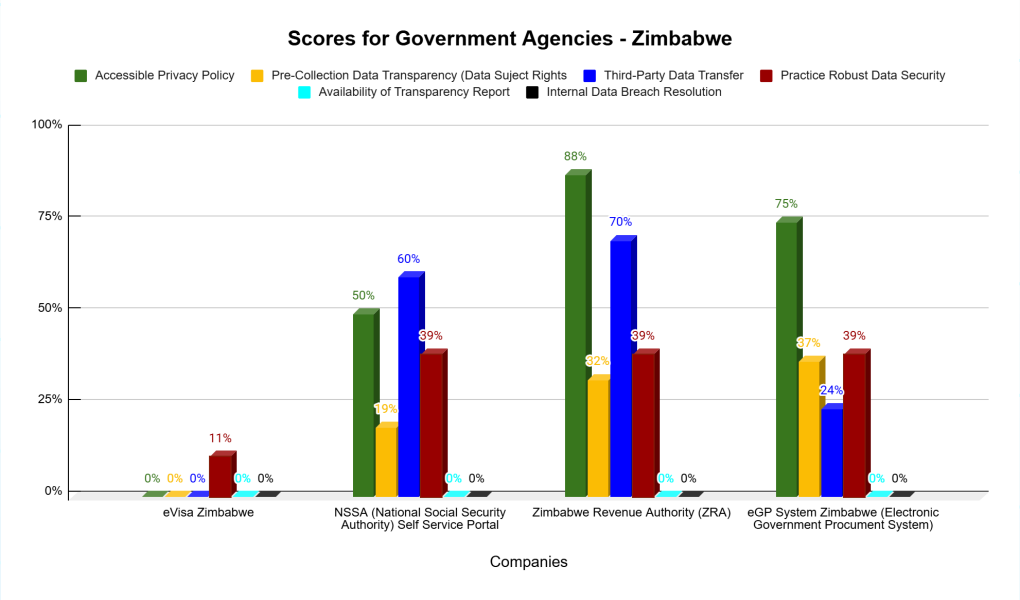
c) *Mauritius Revenue Authority (MRA), MauPass(Mauritius Personal Access), ICTA (Information and Communication TechnologyAuthority) and Passport & Immigration Office Mauritius in Mauritius*

From the figure below, MRA was the only agency credited for having an accessible privacy policy, achieving a score of 88%, while the other agencies displayed weak compliance, scoring as low as 0%. Although all the agencies demonstrated efforts to improve data security, Passport and Immigration Office Mauritius led the sector with a score of 61%, followed by ICTA at 56%, MauPass at 45%, and MRA at 39%. In critical areas such as pre-collection data transparency, third-party data transfers, transparency reports, and internal data breach resolution, all the agencies showed weak performance with scores as low as 0%. These low scores highlight significant gaps in the agencies' privacy practices and their compliance with data protection laws. Without improvement in these essential areas, the agencies risk not only failing to meet regulatory standards but also eroding public trust in their ability to safeguard personal data.



d) *e-Visa Zimbabwe, NSSA (National Social Security Authority) self service portal, Zimbabwe Revenue Authority(ZRA) and eGP System Zimbabwe (Electronic Government procurement System) in Zimbabwe*

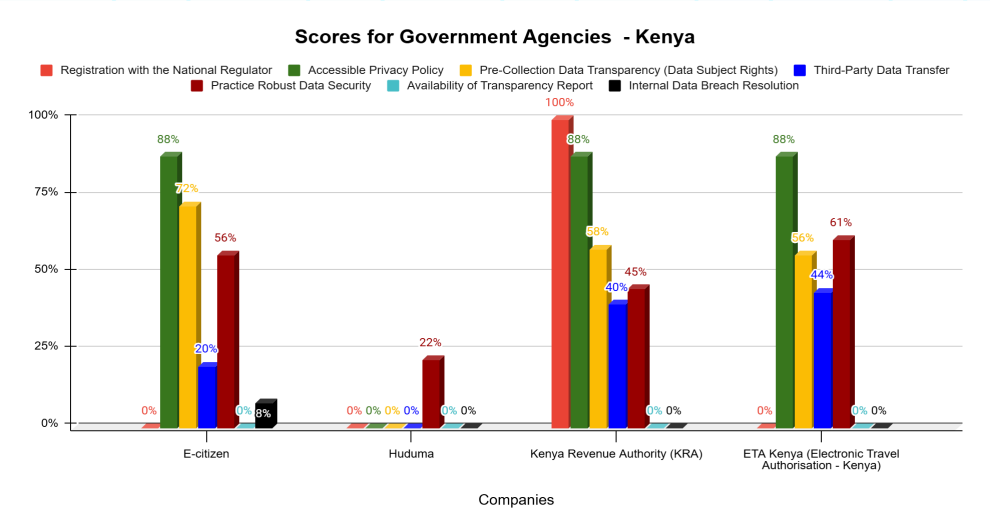
In the figure below, three agencies—ZRA, eGP Systems Zimbabwe, and NSSA—were credited for having accessible privacy policies, with ZRA leading at 88%, followed by eGP Systems Zimbabwe at 75% and NSSA at 50%. Additionally, the agencies' efforts to comply with third-party data transfers were acknowledged, with ZRA again leading at 70%, followed by NSSA at 60%, and eGP Systems Zimbabwe at 24%. However, despite these efforts, the agencies performed poorly in the area of pre-collection data transparency. eGP Systems Zimbabwe topped the sector with just a 37% score, followed by ZRA at 32%, NSSA at 19%, and eVisa Zimbabwe scoring 0%.



Furthermore, all the agencies demonstrated weak performance in transparency reports and internal data breach resolution, with scores as low as 0%. These low scores across multiple critical areas highlight significant gaps in the agencies' privacy practices, raising concerns about their compliance with data protection laws. To avoid regulatory penalties and enhance public trust, these agencies must take immediate action to improve transparency, strengthen data security, and implement robust mechanisms for data breach management and oversight.

e) e-Citizen, Huduma, Kenya Revenue Authority (KRA) and ETA Kenya (Electronic Travel Authorisation – Kenya)

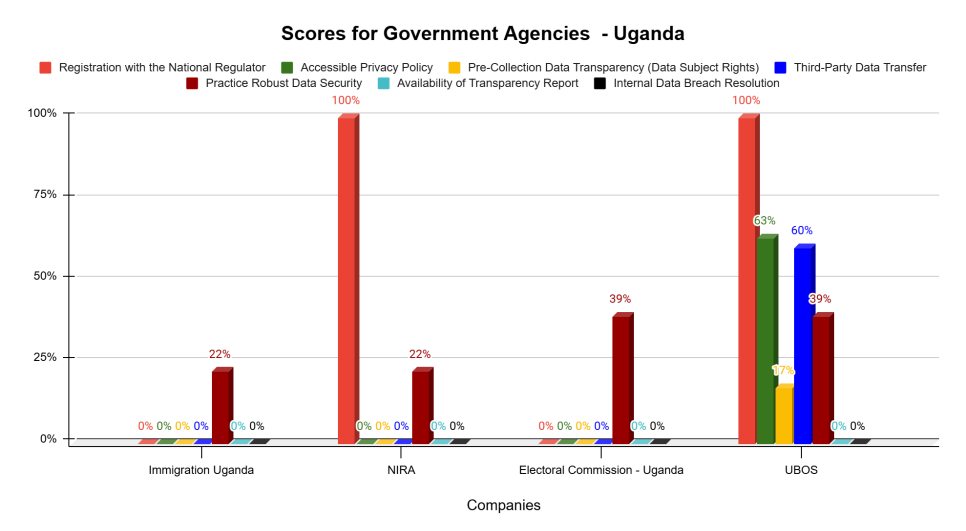
The figure below reveals significant disparities in compliance with privacy practices and data protection laws across various agencies. KRA led the sector with a perfect score of 100% for registration with the national regulator, marking a strong initial step toward compliance. However, the remaining agencies demonstrated weak compliance, with some scoring as low as 0%. E-Citizen, KRA, and ETA Kenya were credited for having accessible privacy policies, each scoring 88%, while Huduma received 0%. These three agencies also made strides in pre-collection data transparency, with e-Citizen leading at 72%, followed by KRA at 58%, and ETA Kenya at 56%. Huduma once again scored 0% in this area. Data security efforts showed similar patterns, with ETA Kenya topping the sector at 44%, KRA at 40%, and e-Citizen at 20%, while Huduma received 0%.



All agencies, however, demonstrated poor performance in providing transparent reports and handling internal data breach resolutions, each scoring 0%. These results highlight the urgent need for improvements in privacy practices, data security, and compliance with data protection laws, particularly for the underperforming agencies.

f) Immigration Uganda, NIRA, Electoral Commission Uganda and UBOS (Uganda Bureau of Statistics)

The assessment of Immigration Uganda, NIRA, Electoral Commission, and UBOS reveals significant gaps in data protection compliance, despite these agencies being key data collectors in Uganda.



The figure above highlights varying levels of compliance with privacy practices and data protection laws. Two agencies scored a perfect 100% for registration with the national regulator, marking an important first step toward compliance. However, Immigration Uganda, the Electoral Commission, and UBOS scored 0% in this area, indicating a serious gap in their regulatory adherence.

UBOS stands out in the sector, being the only agency with an accessible privacy policy, scoring 63% for accessibility. It also led in third-party data transfers (60%) and pre-collection data transparency (17%), while the other agencies scored 0% in both areas. In terms of data security, UBOS (39%) and the Electoral Commission (22%) performed relatively better than Immigration Uganda and NIRA (22%).

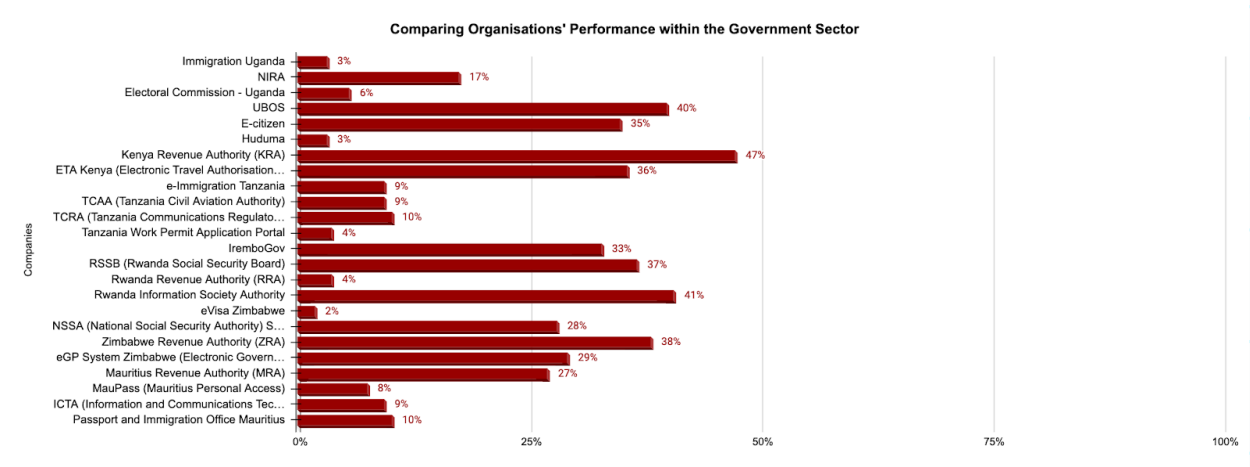
The lack of privacy policies from Immigration Uganda, NIRA, and the Electoral Commission is a major concern, leaving citizens vulnerable to data misuse and eroding public trust. Without policies, it's impossible to assess their compliance with data protection principles, and the absence of clear data rights or security measures increases privacy risks. Despite having a policy, UBOS still faces challenges, with poor pre-collection data transparency (17%) and no mention of data security, leading to low security header scores across all agencies.

Equally, none of the agencies have published a transparency report since 2023 nor offered internal data breach resolution mechanisms. UBOS is the only entity that does not allow third-party access to private personal data, scoring 60% in this indicator. These results underscore the urgent need for significant improvements in Uganda's government agencies' data protection practices, emphasizing the importance of stronger policies, transparency, and accountability to safeguard citizen data.

3.5.6.3 Comparison of companies/entities within the sector

The performance of government agencies in the assessed countries reveals significant gaps in their privacy practices and compliance with data protection laws. While some agencies have made progress in digitizing services, many still face considerable challenges in ensuring the secure and transparent handling of citizens' personal data.

Among the Ugandan agencies, the Uganda Bureau of Statistics (UBOS) stands out with a relatively higher score of 40%, but this is still a modest result considering the scale of data they handle. Immigration Uganda and the Electoral Commission have extremely low scores of 3% and 6% respectively, suggesting severe deficiencies in their privacy practices.



The National Identification and Registration Authority (NIRA) performs slightly better with a score of 17%, indicating some efforts to address privacy concerns but still falling far behind acceptable standards. These low scores reflect the significant risk of non-compliance with data protection regulations, particularly concerning transparency, data security, and informed consent.

In Kenya, Kenya Revenue Authority (KRA) performs relatively well with a score of 47%, indicating a stronger adherence to data protection and privacy practices compared to other agencies. However, agencies like Huduma and E-citizen have much lower scores (3% and 35%, respectively), signaling inadequate privacy measures in their digital services. The Electronic Travel Authorisation (ETA) system scores 36%, showing room for improvement, particularly in ensuring data security and transparent data usage practices. The low scores in several Kenyan agencies point to critical weaknesses in data protection, which could lead to privacy risks such as unauthorized access and misuse of personal data.

Tanzanian agencies such as e-Immigration Tanzania, TCAA, and TCRA score very low (9%, 9%, and 10%, respectively), indicating a major lack of compliance with data protection regulations. These low scores suggest that these agencies may not be implementing necessary security measures or transparent data practices, potentially putting citizens' data at significant risk. The Tanzania Work Permit Application Portal with a score of 4% further highlights the deficiencies in ensuring secure, transparent digital services.

Given these scores, Tanzania's e-government services must address critical gaps in data protection and compliance with privacy laws.

Rwanda's agencies like Rwanda Revenue Authority (RRA) and Rwanda Information Society Authority have relatively higher scores (37% and 41%, respectively), though still indicating a need for improvement in privacy practices. IremboGov has a score of 33%, reflecting some positive steps toward enhancing transparency and data security, though further work is needed. However, the Rwanda Social Security Board (RSSB) and RRA both have suboptimal scores, indicating that privacy practices, particularly in areas like data security and third-party data sharing, need significant enhancement. The scores suggest that while Rwanda is progressing in its digital government services, considerable gaps remain in their privacy and compliance frameworks.

Zimbabwe's agencies, including the Zimbabwe Revenue Authority (ZRA) and NSSA Self Service Portal, show some positive steps with scores of 38% and 28%, but agencies like eVisa Zimbabwe and the e-Government Procurement System score exceptionally low (2% and 29%), indicating major deficiencies in data protection practices.

The low scores in Zimbabwe reflect a lack of robust data security measures and transparency, which could lead to significant privacy risks and non-compliance with data protection laws.

The performance of Mauritian government agencies is similarly weak, with agencies like the Mauritius Revenue Authority (MRA) scoring 27% and MauPass at 8%. Other agencies such as ICTA and the Passport and Immigration Office Mauritius also have low scores (9% and 10%, respectively), suggesting substantial gaps in ensuring privacy and data protection. These agencies must improve their data handling practices, including better transparency regarding the data they collect and the security measures in place to protect citizens' personal information.

The consistently low scores across these countries' government agencies highlight serious privacy concerns and indicate a widespread lack of compliance with data protection laws. These agencies are at risk of exposing sensitive personal information to unauthorized access, misuse, and breaches. The absence of clear transparency about data collection and usage, inadequate data security measures, and insufficient third-party oversight further contribute to the privacy risks in these systems.

To improve, these agencies must prioritize data protection by investing in robust security measures, ensuring transparency in their data practices, and enforcing compliance with national and international data protection laws. Transparency around data collection, sharing, and usage, as well as strong encryption and access control systems, are essential steps to mitigating privacy risks and ensuring that citizens' data is handled securely and lawfully.

In summary, the e-government agencies in these countries face significant challenges in ensuring compliance with privacy and data protection standards. Addressing these issues is crucial not only to comply with legal requirements but also to build public trust and protect citizens' personal information from potential misuse.

3.5.6.4 Identification of sector-specific challenges and best practices

In the rapidly evolving e-government sector, privacy and data protection are paramount concerns as governments increasingly rely on digital platforms to deliver public services. These platforms often involve the collection, storage, and processing of sensitive personal data, creating significant privacy risks. To ensure that citizens' rights are respected and their data is protected, government agencies must address key privacy issues through best practices in transparency, security, citizen rights, and surveillance oversight.

I. Transparency

One of the biggest privacy concerns is the lack of transparency regarding how citizen data is collected, used, and retained by government agencies. Citizens are often unaware of why their data is being collected, how long it will be kept, and who will have access to it. This lack of transparency undermines trust in e-government services and can lead to a sense of powerlessness and vulnerability among the public.

Government agencies should provide clear and accessible privacy policies that explain the purpose, legal basis, and retention period for collecting personal data. These privacy notices should be easy to understand, written in plain language, and available to citizens at the point of data collection. Agencies must ensure that citizens are fully informed about how their data will be used and who will have access to it, which can help build trust and ensure compliance with data protection laws.

II. Security Infrastructure

With the increasing digitalization of government services, ensuring the security of citizen data is more critical than ever. Inadequate security infrastructure can expose citizens' personal information to breaches, hacking, or unauthorized access. Data breaches could lead to identity theft, financial fraud, or other forms of exploitation.

Governments should implement robust data security systems to protect sensitive data. This includes using encryption, secure data storage practices, and multi-factor authentication. Regular security audits should be conducted to identify vulnerabilities and ensure that security measures are up-to-date with evolving threats. Agencies should invest in training for their employees to ensure they understand security protocols and are vigilant in preventing unauthorized access or leaks of citizen data. Adoption of industry-standard security frameworks, such as the General Data Protection Regulation (GDPR) or ISO/IEC 27001, can provide a solid foundation for securing government systems and ensuring data protection.

III. Citizen Rights

IAs data collection and processing increase, citizens must have the ability to exercise their rights over their personal information.

This includes the right to access, correct, or delete data that government agencies hold about them. If these rights are not adequately protected, citizens may face difficulties in managing their personal data, leading to frustration and mistrust.

Government agencies should establish clear and accessible mechanisms for citizens to access their personal data, correct inaccuracies, and request deletion where applicable. A user-friendly portal or hotline should be made available for citizens to exercise these rights and get timely responses. Agencies should ensure compliance with data protection laws that grant individuals rights over their personal information, such as the GDPR's right to access, rectify, or erase data (also known as the "right to be forgotten"). These mechanisms should be clearly communicated to the public so that citizens are aware of how to assert their rights.

IV. Surveillance and Oversight

Many governments use digital platforms for surveillance purposes, whether for national security, law enforcement, or public safety. While surveillance can be beneficial, it raises serious privacy concerns, especially if it exceeds legal boundaries or lacks adequate oversight. Overreach in surveillance programs can infringe on citizens' fundamental rights to privacy and freedom of expression.

Surveillance programs should be governed by clear legal frameworks that specify the scope and limits of data collection and monitoring. Government agencies must ensure that surveillance practices are transparent, and they should publicly disclose the purpose and extent of any data collection or surveillance activities. There should be strong oversight mechanisms in place, such as independent bodies or data protection authorities, to ensure that surveillance programs are compliant with privacy laws and respect individual rights. Agencies should only collect and retain data that is necessary for the specific purpose at hand, ensuring that the data is not used for purposes beyond the initial mandate. Regular reviews and audits of surveillance programs should be conducted to ensure that they do not overreach or violate privacy rights.

In summary, privacy concerns in the e-government sector are crucial to ensuring that citizens' data is protected and their rights are respected. By prioritizing transparency, enhancing security infrastructure, safeguarding citizen rights, and ensuring proper oversight of surveillance programs, government agencies can mitigate risks and build public trust in digital governance.

Implementing these best practices will not only improve compliance with data protection laws but will also foster a more accountable, transparent, and secure environment for citizens interacting with e-government services.

3.5.7 Health Sector Analysis

3.5.7.1 Overview of the sector and data collectors evaluated

The health sector in East and Southern Africa, including countries like Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda, is characterized by ongoing efforts to digitize and improve healthcare services. These countries have made strides in using electronic health records, mobile health initiatives, and data collection systems to enhance service delivery and improve health outcomes. However, privacy practices among data collectors in these regions remain varied and often insufficient, raising concerns over data protection and compliance with privacy laws.

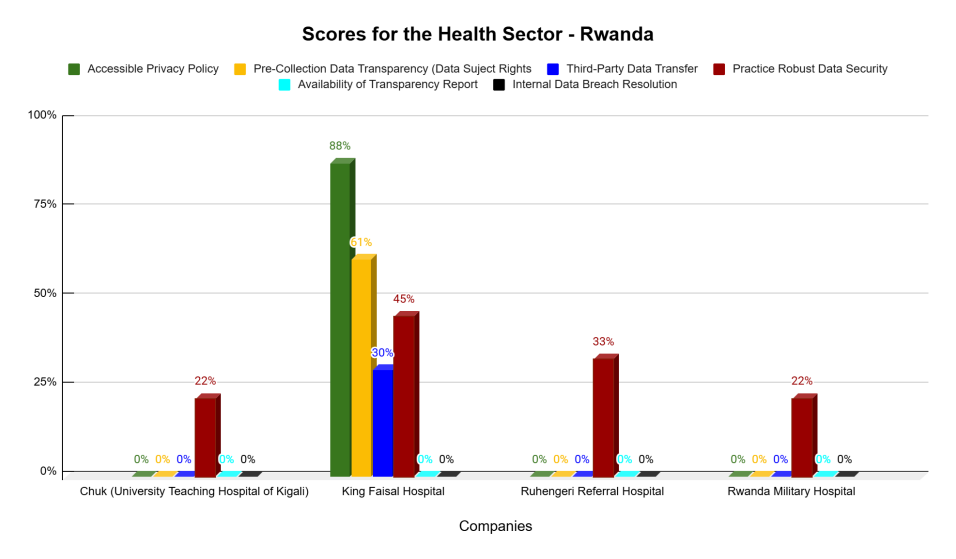
In terms of privacy practices, Rwanda has made notable progress with strong data protection laws and systems in place for health data privacy, but enforcement remains inconsistent. Kenya has made advancements, especially with the Health Data Governance Framework, though there are concerns over data security, particularly with mobile health data collection. Uganda and Tanzania face challenges with limited privacy regulations, and privacy violations are common in health data collection processes. Zimbabwe and Mauritius have some regulatory frameworks in place, but their enforcement and the implementation of strong data protection practices are still weak.

A major issue across the region is the lack of comprehensive privacy policies among health data collectors, leading to concerns about the unauthorized sharing of personal health information. Many countries lack robust mechanisms for safeguarding data from breaches, and there is a general absence of transparency in data collection and usage practices. These gaps highlight the urgent need for stronger enforcement of privacy laws and more rigorous data protection measures to ensure the confidentiality and security of health data in the region.

3.5.7.2 Analysis of compliance with each criterion

a) Chuk (University Teaching Hospital of Kigali), King Faisal Hospital, Ruhengeri Referral Hospital and Rwand Military Hospital in Rwanda

Among the health facilities assessed, King Faisal Hospital emerged as the leader in privacy practices, achieving an impressive 88% overall score, making it the only facility with an accessible privacy policy. The hospital also led in compliance with pre-collection data transparency and third-party data transfer, scoring 61% and 30%, respectively.



However, the rest of the hospitals demonstrated significantly weaker performance in these areas, with some scoring as low as 0%. In terms of data security, while all hospitals received recognition for their efforts, King Faisal Hospital again outperformed others, though it only scored 45%. The next highest scores were Rwanda's Ruhengeri Referral Hospital at 33%, followed by Chuk and Rwanda Military Hospital, both scoring just 22%. Additionally, all hospitals exhibited poor performance in providing transparent reports and handling internal data breaches, with scores again falling to 0%. These results underscore the pressing need for improvements in data privacy practices and compliance with data protection laws across the sector, particularly in areas such as transparency, data security, and breach resolution.

The data policy of King Faisal as already observed is publicly available on their website, noticeable, and fairly readable, with a word count of 354 and a Hemingway readability score of 11.

Key points: Contact information is not provided, reason for data collection is not mentioned, data types summarily stated, duration of control is stated as lawfully permissible, third-party sharing - not listed, but data can be shared with third parties, excluding advertisers and personalized advertising is not allowed. Data rights - access, correction, and permanent deletion are mentioned, but the process is not detailed. Restriction of data processing is unconditional and complaint rights are not mentioned. Law enforcement access is granted when reasonably requested.

Regarding data security, King Faisal mentions security measures but does not provide specifics. The SSL server score is B, and the security header score is F.

Other hospitals like Chuk, Ruhengeri, and Rwanda Military Hospital do not mention data security, while King Faisal's policy makes a vague reference.

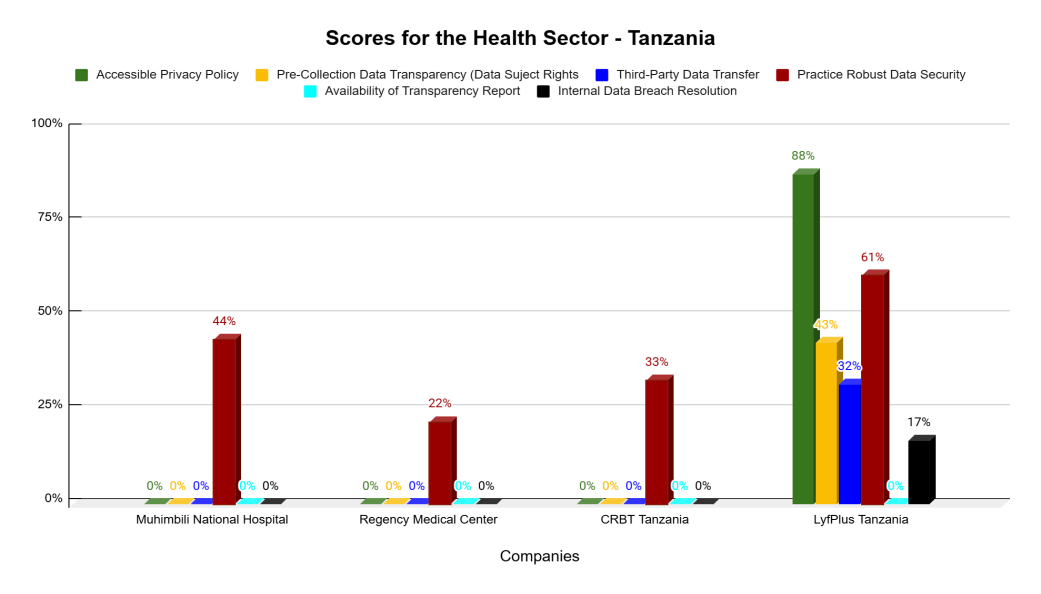
b) Muhimbili National Hospital, Regency Medical Center, CRBT Tanzania and LyfPlus Tanzania in Tanzania

The health facilities assessed all received credit for efforts to advance data security, but performance varied significantly across the sector. LyfPlus Tanzania emerged as the leader, scoring 61% in data security, followed by Muhimbili National Hospital at 44%, CRBT Tanzania at 33%, and Regency Medical Center at 22%. In terms of privacy practices, LyfPlus Tanzania also outperformed the other facilities, achieving top scores in having an accessible privacy policy (88%), pre-collection data transparency (43%), third-party data transfers (32%), and internal data breach resolution (17%). However, the rest of the hospitals—Muhimbili National Hospital, Regency Medical Center, and CRBT Tanzania—demonstrated weak performance across these areas, with scores as low as 0% in transparency reports and internal data breach resolution.

Lyfplus, a digital clinic in Tanzania offering medical services through its app and website has its privacy policy with 2875 words long, easy to read, and provides important details regarding data collection and security.

Additionally, the policy explains why data is collected, the types of data, and how it is used. It also specifies the company's contact details (phone number, address, and email). Personal data may be shared with advertisers, but the specific third parties are not listed. The policy does not mention the right to access, correct, or restrict data, nor does it explain how complaints about data breaches can be lodged. Instructions for reporting breaches are unclear. The policy outlines security measures, but the website's security score is below an 'F'. The app has one tracker, which presents minor concerns. Data can only be shared with law enforcement upon reasonable request. The policy does not specify how data breaches will be handled or provide a clear timeframe for investigations.

Muhimbili National Hospital does not have a privacy policy, so it couldn't be assessed on privacy-related issues such as data rights or breach handling. However, the hospital's website has a relatively good security score (C) and uses 5 trackers, though this is not a major concern due to the lack of a privacy policy and the availability of a transparency report.



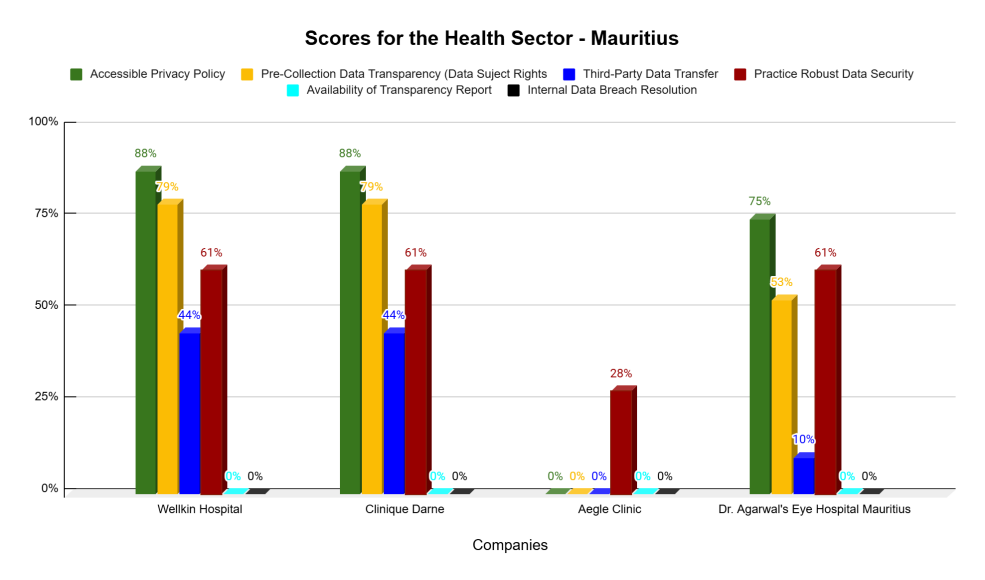
In summary, Lyfplus provides a comprehensive privacy policy, but there are significant gaps in terms of data rights and breach resolution, while Muhimbili lacks a policy altogether, making it difficult to evaluate its data privacy practices. Equally the results above indicate that while some facilities have made efforts to improve data security and privacy practices, there is a widespread need for stronger policies, enhanced transparency, and better management of data breaches to comply with data protection laws and protect patient privacy.

c) *Wellkin Hospital, Clinique Darne, Aegle Clinic and Dr Agarwal's Eye Hospital Mauritius in Mauritius*

Three health facilities were recognized for having accessible privacy policies, with Wellkin Hospital and Clinique Darne leading the sector at 88% each, followed by Dr. Agarwal's Eye Hospital Mauritius at 75%. These facilities were also acknowledged for their efforts in advancing data security, each scoring 61%, while Aegle Clinic lagged behind with only 28%. In terms of pre-collection data transparency, Wellkin Hospital and Clinique Darne again led the sector, both scoring 75%, with Dr. Agarwal's Eye Hospital Mauritius scoring 53%. When it comes to third-party data transfers, Wellkin Hospital and Clinique Darne topped the sector with scores of 44% each, followed by Dr. Agarwal's Eye Hospital Mauritius at 10%. However, all the assessed facilities demonstrated weak performance in areas such as transparency reports and internal data breach resolution, each scoring 0%.

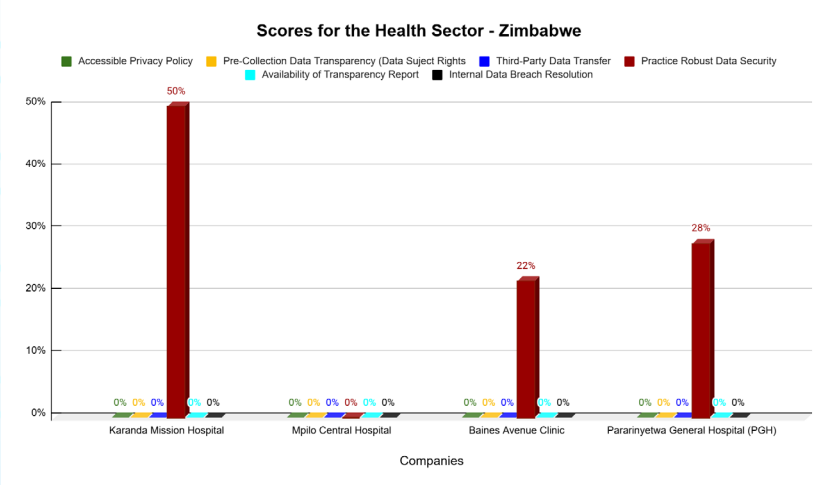
Aegle Clinic, in particular, exhibited lower compliance across the sector, highlighting significant gaps in its privacy practices and data protection efforts.

Overall, while the leading facilities made notable progress in privacy policies, data security, and third-party data transfer practices, there is a clear need for improvement in areas like transparency and breach management to ensure full compliance with data protection laws and enhance patient trust.



d) *Karanda Mission Hospital, Mpilo Central Hospital, Baines Avenue Clinic and Pararinyetwa General Hospital (PGH) in Zimbabwe*

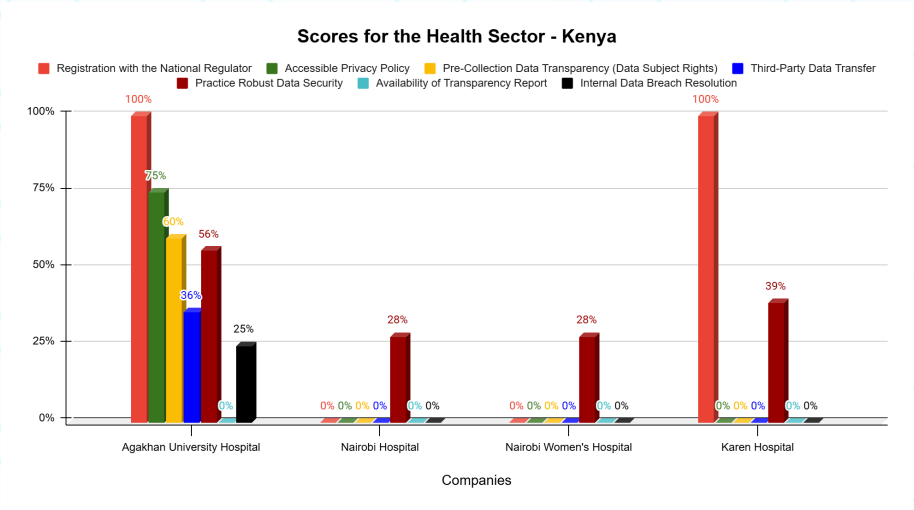
Although three health facilities were recognized for their efforts to advance data security, Karanda Mission Hospital, which topped the sector, only achieved a score of 50%, followed by Pararinyetwa General Hospital at 28% and Baines Avenue Clinic at 22%.



Despite these efforts in data security, all the facilities demonstrated weak compliance in several critical areas, including accessible privacy policies, pre-collection data transparency, third-party data transfers, transparency reports, and internal data breach resolution. In fact, each of these areas saw scores as low as 0%. These low scores indicate that while there are some efforts to improve data security, significant gaps remain in other crucial aspects of privacy and data protection. The facilities must urgently address these deficiencies to improve their overall compliance with data protection laws and better protect patient data.

e) Agakhan University Hospital, Nairobi Hospital, Nairobi Women's Hospital Karen Hospital in Kenya

From the figure below, two health facilities, Agakhan University Hospital and Karen Hospital, were commended for taking the initial step toward compliance with data protection laws by registering with the national regulator, each achieving a perfect score of 100%. However, the remaining facilities scored 0%. Agakhan University Hospital also led the sector with a privacy policy accessibility score of 75% and pre-collection data transparency at 60%. While it performed well in some areas, such as third-party data transfers and internal data breach resolution, scoring 36% and 25% respectively, its overall data protection efforts still leave room for improvement.

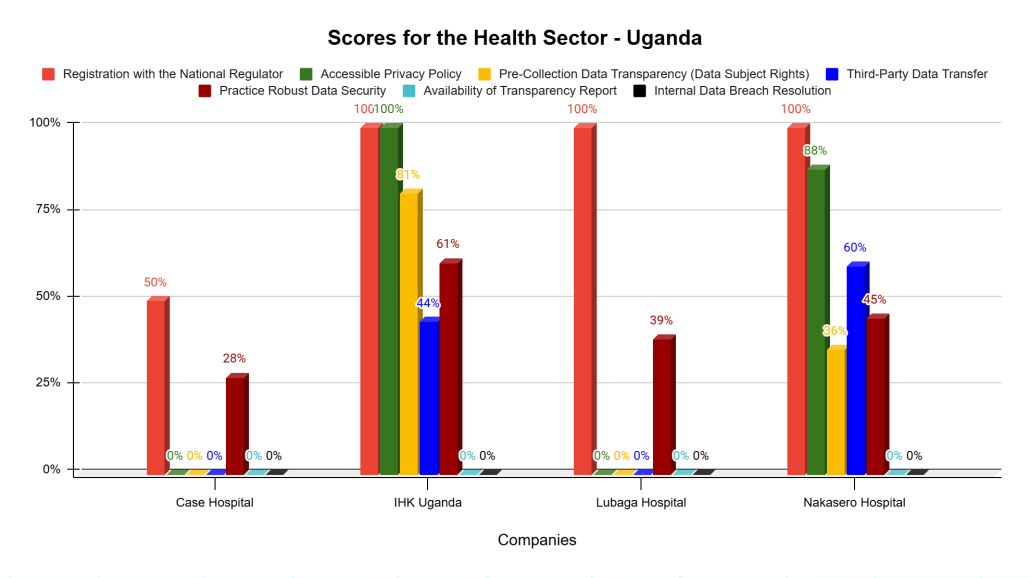


Despite being recognized for advancing data security, Agakhan University Hospital's data security score was only 56%, followed by Karen Hospital at 39%, and both Nairobi Hospital and Nairobi Women's Hospital scored just 28%. These scores reflect a concerning gap in the health facilities' ability to meet key data protection standards, which could have significant implications for their compliance with data protection laws and their commitment to safeguarding patient privacy. The varying performance levels suggest a need for further efforts in addressing privacy practices and enhancing data security measures to fully comply with legal and ethical obligations.

f) Case Hospital, IHK Hospital, Lubaga Hospital and Nakasero Hospital in Uganda

The evaluation of Case Hospital, IHK Uganda, Lubaga Hospital, and Nakasero Hospital reveals significant gaps in data protection practices among private healthcare providers in Uganda. While all four hospitals are registered with Uganda's national privacy regulator (NITA-U), Case Hospital's registration is inactive.

Three hospitals—IHK Uganda, Lubaga Hospital, and Nakasero Hospital—received perfect scores for registration (100%), while Case Hospital scored only 50%. There was a notable contrast in the availability of privacy policies: IHK Uganda (100%) and Nakasero Hospital (88%) had clear, accessible policies, whereas Case and Lubaga Hospitals scored 0% due to the absence of privacy policies altogether.

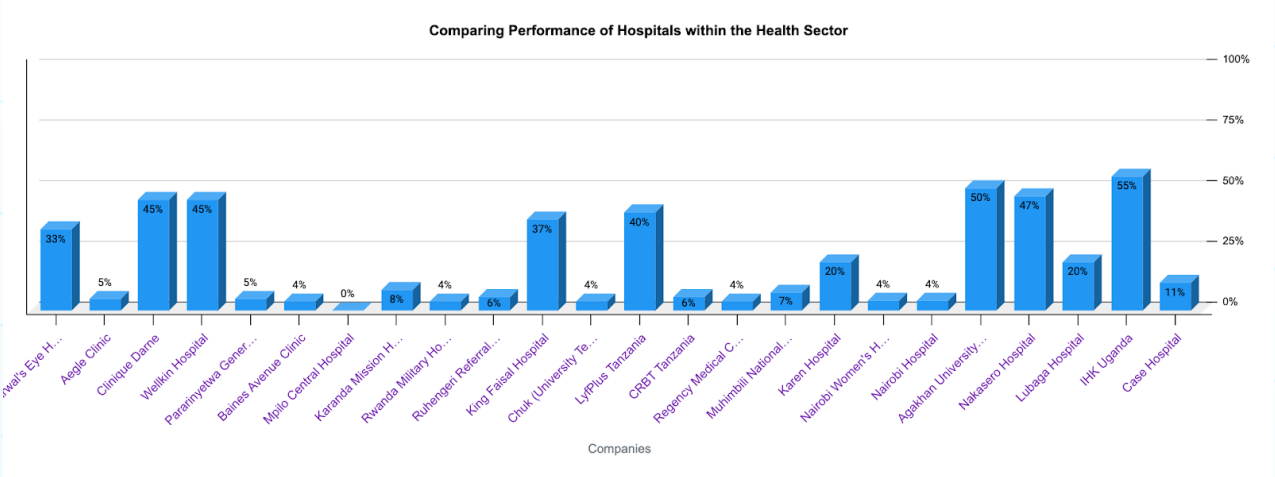


Additionally, IHK Uganda scored the highest in pre-collection data transparency (81%), while Nakasero Hospital scored only 36%. Nakasero Hospital outperformed others in third-party data transfers, scoring 60%, while IHK Uganda scored 44%. In terms of data security, IHK Uganda led with 61%, followed by Nakasero Hospital (45%), Lubaga Hospital (39%), and Case Hospital (28%). Case and Lubaga Hospitals showed weaknesses across multiple areas, including a lack of data subject rights, third-party data transfer policies, and internal data breach resolution mechanisms. None of the hospitals published a transparency report since 2023, reflecting a significant lack of accountability.

Despite efforts to improve data security, Case and Lubaga Hospitals' lack of privacy policies raises serious concerns about patient data protection. Stronger privacy frameworks, transparency, and data security measures are urgently needed to ensure compliance with data protection laws and to protect sensitive patient information in Uganda's healthcare sector.

3.5.7.3 Comparison of companies/entities within the sector

The scores of health facilities across Uganda, Kenya, Tanzania, Rwanda, Zimbabwe, and Mauritius, as reflected in the scorecard report, reveal concerning trends in privacy practices and compliance with data protection laws. In Uganda, hospitals like IHK Uganda (55%) and Nakasero Hospital (47%) scored the highest, though their scores still indicate significant gaps in privacy and data protection compliance.



Other Ugandan hospitals, such as Case Hospital (11%), Lubaga Hospital (20%), and Nakasero Hospital (47%), performed poorly, signaling insufficient privacy policies, data security measures, and transparency in handling health data. Kenya shows similarly weak performance, with Agakhan University Hospital (50%) showing the best score among the listed institutions. Nairobi Hospital and Nairobi Women's Hospital, both scoring a dismal 4%, indicate that these facilities are severely lacking in implementing even basic privacy practices or complying with data protection regulations. Karen Hospital (20%) falls in between, further highlighting inconsistencies within the country's health data management sector.

Tanzania's health facilities also exhibited low scores, with Muhimbili National Hospital (7%), Regency Medical Center

(4%), and CRBT Tanzania (6%) reflecting poor adherence to data protection laws. LyfPlus Tanzania (40%) performed relatively better, but still, all these facilities clearly struggle with ensuring robust privacy policies and securing personal health data. In Rwanda, most hospitals scored poorly, with Chuk (University Teaching Hospital of Kigali), King Faisal Hospital, and Rwanda Military Hospital each scoring just 4%. Rwanda's healthcare facilities show major gaps in both policy implementation and compliance. Only King Faisal Hospital (37%) showed moderate progress, but still far from meeting the expected standards for health data privacy.

Zimbabwe's health facilities had very low scores across the board, with Mpilo Central Hospital scoring 0% and Karanda Mission Hospital (8%) and Baines Avenue Clinic (4%) also failing to demonstrate adequate privacy practices. Only Pararinyetwa General Hospital (PGH) showed a slight improvement with 5%, indicating widespread challenges in data protection across the sector in Zimbabwe. In Mauritius, both Wellkin Hospital and Clinique Darne scored 45%, reflecting moderate compliance with privacy and data protection practices. Aegle Clinic (5%) and Dr. Agarwal's Eye Hospital Mauritius (33%) lag behind, demonstrating inconsistencies and room for improvement.

The overall low performance of these health facilities signals significant issues with privacy practices and compliance with data protection laws. Low scores reflect a lack of comprehensive data security measures, insufficient privacy policies, and minimal transparency in data collection, usage, and sharing. These deficiencies pose risks of unauthorized access to sensitive health information, data breaches, and potential misuse of patient data. For the facilities scoring poorly, such as Nairobi Women's Hospital (4%) or Mpilo Central Hospital (0%), urgent steps are needed to address these gaps. These facilities must implement stronger data protection frameworks, enhance staff training, and improve transparency with patients regarding data handling and privacy.

Overall, the health sector across East and Southern Africa appears to require significant reforms and stronger enforcement of data protection laws to ensure the safety and privacy of patient data. These scores suggest that healthcare providers must prioritize compliance with national and international data protection standards to build trust, safeguard patient confidentiality, and avoid legal and reputational risks.

3.5.7.4 Identification of sector-specific challenges and best practices

The health sector faces several key privacy concerns and risks, particularly as health data becomes increasingly digitized and shared across various platforms. Below are some of the primary concerns and how data collectors can address them:

I. Data Breaches and Unauthorized Access

Health data is highly sensitive and often targeted by cybercriminals. A breach can expose personal medical information, leading to identity theft, blackmail, or misuse. Data collectors must implement strong security measures such as encryption, firewalls, and multi-factor authentication to protect data from unauthorized access. Regular audits and security updates are essential to stay ahead of potential threats. Additionally, access to sensitive data should be strictly limited to authorized personnel only.

II. Inadequate Consent Management

Patients may not be fully informed about how their data is being collected, used, or shared. This lack of transparency can lead to breaches of trust and violations of privacy laws.Data collectors should obtain explicit and informed consent from patients before collecting or using their data. This involves clearly explaining the purpose, scope, and duration of data collection. Consent management systems should be implemented to track and update consent regularly, especially if data is shared with third parties.

III. Inconsistent Data Handling Across Platforms

Health data often flows across multiple systems (e.g., hospitals, insurance providers, and research organizations). Inconsistent handling and security across these platforms increase the risk of data loss, misuse, or exposure. Standardized data protection protocols should be implemented across all platforms. Health data should be shared only when necessary, and whenever possible, data should be anonymized or pseudonymized to reduce privacy risks.

Additionally, data collectors should use secure, interoperable platforms that comply with data protection laws.

IV. Lack of Data Minimization

Collecting excessive data that is unnecessary for patient care or business purposes increases the risk of mishandling, leaks, or misuse. Data collectors should adopt the principle of data minimization, meaning they only collect the data that is necessary for specific, legitimate purposes. Regular reviews should be conducted to ensure that data collection practices remain relevant and appropriate.

V. Third-Party Sharing and Data Transfers

Health data is frequently shared with third-party vendors (e.g., cloud services, insurance companies, or research entities), which may not have sufficient privacy protections in place. This increases the risk of data exposure and unauthorized use. Data collectors should implement strict data-sharing agreements and ensure third parties comply with privacy standards. This includes ensuring that third-party vendors use encryption, secure data storage, and have robust access controls. Additionally, data transfers across borders should comply with international data protection regulations, such as GDPR.

VI. Lack of Transparency in Data Usage

Patients often don't understand how their data is being used beyond their direct care, such as for research or marketing purposes. Health data collectors should provide clear, accessible privacy policies that outline how patient data is used, stored, and shared. Patients should have the option to opt-out of non-essential uses of their data, and transparency should be maintained at all stages of data collection.

VII. Retention and Disposal of Data

Retaining health data longer than necessary or failing to securely dispose of data when it is no longer needed creates unnecessary risks of exposure or misuse. Data retention policies should be established to ensure that health data is only kept for as long as necessary for its intended purpose. When data is no longer required, it should be securely destroyed or anonymized to prevent unauthorized access or use.

VIII. Failure to Comply with Regulations

Inadequate compliance with privacy laws such as GDPR, HIPAA, or national data protection laws can result in legal liabilities, fines, and damage to reputation. Data collectors must ensure they are familiar with and compliant with local, regional, and international data protection laws. Regular compliance audits should be conducted to identify gaps in privacy practices and address them proactively. It's essential to appoint a data protection officer (DPO) or establish a privacy team to oversee compliance efforts.

In sum, the health sector faces significant privacy challenges, but by adopting strong security measures, transparent data policies, and ensuring compliance with data protection laws, health data collectors can mitigate risks and safeguard sensitive information. Data collectors must prioritize privacy by design and default, ensuring that all health data handling practices respect patient rights and maintain trust.

3.5.8 Digital Loans Sector Analysis

3.5.8.1 Overview of the sector and data collectors evaluated

The digital loan services sector in East and Southern Africa has experienced rapid growth in recent years, driven by increased smartphone usage, mobile money platforms, and a rising demand for accessible financial services. Digital lenders have made it easier for individuals to access quick, short-term loans, often without the need for traditional credit history checks. This sector is particularly important in countries like Uganda, Kenya, Tanzania, Rwanda, Mauritius, and Zimbabwe, where access to traditional banking services remains limited, and financial inclusion is a priority for governments and institutions.

In Kenya, Uganda, and Tanzania, mobile lending platforms, such as M-Shwari, Branch, Tala, and other fintech services, have become popular. These platforms offer loans directly via mobile phones, often using alternative data sources (like mobile phone usage and payment history) for credit scoring.

The market is growing, with millions of users depending on these services for quick access to funds. In Mauritius and Zimbabwe, the landscape is a bit more developed, with digital lending services becoming more regulated as they gain popularity. While Rwanda's digital loan market is still emerging, the country is showing signs of embracing digital financial services, including for loans.

The increasing collection and use of personal and financial data by digital lenders raise significant privacy concerns. These companies typically gather sensitive information, such as mobile phone records, social media activity, and transaction history, to assess creditworthiness. While this data collection can enable more inclusive lending, it also exposes individuals to potential misuse, data breaches, or exploitation of personal data.

In East and Southern Africa, concerns about data privacy in the digital lending sector are growing. In Kenya, companies often share borrowers' data with third parties or use it for marketing without proper consent, despite the 2019 Data Protection Act aiming to improve privacy practices. However, enforcement remains inconsistent, and many lenders don't fully comply. Uganda faces similar issues, with the relatively new 2019 Data Protection and Privacy Act offering limited enforcement, leading to non-compliance with data storage and sharing requirements. Tanzania's 2022 Data Protection Act addresses data privacy but struggles with transparency and misuse of personal data in lending. Rwanda's 2021 law on personal data protection includes strict requirements, but the rapid growth of digital lenders raises concerns about full compliance.

Mauritius has stronger regulations, but concerns remain about how personal data is used by fintechs. Zimbabwe's data protection framework is still developing, and the informal nature of some lenders raises significant privacy risks. Overall, while progress is being made, enforcement gaps and inconsistent practices continue to undermine effective data protection in the digital lending industry across these countries.

Many digital lenders fail to implement adequate security measures to protect consumers' personal and financial data. The sharing of data between lenders, third parties, and even with government entities often occurs without clear consent from the borrower, risking misuse or exploitation. Borrowers are often unaware of how their data is being used or shared, which raises concerns about informed consent. The terms and conditions of loan agreements are sometimes not clear, and the use of alternative data for credit scoring is not always explained. Digital lenders often use aggressive marketing tactics and offer loans with high-interest rates, which can lead to a cycle of debt for vulnerable borrowers. In some cases, lack of regulation allows lenders to push borrowers into situations where they are unable to repay. Although many countries have introduced data protection laws, enforcement remains weak. Additionally, digital lenders often operate across borders, making it difficult to hold them accountable under national laws. Some lenders may also circumvent regulations by operating under the guise of non-traditional financial services.

Consumers often lack avenues to challenge unfair lending practices or to seek redress for data misuse. As digital lenders expand, the need for stronger consumer protection mechanisms becomes more urgent. The digital loan services sector holds significant promise for financial inclusion but presents a range of privacy and regulatory challenges.

While countries like Kenya and Uganda have introduced data protection laws, inconsistent enforcement, lack of awareness, and weak consumer protection mechanisms continue to hinder the sector's compliance with data protection standards. The rapid growth of digital lending platforms makes it crucial for governments to strengthen regulations and ensure that lenders uphold data privacy, transparency, and security to protect consumers in this fast-evolving market.

3.5.8.2 Analysis of compliance with each criterion

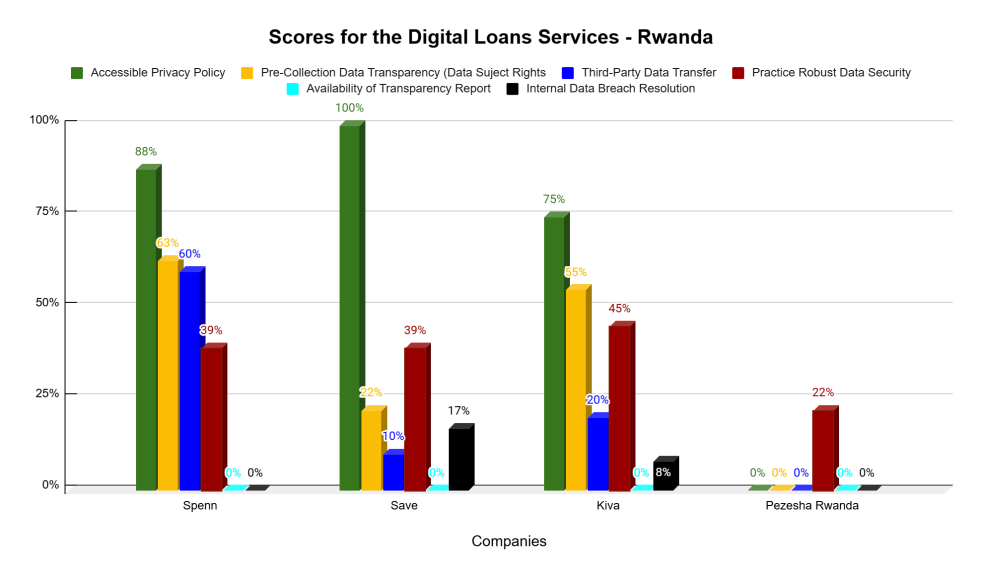
a) Spenn, Save, Kiva and Pezesha Rwanda in Rwanda

Three digital lending platforms were recognized for having accessible privacy policies, with Save leading at 100%, followed by Spenn at 88% and Kiva at 75%, while Pezesha Rwanda scored 0%. In terms of pre-collection data transparency, Spenn took the lead with a score of 63%, followed by Kiva at 55%, and Save at just 22%. On third-party data transfers, Spenn again led at 60%, with Kiva at 20% and Save at 10%. Although all platforms were acknowledged for their efforts in advancing data security, Kiva topped the sector with a score of 45%, while Spenn and Save tied at 39%, and Pezesha Rwanda scored only 22%.

Save and Kiva made some efforts to address internal data breach resolution, scoring 17% and 8%, respectively, while other platforms scored 0%, including for transparency reports. These scores highlight significant gaps in the platforms' compliance with data protection laws and privacy practices.

While some platforms are making progress, particularly with privacy policies and data transparency, their overall performance indicates weaknesses in securing user data, managing third-party data transfers, and resolving internal data breaches.

With the exception of Pezesha Rwanda, which does not have a policy, the other digital loan service providers (Spenn, Save, and Kiva) have publicly posted data policies. These policies are noticeable, with word counts of 187, 797, and 3994 respectively. In terms of readability, Save's policy is highly readable (score of 8 on Hemingway), Spenn's is fairly readable (score of 2), while Kiva's policy is less readable (score below 14).



Additionally, Spenn's policy does not provide contact details, mentions the reason for data collection and the type of data, and states the duration of control as lawfully permissible, does not allow sharing data with third parties or advertisers, but allows personalized advertising with opt-in, unconditional rights to correction and deletion, but conditional rights to access and restriction, rights to lodge complaints are mentioned, law enforcement access is allowed with a court order or subpoena and no specifics on data breach resolution or law enforcement access.

Kiva's policy does not provide contact details, details data collection reasons, types of data, and duration of control as lawfully permissible, allows data sharing with advertisers, with opt-in for personalized advertising, rights to deletion and restriction are unconditional; access and correction are not mentioned. Rights to lodge complaints are mentioned, law enforcement access is granted when reasonably requested and no clear instructions for data breach resolution or reporting.

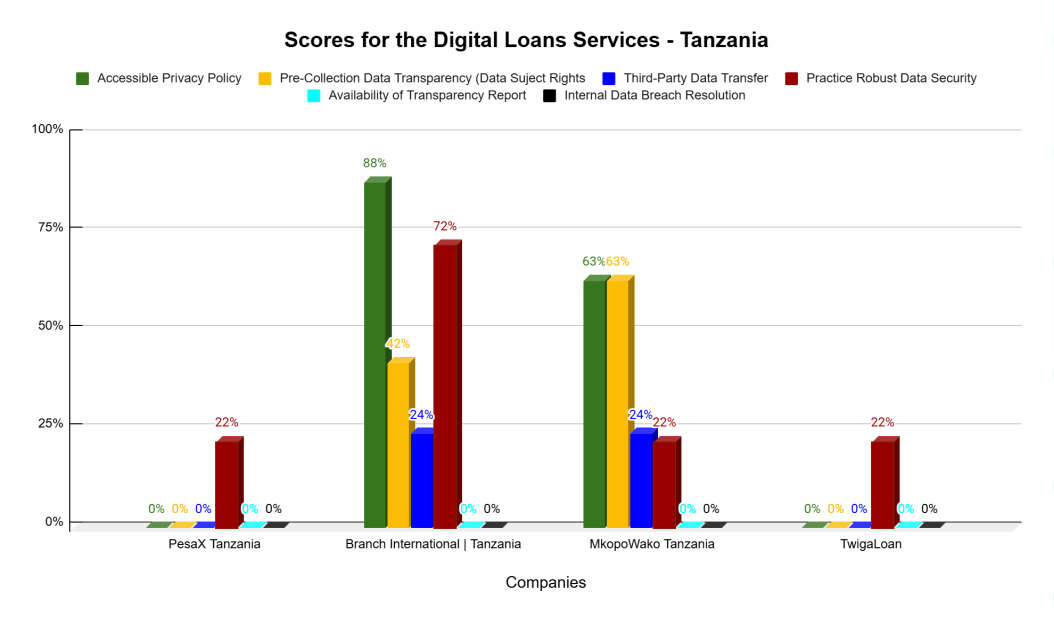
On the hand, Save's policy does not provide contact details. Mentions data collection reasons and types, but not the duration of control. Allows data sharing with advertisers, but no personalized advertising, does not mention rights to access, correction, restriction, or deletion. No complaints rights are mentioned nor is law enforcement access specified. Mentions a limited mechanism for reporting data breaches, but the process is unclear.

Data Security: All three policies mention data security but lack specifics. Pezesha does not mention data security. SSL Server Scores: B (Spenn), B (Save), A (Kiva), A (Pezesha). Security Header Scores: F (Spenn), F (Save), F (Kiva), F (Pezesha). None of the entities had a transparency report.

This raises concerns about their ability to fully comply with data protection regulations, potentially putting user privacy at risk and exposing the platforms to regulatory challenges.

b) PesaX Tanzania, Branch International Tanzania, MkopoWako Tanzania and TwigaLoan in Tanzania

Two digital lending platforms, Branch International Tanzania and MkopoWako Tanzania, were credited for having accessible privacy policies, with Branch leading the sector at 88%, followed by MkopoWako at 63%. In terms of pre-collection data transparency, MkopoWako Tanzania scored highest at 63%, while Branch International Tanzania followed at 42%, and both PesaX and TwigaLoan scored 0%.



Both Branch International Tanzania and MkopoWako Tanzania were recognized for efforts to comply with third-party data transfer regulations, but their scores were low at only 24% each.

All platforms were acknowledged for efforts to improve data security, with Branch International Tanzania leading at 72%, while the others scored 22%. However, all platforms displayed weak performance in areas such as transparency reports and internal data breach resolution, with scores as low as 0%. These results suggest that while some platforms have made strides in certain areas, significant gaps remain in their overall privacy practices and compliance with data protection laws. The low scores in third-party data transfers, data transparency, and internal breach management indicate that these platforms may be at risk of non-compliance with key privacy regulations, potentially compromising user data security and leaving them vulnerable to legal and reputational risks.

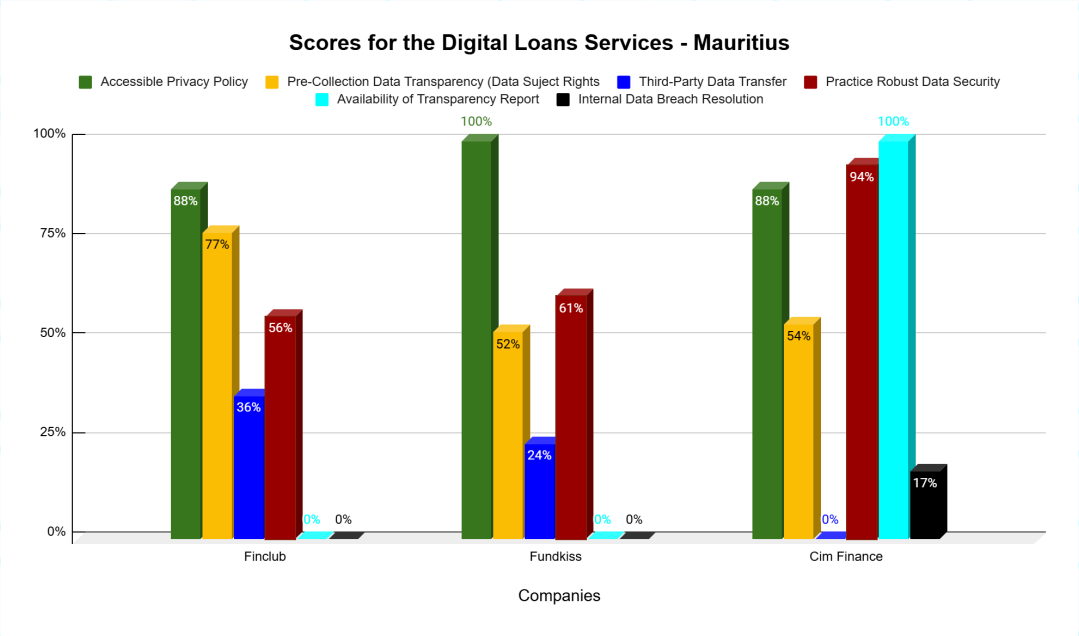
Branch, a personal finance app offering services like loans, money transfers, and bill payments has a privacy policy clearly published on its website footer and scored 12 on the Hemingway Editor, indicating it is generally understandable. The policy is 1714 words long, providing relatively detailed information.

Additionally, the policy lists reasons for collecting data and details the personal data collected. It allows for marketing with prior notice and provides the right to delete personal data. However, it does not mention data access rights or the duration of data storage. Only an email is provided for privacy concerns, with no phone number or physical address. The app and website have 2 and 3 trackers respectively, raising minor security concerns. The lack of a transparency report is more concerning.

Mkopowako, another online lending app in Tanzania with a privacy policy that is 2051 words long and scored 23 on readability, slightly better than Branch. The policy also provides the company's contact details (address, phone number, and email), lists the personal data collected, and explains the reasons for collecting data. The right to access and delete data is conditional, and it is unclear whether users can file complaints and clear contact details are provided. The app's website uses 2 trackers, but the security scan results were poor. The policy does not mention how data is secured. Both companies have some cybersecurity concerns, but Branch's lack of a transparency report is a notable issue.

c) Finclub, Fundkiss and Cim Finance from Mauritius

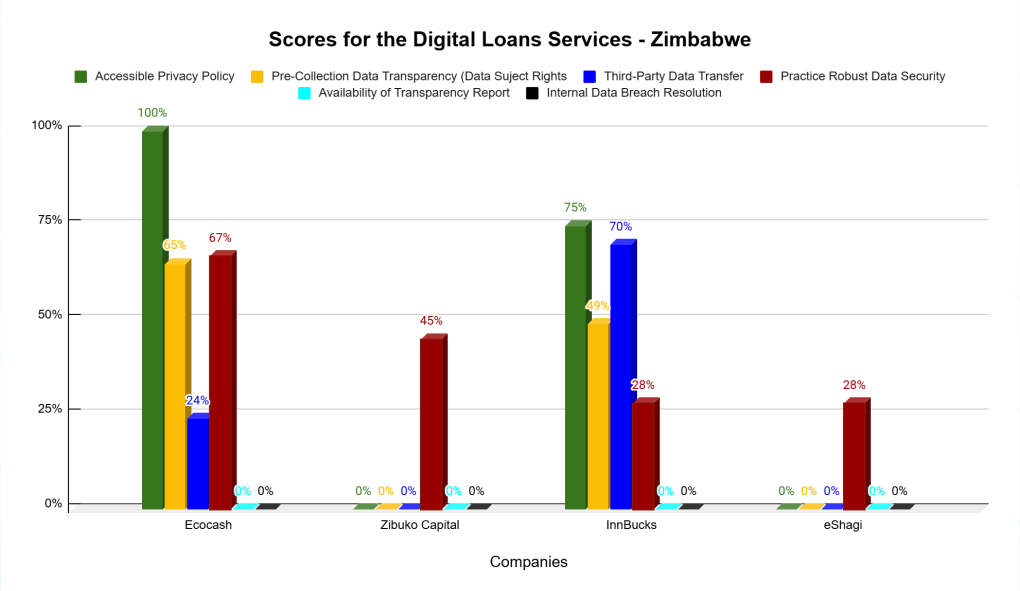
All the platforms were recognized for having accessible privacy policies, with Fundkiss leading the sector at 100%, followed by Finclub and Cim Finance, both at 88%. Cim Finance stood out for having a transparency report, achieving a perfect score of 100%, while the other platforms scored 0%. In terms of pre-collection data transparency, Finclub led with 77%, followed by Cim Finance at 54% and Fundkiss at 52%. They were also credited for their efforts to advance data security, with Cim Finance leading at 94%, followed by Fundkiss at 61% and Finclub at 56%.



However, in the area of third-party data transfers, although Finclub topped the sector, its score of 36% was still relatively low, with Fundkiss at 24% and Cim Finance scoring 0%. Regarding internal data breach resolution, only Cim Finance made an effort, scoring 17%, while the other platforms scored 0%. These scores highlight that while some platforms, particularly Fundkiss and Cim Finance, have made strides in data privacy and security, significant gaps remain in their compliance with data protection laws, especially in areas such as third-party data transfers and internal breach management. The low scores in key compliance areas raise concerns about their ability to fully safeguard user data and meet legal requirements, potentially exposing them to regulatory risks and reputational damage.

d) Ecocash, Zibuko Capital, InnBucks and eShagi from Zimbabwe

Among the four platforms, only Ecocash and InnBucks were recognized for having accessible privacy policies, with Ecocash leading at 100% and InnBucks at 75%, while Zibuko Capital and eShangi scored 0%. In terms of pre-collection data transparency, Ecocash and InnBucks were the only platforms credited, with scores of 65% and 49%, respectively. Both platforms also made demonstrable efforts toward compliance with third-party data transfers, scoring 70% for Ecocash and 24% for InnBucks. All platforms were recognized for efforts toward data security, with Ecocash leading the sector at 67%, followed by Zibuko Capital at 45%, and both InnBucks and eShangi scoring 28%.

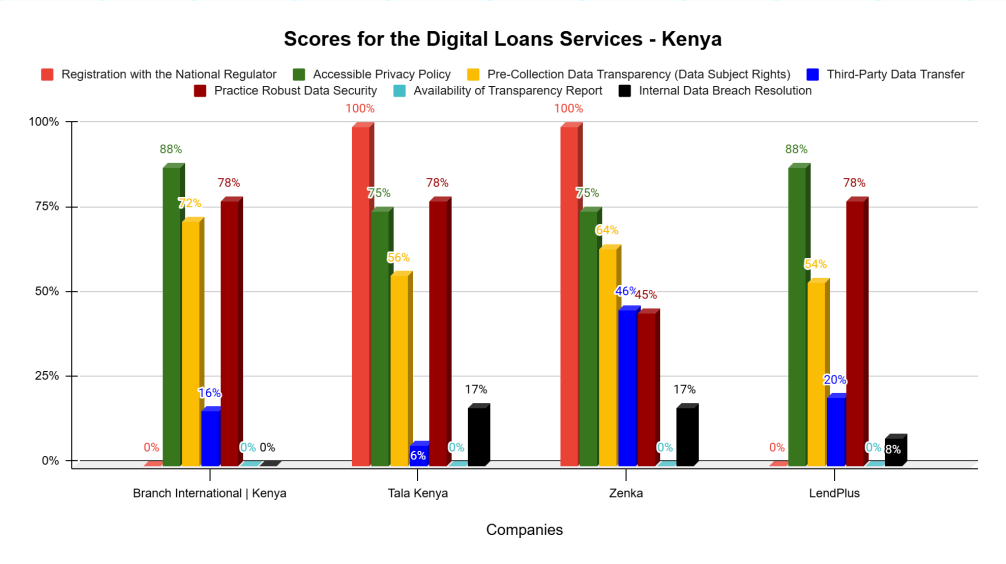


However, all four platforms showed weak performance in the areas of transparency reports and internal data breach resolution, with scores as low as 0%. These results suggest that while Ecocash and InnBucks have made some progress in complying with data protection regulations, particularly in privacy policies, pre-collection transparency, and third-party

data transfers, there are significant gaps in their overall compliance, especially regarding data breach management and transparency. Zibuko Capital and eShangi, with their very low scores, appear to be struggling to meet key privacy and data protection requirements, raising concerns about their ability to protect user data and adhere to regulatory standards.

e) Branch International Kenya, Tala Kenya, Zenka and LendPlus from Kenya

Two platforms, Tala Kenya and Zenka, were recognized for registering with the national regulator, marking an important initial step toward compliance with data protection laws, each scoring 100%. All platforms were acknowledged for having accessible privacy policies, with Branch International Kenya and LendPlus leading at 88% each, followed by Tala Kenya and Zenka at 75% each. In terms of pre-collection data transparency, Branch International Kenya topped the sector at 72%, followed by Zenka at 64%, Tala Kenya at 56%, and LendPlus at 54%. All platforms demonstrated efforts toward data security, with Branch International Kenya, Tala Kenya, and LendPlus leading at 78% each, while Zenka scored much lower at 45%. In the area of third-party data transfers, Zenka led with a score of 46%, followed by LendPlus at 20%, Branch International Kenya at 16%, and Tala Kenya at only 6%.

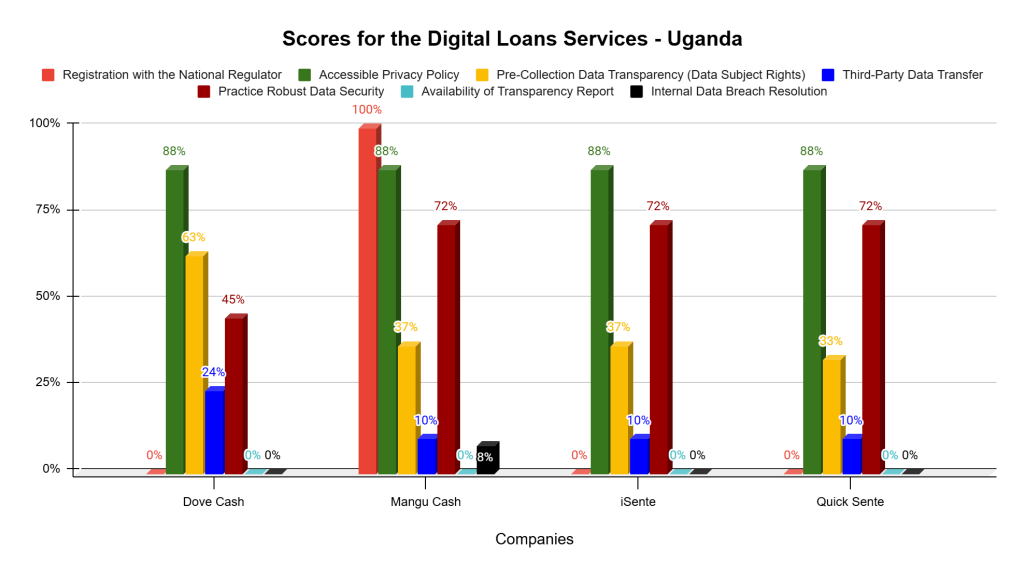


While Tala Kenya and Zenka were credited for efforts toward internal data breach resolution, they scored only 17% each, with LendPlus scoring 8%. All platforms showed weak performance in the area of transparency reports, scoring 0%. These results indicate that while platforms like Tala Kenya and Zenka are making progress, particularly in registration and accessible privacy policies, significant gaps remain in their compliance with key areas of data protection, such as third-party data transfers, transparency reports, and internal breach resolution. The low scores in these critical areas suggest that these platforms may struggle to fully meet regulatory requirements, potentially exposing them to legal risks and undermining user trust in their ability to safeguard personal data.

f) Dove Cash, Mangu Cash, iSente and Quick Sente from Uganda

The analysis of Dove Cash, Mangu Cash, iSente, and Quick Sente reveals notable strengths and weaknesses in their data privacy and protection practices. While all platforms are recognized for having accessible privacy policies, each earning an 88% for policy accessibility, only Mangu Cash complies with registration with NITA-U, Uganda's national privacy regulator, achieving a top score of 100%, while the others scored 0%.

Additionally, Dove Cash leads with 63%, though it still imposes restrictions on key rights like data access and permanent deletion. Mangu Cash (37%), iSente (37%), and Quick Sente (33%) score poorly, indicating limited recognition of user rights.

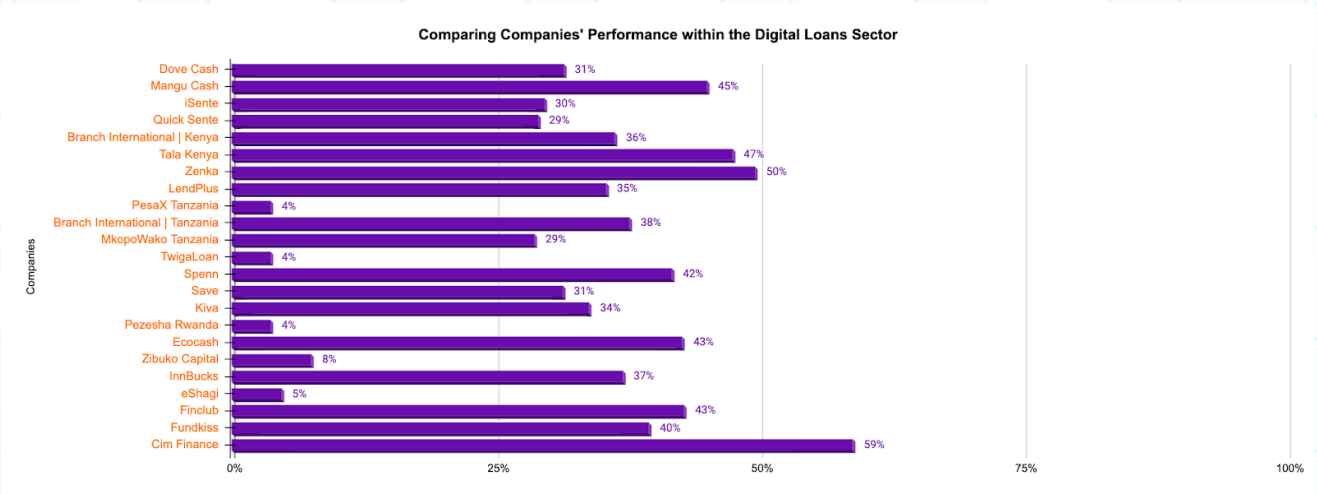


All platforms, except Dove Cash (24%), score 10% due to sharing personal data with third parties and advertisers without clear specifications on which third parties or types of data are shared. Mangu Cash, iSente, and Quick Sente score well at 72%, while Dove Cash lags behind with only 45% due to a poor security header rating on its website. Dove Cash leads with 63%, followed by Mangu Cash and iSente at 37%, and Quick Sente scoring 33%.

None of the companies have published a transparency report since 2023. Data breach resolution is weak across all platforms, with Mangu Cash scoring 8% for vague mention of data breaches, while the others scored 0%. While Mangu Cash stands out for its registration and data security efforts, all platforms face significant challenges in crucial areas such as data subject rights, third-party data transfers, and data breach resolution. The low scores in these key areas suggest that the platforms are at risk of failing to fully comply with data protection laws, potentially exposing them to regulatory penalties and eroding user trust.

3.5.8.3 Comparison of companies/entities within the sector

The performance of digital loan service providers across East and Southern Africa reveals a diverse landscape in terms of compliance with privacy practices and data protection laws. While some platforms show considerable efforts toward meeting legal requirements, many still face significant gaps in their adherence to privacy and data security regulations.



In Uganda, Mangu Cash led with a score of 45%, significantly higher than other platforms like iSente (30%) and Quick Sente (29%), and Dove Cash (31%). Mangu Cash's relatively better score suggests it may have made more progress in establishing privacy policies, data transparency, and security measures, though it still faces challenges in areas like third-party data transfers and internal data breach resolution. The low overall scores indicate that these platforms collectively struggle with regulatory compliance and protecting user data, leaving them vulnerable to data privacy risks and regulatory scrutiny.

In Kenya, Tala Kenya (47%) and Zenka (50%) had the highest scores in the sector, showing some commitment to data security, accessible privacy policies, and data transparency. However, their scores remain below the threshold for full compliance with data protection laws, particularly in the areas of third-party data transfers and internal data breach management. Branch International Kenya (36%) and LendPlus (35%) performed weaker in comparison, highlighting ongoing deficiencies in addressing key privacy practices. These gaps could expose them to legal risks related to user data handling.

In Tanzania, PesaX (4%) and TwigaLoan (4%) scored the lowest, indicating a severe lack of compliance with data protection regulations. Branch International Tanzania (38%) and MkopoWako Tanzania (29%) performed somewhat better but still faced challenges in areas such as data transparency and third-party data transfers. These platforms' low scores suggest that data protection practices are not sufficiently robust, potentially putting consumers' personal information at risk.

Rwanda showed a bit more diversity in scores, with Spenn (42%) and Save (31%) showing better efforts towards data security and privacy practices. However, Pezesha Rwanda (4%) had the lowest score, suggesting poor compliance with key data protection laws. The platforms' struggles with transparency and third-party data transfers point to potential risks in handling sensitive user data. Kiva (34%) falls in between, with room for improvement across all privacy and compliance areas.

In Zimbabwe, Ecocash (43%) performed better than other platforms, reflecting a stronger commitment to data privacy and security. InnBucks (37%) followed closely, but Zibuko Capital (8%) and eShagi (5%) performed poorly in all areas, highlighting significant gaps in compliance and privacy practices. This weak performance across the board raises concerns about how user data is handled and the platforms' capacity to comply with data protection regulations.

Cim Finance (59%) was the standout performer in Mauritius, reflecting strong compliance with data protection regulations, especially in terms of data security and transparency. Finclub (43%) and Fundkiss (40%) also showed efforts to comply but with room for improvement. While these platforms have made progress, particularly in accessible privacy policies and data security, their lower scores in third-party data transfers and internal breach resolution indicate that they still have compliance gaps.

Across the board, the platforms' performance in data privacy and protection suggests significant room for improvement. While some platforms have made strides, particularly in establishing privacy policies and ensuring data security, many remain weak in areas such as third-party data transfers, internal breach resolution, and transparency. The low overall scores in several countries, especially in Tanzania, Uganda, and Zimbabwe, point to a lack of adequate data protection practices, which can expose users to privacy risks, including unauthorized data sharing, security breaches, and misuse of personal information. These deficiencies also imply potential regulatory risks, as countries in the region are increasingly focusing on enforcing data protection laws. Digital lending platforms that fail to meet these standards could face legal actions, fines, and loss of consumer trust. To mitigate these risks, platforms must strengthen their data security practices, ensure transparency in their data collection and use, and fully comply with third-party data transfer regulations.

3.5.8.4 Identification of sector-specific challenges and best practices

The digital loan services sector in East and Southern Africa faces several key privacy concerns related to data protection and compliance with relevant laws. These concerns highlight significant risks to consumer privacy, security, and the overall integrity of the financial ecosystem.

The main privacy issues include:

I. Data over-Collection and lack of informed Consent

Many digital loan platforms collect vast amounts of personal data, including mobile phone numbers, financial information, and even location data, often without obtaining clear, informed consent from users. This raises concerns about whether users are fully aware of what data is being collected and how it will be used. Some platforms collect more data than necessary for processing loans, which increases the risk of misuse or unauthorized access. There is often no clear justification for the collection of sensitive information.

II. Unclear or Excessive Sharing and risk of data misuse

Digital lenders often share borrower data with third parties, including marketing companies, credit bureaus, or even other financial institutions. The lack of transparency in these data-sharing practices, and the absence of clear user consent, exacerbates privacy risks. Borrowers' personal information may be misused for purposes beyond loan-related activities, such as targeted advertising or unauthorized credit assessments, especially when third-party relationships are not adequately disclosed.

III. Weak Security Measures and data breaches

Many platforms score poorly in ensuring robust data security practices. Insufficient encryption, inadequate network security protocols, and poor internal data protection measures make user data vulnerable to breaches, hacking, and unauthorized access. The platforms' ability to detect, respond to, and resolve internal data breaches is often lacking, which heightens the risk of large-scale data compromises affecting customers' sensitive information.

IV. Lack of Transparency in Data Practices

While many platforms have privacy policies in place, these policies are often vague, difficult to understand, or hard to find. Inadequate transparency about data collection practices, processing, storage, and retention leads to confusion and distrust among users. Many platforms fail to provide regular transparency reports outlining how they collect, process, store, and share user data, leaving users uncertain about how their data is being handled.

V. Regulatory Noncompliance & Data Retention Gaps

In many countries, digital lending platforms struggle to comply with national data protection laws (such as Uganda's Data Protection and Privacy Act or Kenya's Data Protection Act).

Weak enforcement and inconsistent regulatory oversight in the region result in significant compliance gaps. Some platforms fail to clearly define how long user data will be retained, potentially leading to unnecessary storage of sensitive personal information, which increases the risk of unauthorized access or misuse over time.

VI. Inadequate Breach Management

Few platforms have established proper internal processes to identify, address, and report data breaches. This lack of internal breach resolution mechanisms puts consumers at risk of long-term exposure to the consequences of data leaks or unauthorized access.

The key privacy concerns in this sector are rooted in poor data management practices, lack of transparency, insufficient security measures, and inconsistent compliance with data protection laws. These issues expose users to significant risks, including data breaches, unauthorized data sharing, and privacy violations. As the digital lending market continues to grow, there is an urgent need for stronger data protection frameworks, improved transparency, and better enforcement of privacy regulations to safeguard consumers' personal information and ensure trust in the sector.

4. COMPARATIVE REVIEW OF DATA PROTECTION *LANDSCAPE IN ASSESSED COUNTRIES*

This part examines the data protection frameworks in Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda, highlighting key regulations, compliance requirements, and enforcement efforts. It compares how each country safeguards personal data, aligns with international standards, and addresses challenges such as data retention, user rights, and cross-border transfers. By assessing the legal and institutional landscapes, the report provides insights into regional trends, gaps, and best practices in data protection.

4.1 Data Protection Landscape in Rwanda

Rwanda has witnessed remarkable technological advancements, positioning Information and Communication Technology (ICT) as a central driver of its transformation into a knowledge-based economy.[7] The government's commitment is evident in its budgetary allocations to ICT, which align with global standards, including those of many OECD countries.[8]

ICT plays a critical role in achieving Rwanda's National Strategy for Transformation & Prosperity and Vision 2035 and 2050 goals. The strategic plan emphasizes a real-time, service-oriented governance system, with key pillars such as Smart Cities, Fintech, Smart Agriculture, Trade & Industry, Health, Education, Government, and Women and Youth Empowerment in ICT.[9]

A significant milestone in Rwanda's digital landscape is the enactment of the Data Protection and Privacy (DPP) Law on October 15, 2021. This law provided a two-year compliance grace period, which ended on October 15, 2023. The establishment of the Data Protection and Privacy Office (DPPO) under the National Cyber Security Authority (NCSA) in March 2022 further reinforced the implementation of this framework.

Rwanda has achieved significant digitalization across various sectors:

- *Telecommunications:* Nearly 100% 4G network coverage, with an operating speed of 48.12 kbit/s, [10] and mobile-cellular subscriptions exceeding 78.1%.[11]
- *Financial Services:* A 96% financial inclusion rate among adults, with 92% formally served. Mobile money transactions have surged, with 86% (6.9 million) of Rwandans using mobile money services.
- *Justice System:* Implementation of the Rwanda Integrated Electronic Case Management System (IECMS), enhancing efficiency in legal proceedings.

7 Rwanda Development Board, ' ICT in Rwanda' available at < https://rdb.rw/departments/information-communication-technology/ > accessed on 14th July, 2024.
8 The New Times, 'ICT Regulation: Efficiency in transforming Rwanda's economy' (8th August 2017, The New Times) available at < https://www.newtimes.co.rw/article/143082/News/sponsored-ict-regulation-efficiency-in-transforming-rwandas-economy > accessed on 11th July, 2024; See also, Microsoft at < https://www.microsoft.com/mea/trustedcloud/rwanda/public-sector.aspx > accessed 11th July, 2024; See also, Rwanda Development Board, ' ICT in Rwanda' available at < https://rdb.rw/departments/information-communication-technology/ > accessed on 14th July, 2024.
9 See, MITEC, ' ICT sector strategic plan (2018 – 2019): Towards digital enabled economy' (November 2017), available at < https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Policies/ICT_SECTOR_PLAN_18-24_.pdf > accessed on 5th July, 2024.
10 Statista,'Digital and connectivity indicators – Rwanda ' available at < https://www.statista.com/outlook/co/digital-connectivity-indicators/rwanda > accessed on 10th July, 2024.
11 MINICT, 'Rwanda ICT Sector profile: ICT for sustainable development' (September 2019) available at < https://www.minict.gov.rw/publications/ict-sector-profile > last accessed on 6th July, 2024.

Despite progress, concerns remain regarding the independence of the Data Protection Office (DPO), both administratively and financially. The DPO operates under the NCSA, which has multiple responsibilities and budgetary constraints. The dependency on NCSA funding limits its ability to function autonomously.

However, the DPO has actively enforced the DPP law through:

- Public sensitization campaigns, including the 'Tekana Online' initiative.
- Capacity building for DPO staff.
- Publication of regulatory documents, including data transfer authorization forms and complaint filing guides.

The NCSA issued its first regulation under Article 66 of the DPP Law, two years after its establishment, clarifying the renewal process for data processors and controllers.

Rwanda's right to privacy is constitutionally enshrined in Article 23, prohibiting arbitrary interference with citizens' private lives.[12] This is reinforced by the DPP Law,[13] which aligns with international standards, including the African Union Convention on Cyber Security and Personal Data Protection and the European Union's General Data Protection Regulation (GDPR).

Complementary legal instruments supporting data governance in Rwanda include:

- *National Data Revolution Policy:* Centralizing government data in a national data center.[14]
- *Organic Law on Statistics:* Regulating the production, access, and dissemination of statistical data.[15]
- *Penal Code & Law No. 18/2010*: Governing electronic messages, signatures, and transactions.[16]

The DPP Law applies to: Data controllers and processors established or residing in Rwanda and entities processing personal data within or outside Rwanda concerning Rwandan nationals.

The law mandates: Consent-based data processing[17]; Differentiation between personal and sensitive data[18]; stringent data collection, control, and processing guidelines[19]; registration and renewal procedures for data controllers and processors.[20]

The DPP Law imposes strict penalties for violations, including:

- *Unlawful access, collection, use, or disclosure of personal data: 1-3 years imprisonment and fines of RWF 700,000 to RWF 10 million.*
- *Unlawful re-identification of de-identified data: 3-5 years imprisonment and similar fines.*
- *Unlawful destruction, erasure, or alteration of personal data: 1-3 years imprisonment.*
- *Unlawful sale of personal data: 5-7 years imprisonment and fines up to RWF 15 million.*
- *Unlawful processing of sensitive personal data: 7-10 years imprisonment and fines up to RWF 25 million.*

12 Available at < https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.cpaafricaregion.or.tz/uploads/member_country/constitutions/1551774581-constitution-rwanda.pdf&ved=2ahUKEwio6_-d07-HAxVwBNsEHTO2BvcQFnoECBcQBg&usg=AOvVaw3V--hLjXW9YUHV6gkQg1dH > accessed on 10th July, 2024.
13 Law No 058 of 2021, Available at < https://www.risa.gov.rw/index.php?eID=dumpFile&t=f&f=65369&token=15e7fad700949646dd7c1faae89f9663048f4f92 > accessed 29th July, 2024.
14 Ministerial Order No. 001/MINICT/2012, available at < https://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data > accessed on 1st July, 2024.
15 Law No. 45 of 2013, available at < https://www.statistics.gov.rw/sites/default/files/publications/031a2a22-05a1-4874-a69a-226ae8b5b7d5/Official_Gazette_no_Special_of_16.06.2013%20%281%29%20%281%29.pdf > accessed 1st July, 2024.
16 Available at < https://ictpolicyafrica.org/en/document/tdbqoq8ft4?page=11 > accessed on 1st July,2024.
17 See article 6.
18 See articles 4 and 10.
19 See articles 11, 12 and 13.
20 See Article 17.

The NCSA, established under Law No.26/2017, is the primary regulator responsible for implementing the DPP Law.[21] Key responsibilities include: Maintaining a registry of data controllers and processors; investigating complaints and enforcing compliance; advising on data protection policies; cooperating with national and international data protection authorities; issuing regulations, including recent rules on registration certificate renewal. It still remains to be seen that the authority passes more regulations to elaborate on more critical aspects like dispute resolutions and appellate procedures.

The DPPO operates under the NCSA, limiting its financial and operational independence. Nonetheless, it plays a vital role in: Enforcing data protection laws through sensitization campaigns, providing resources for compliance, including complaint forms and procedural guides, and conducting awareness initiatives such as cybersecurity and data protection training.

Rwanda has made significant strides in data protection, backed by a robust legal framework and institutional mechanisms. However, challenges such as the financial and administrative dependence of the DPO require attention. Strengthening regulatory independence and expanding enforcement efforts will enhance Rwanda's data governance landscape, fostering digital trust and attracting further investment.

Efforts were also made to engage with Rwanda's Data Protection and Privacy Office to gain direct insights into critical regulatory areas such as registration, enforcement, institutional capacity, public engagement, and compliance oversight. While the Data Protection and Privacy Law of 2021 marked a crucial milestone in Rwanda's data protection framework, there has been little progress in its practical implementation, enforcement, and regulatory engagement. Unlike other regional counterparts, Rwanda has yet to introduce supporting regulations, operational guidelines, or an enforcement framework to ensure organizations comply with the law.

The assessment sought to evaluate progress in the following areas:

- Rwanda lacks a publicly accessible register of data controllers and processors, and there is no available data on active or inactive registrations. This lack of transparency raises concerns about whether organizations are effectively complying with data protection requirements.
- Information regarding complaints filed, investigations conducted, and penalties imposed is unavailable, suggesting that no significant enforcement actions have taken place since the law was enacted.
- There is limited public information on the staffing, technological capabilities, and financial resources of the Data Protection Office, making it unclear whether it has the capacity to enforce compliance effectively.
- Unlike other jurisdictions that have established operational guidelines, codes of conduct, or updates to address emerging privacy challenges, Rwanda has yet to introduce detailed regulations to support the law's implementation.
- Although some awareness efforts have been made, there are no structured initiatives to educate citizens and businesses about their data privacy rights, complaint procedures, or compliance obligations.
- There is no evidence of compliance audits, proactive investigations, or sector-specific risk assessments, particularly in high-risk industries like telecommunications, finance, and healthcare.

Thus, the lack of regulatory enforcement and transparency creates several challenges:

1. *Limited Transparency:* Without publicly available compliance data, businesses, policymakers, and civil society groups struggle to evaluate enforcement trends, compliance levels, and overall regulatory effectiveness.
2. *Weak Oversight:* The absence of enforcement reports and compliance monitoring mechanisms raises uncertainty over whether the Data Protection Office is actively regulating data privacy or has the necessary capacity to do so.
3. *Public Trust Deficit:* With no clear enforcement mechanisms or regulatory updates, citizens and businesses lack guidance on their rights and responsibilities, which may undermine trust in the law's effectiveness.
4. *Limitations in the Privacy Scorecard:* Due to the lack of direct regulatory engagement and enforcement data, this assessment relies primarily on publicly available resources, independent research, and industry insights. Consequently, the Privacy Scorecard may not fully capture the current state of compliance and regulatory challenges in Rwanda.

21 Law Establishing the National Council for Cyber Authority and Determining its mission, organisation and functioning.

Hence, to ensure that Rwanda's Data Protection and Privacy Law is meaningfully implemented, the Data Protection and Privacy Office must take proactive steps to strengthen oversight, including:

- Issuing comprehensive regulations to provide clear compliance guidelines, enforcement procedures, and sector-specific obligations.
- Developing a publicly accessible register of data controllers and processors to improve transparency and compliance tracking.
- Publishing enforcement reports that detail complaints, investigations, and regulatory actions, ensuring accountability and deterrence.
- Engaging with stakeholders, including businesses, civil society, and international data protection bodies, to align Rwanda's approach with global data privacy standards.
- Expanding public awareness initiatives to ensure individuals understand their data privacy rights and that organizations receive adequate compliance guidance.
- Enhancing institutional capacity, including hiring more regulatory staff, increasing budget allocations, and fostering international collaborations to strengthen enforcement efforts.

While Rwanda has established a strong legal foundation for data protection, the law remains largely theoretical without concrete enforcement and regulatory action. Strengthening transparency, enforcement, and stakeholder engagement is essential to bridge the gap between policy and practice, ensuring that data protection is not just a legal obligation but an actively enforced right.

4.2 Data Protection Landscape in Tanzania

Tanzania's legal landscape on data protection and privacy is composed of various laws that either primarily or secondarily address these concerns. The supreme law, the Constitution of Tanzania, sets the foundation for privacy rights, as outlined under Article 16, which states: *"Every person is entitled to respect and protection of his person, the privacy of his own person, his family and of his matrimonial life, and respect and protection of his residence and private communications*." However, this right is not absolute, as Article 16(2) allows the state to establish legal procedures that may limit the right to privacy in certain circumstances.

Before the enactment of the Personal Data Protection Act (PDPA), Tanzania lacked a comprehensive data protection framework, relying on sector-specific regulations such as the Electronic and Postal Communications Act, 2010 (EPOCA)[22] and its supporting regulations. These include: The Electronic and Postal Communication (Consumer Protection) Regulations,[23] the Electronic and Postal Communications (Investigation) Regulations,[24] The Electronic and Postal Communications (Computer Emergency Response Team) Regulations.[25]

The PDPA, enacted to fill these legislative gaps, provides a robust regulatory framework governing the collection, processing, and use of personal data. The PDPA governs data protection and privacy in both Mainland Tanzania and Zanzibar, but for Zanzibar, it applies only to Union matters such as defense, immigration, and national security. The Act adopts key principles from the European General Data Protection Regulation (GDPR), including: Lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality.

The PDPA grants individuals several rights concerning their personal data, including: accessing personal data held by data controllers, rectification of inaccurate or incomplete data, prevention of processing likely to cause harm, erasure (right to be forgotten), objection to direct marketing and, compensation for damage caused by misuse of personal data.

These rights, however, are subject to exceptions. For instance, individuals may not be notified about data collection if it is publicly available, authorized by law, or necessary for law enforcement purposes. Under the PDPA, data controllers and processors must: Register with the PDPC before collecting or processing personal data, obtain explicit consent from individuals before collecting their data, ensure data accuracy and relevance, process data only for the stated purposes, and maintain security safeguards to protect against unauthorized access, loss, or destruction.

22 Act No.3 of 2010, The Laws of Tanzania.
23 Government Notice No. 61 published on 23/02/2018.
24 Government Notice No.287 published on 16/08/2017.
25 Government Notice No. 60 published on 23/02/2018.

Additionally, processing of sensitive personal data (e.g., genetic data, biometric data, political or religious beliefs, financial transactions) requires explicit prior consent from the data subject. The PDPA imposes strict controls on international data transfers, allowing them only if the receiving country has adequate data protection laws or the transfer meets specified safeguards.

Before the PDPA, responsibilities for data protection were dispersed among different sectoral regulators, including the Tanzania Communications Regulatory Authority (TCRA) and the Tanzania Police Force. The PDPA has centralized this under the Personal Data Protection Commission (PDPC).

The Ministry of Communication and Information Technology, established in 2020, plays a crucial role in ICT policy formulation. The Minister of ICT appoints members to the PDPC board[26] and hears appeals on data controller registrations.[27]

Tanzania Communications and Regulatory Authority (TCRA) established in 2003, regulates telecommunications and broadcasting. It maintains the Central Equipment Identification Register (CEIR), storing mobile subscriber data,[28] which has raised privacy concerns due to potential surveillance risks. The Content Committee within TCRA handles consumer complaints regarding data privacy violations by content service providers (CSPs). Under the Electronic and Postal Communications (Online Content) Regulations, 2020, CSPs must resolve complaints within 12 hours, failing which consumers can escalate matters to the Content Committee.

Tanzania Police Force (Cybercrimes Unit) investigates computer-related crimes and enforces the Cybercrimes Act, particularly in cases of unlawful data access, identity fraud, and online offenses.[29]

The Personal Data Protection Commission (PDPC), established under the PDPA, is the primary data protection regulator.[30] It is important to note that whereas the PDP Act came into effect on May 1st 2023, the commission was launched on 3rd April 2024.[31] Its key functions include: Enforcing data protection laws, registering data controllers and processors, investigating complaints of data privacy violations, conducting public awareness campaigns on data protection, advising the government on data protection policies and collaborating internationally on data protection matters.[32] Equally, the PDPC is the main regulatory body overseeing compliance with key principles underpinning the Act as higlighted above.

In sum, Tanzania's data protection and privacy landscape has significantly evolved with the introduction of the Personal Data Protection Act (PDPA). The Act provides a comprehensive legal and institutional framework for personal data governance. While it enhances privacy rights, it also imposes obligations on businesses, government entities, and individuals handling personal data. However, challenges remain, including potential limitations on privacy rights due to broad exemptions for law enforcement and national security. Ensuring effective enforcement and public awareness will be crucial for realizing the full benefits of the PDPA in protecting personal data in Tanzania.

As part of this assessment, efforts were made to engage with Tanzania's PDPC to obtain firsthand insights into key regulatory areas, including registration, enforcement actions, institutional capacity, public engagement, and compliance monitoring.

Tanzania has taken significant steps in data protection governance, particularly through the enactment of the Personal Data Protection Act, 2022, and the establishment of the PDPC as the regulatory authority. However, despite these positive advancements, direct outreach to obtain specific enforcement data, institutional capacity details, and regulatory updates did not yield responses.

The assessment sought insights into the following areas:

- Availability of a public register listing data controllers and processors, as well as statistics on active versus inactive registrations. While Tanzania has made efforts to establish a registration system, there is limited publicly available information on its implementation and accessibility.

26 Section 8(3) PDP Act.
27 Section 20 PDP Act.
28 Bowmans Law,Privacy and Data Protection in Tanzania (part 1) <https://bowmanslaw.com/insights/privacy-and-data-protection-in-tanzania-part-1/> Accessed 24th July 2024.
29 For instance Sections 4 & 6.
30 Section 6(1) of the PDP Act.
31 The Citizen, Tanzania launches commission to oversee personal data protection, Thursday 4th April, 2024 <https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-commission-to-oversee-personal-data-protection-4577912> Accessed 25th July 2024.
32 Section 7(a) – (h).

- Information on complaints received, investigations conducted, and penalties imposed, particularly in high-profile cases, remains largely unavailable.
- An assessment of the PDPC's staffing levels, technological resources, budget allocations, and international collaborations to support enforcement efforts.
- Updates on operational guidelines, codes of conduct, and amendments to address emerging privacy and cybersecurity challenges.
- Efforts to educate citizens and businesses on their data privacy rights, complaint mechanisms, and compliance obligations. Tanzania has made commendable efforts in awareness-building initiatives, including training programs for data protection officers (DPOs).
- Insights into compliance audits, proactive investigations, and risk-based monitoring, particularly for high-risk sectors like telecommunications, banking, and healthcare.

Despite these inquiries, regulatory responses were not forthcoming, making it difficult to fully assess the scope of enforcement actions and the overall effectiveness of Tanzania's data protection implementation. Thus, the lack of direct engagement and enforcement data accessibility presents several concerns:

1. *Transparency Deficits:* Limited publicly available information makes it difficult for businesses, policymakers, and civil society organizations to assess compliance trends and regulatory effectiveness.
2. *Regulatory Oversight and Capacity Gaps:* The absence of clear enforcement reports and compliance statistics raises concerns about whether sanctions and corrective measures are consistently applied and whether the PDPC has sufficient capacity to oversee compliance.
3. *Impact on the Privacy Scorecard:* Due to the lack of direct engagement with the regulator, this assessment relies on publicly available resources, independent research, and sectoral insights. As a result, the Privacy Scorecard may not fully capture Tanzania's latest enforcement trends or compliance rates.

Tanzania has demonstrated commitment to strengthening its data protection regime through regulatory advancements. To further enhance transparency and accountability, the PDPC is encouraged to:

- Establish a publicly accessible register of data controllers and processors to enhance transparency and allow stakeholders to monitor compliance.
- Regularly publish enforcement reports, detailing investigations, compliance trends, and regulatory interventions to reinforce accountability.
- Enhance engagement with stakeholders, including businesses, civil society, and international data protection bodies, to ensure alignment with global privacy standards.
- Expand access to enforcement data, ensuring that businesses and individuals can easily track regulatory actions, penalties, and compliance trends.
- Invest in professional training, such as DPO certification programs, to further enhance compliance capabilities across industries.

Tanzania has made significant progress in strengthening its data protection framework, but sustained efforts in transparency, enforcement reporting, and stakeholder engagement will be key to ensuring the effective implementation of data protection laws. By improving public access to compliance data and fostering open regulatory dialogue, Tanzania can solidify its position as a leader in data privacy governance in the region.

4.3 Data Protection Landscape in Mauritius

Mauritius established a strong legal framework for data protection, with the right to privacy explicitly enshrined in Sections 3 and 9 of the Constitution and Article 22 of the Civil Code.

These provisions are implemented through the Data Protection Act 2017 (DPA), which governs the collection, storage, and processing of personal data. Mirroring the General Data Protection Regulation (GDPR), the DPA mandates that data subjects (individuals whose data is being collected and processed) provide explicit consent before their personal data is handled. Data controllers and processors are also required to inform individuals about the purpose of data collection and where their data is stored.

The DPA 2017 grants data subjects several rights, including: The right to access their personal data.The right to rectify inaccurate information. The right to request data deletion (right to be forgotten). Additionally, the Act differentiates between personal data and special categories of data, imposing stricter regulations on the latter. It also prohibits processing personal data of children under 16 without parental or guardian consent and requires organizations to incorporate child protection measures in their systems. The Act further establishes clear guidelines for cross-border data transfers and mandates the appointment of a Data Protection Officer (DPO), who serves as the first point of contact for both the Data Protection Office and data subjects.

While the Act ensures strong privacy protections, it also allows certain exceptions where restrictions on data processing may be lifted. These include justifications for: National security, defence, or public security; historical, statistical, or scientific research; judicial independence and legal proceedings, crime prevention, investigation, or prosecution; public interest objectives, protection of the rights and freedoms of others.

Complementing the DPA, the Cybersecurity and Cybercrime Act 2021 reinforces data security by protecting digital infrastructure, devices, and stored information from unauthorized access, modification, disruption, or destruction. More recently, the Data Protection Office (DPO) introduced a financial data protection guide, aimed at developing regulations and codes of practice to enhance compliance and implementation of data protection laws.

Additionally, efforts were made to engage with Mauritius' Data Protection Office (DPO) to obtain firsthand insights into key regulatory aspects, including registration processes, enforcement actions, institutional capacity, public engagement, and compliance monitoring. As already noted above, Mauritius has made notable strides in strengthening its data protection framework, through the Data Protection Act, 2017, which aligns with international best practices, including EU GDPR standards. The DPO has demonstrated commendable efforts in sensitization and capacity building, including awareness campaigns and training programs aimed at enhancing compliance. However, despite these positive advancements, direct outreach to obtain specific enforcement data, institutional capacity details, and regulatory effectiveness updates did not yield responses. While Mauritius has demonstrated strong leadership in regulatory awareness and compliance promotion, the lack of publicly available enforcement data and direct engagement challenges make it difficult to fully assess the extent of enforcement actions and regulatory impact.

Particularly;

1. While Mauritius has a robust legal framework, the absence of publicly available information on regulatory investigations, penalties, and compliance rates makes it difficult to assess the full extent of enforcement efforts.

2. Without clear, updated enforcement data, concerns arise about whether penalties and corrective measures are consistently applied and whether the DPO has sufficient resources to effectively monitor compliance.

3. Mauritius has taken proactive steps in awareness campaigns and DPO training, but greater transparency in compliance reporting would further enhance public confidence in regulatory enforcement.

4. Due to the lack of direct engagement with the regulator, this assessment relies on publicly available resources, independent research, and sectoral insights. As a result, the Privacy Scorecard may not fully capture Mauritius' latest enforcement trends or compliance rates.

Mauritius has emerged as a leader in data protection governance in the region, with commendable efforts in public awareness, transparency, and regulatory capacity-building. By enhancing enforcement data accessibility and deepening stakeholder engagement, Mauritius can solidify its position as a model for data protection oversight in Africa and beyond.

4.4 Data Protection Landscape in Zimbabwe

Zimbabwe's digital transformation has accelerated significantly, driven by initiatives such as the Digital Economy Strategy, which aims to enhance digital penetration and promote e-governance. The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) has reported[33] continuous growth in mobile, internet, and fixed telephony subscriptions,[34] as well as increasing internet and data usage.[35]

33 The reports highlights the key trends observed in the Postal and Telecommunication sectors during the third quarter of 2023.
34 A 6.0% increase in mobile subscriptions from the previous quarter.
35 Internet and data usage increased by 6.2 % to reach 44.6 Petabytes.

Investments in digital infrastructure, such as fiber optics, mobile money services (EcoCash, OneMoney, Telecash), and online payment systems (Paynow, Zimswitch, Vpayments), have further facilitated financial inclusion and streamlined digital transactions.[36] The government has also expanded e-government services, including platforms for passport applications, tax payments, and business registrations, reducing the need for physical interactions and improving efficiency and transparency.[37]

However, this rapid digitalization has heightened the risks of privacy violations, particularly given the collection of sensitive personal data such as physical addresses, bank details, and health records. The right to privacy, as enshrined in Article 57 of the Constitution of Zimbabwe, necessitates stringent safeguards to ensure informed consent and secure data handling practices.

The Data Protection Act is Zimbabwe's primary legislation governing data privacy. Enacted in 2021, its primary objective is to enhance data protection by fostering trust in the use of information and communication technologies (ICTs). The Act: Grants data subjects rights, including the right to be informed about how their data is used and processed;[38] differentiates between sensitive and non-sensitive data, requiring stricter consent protocols for processing sensitive data;[39] requires that parents or legal guardians exercise data rights on behalf of minors and legally incapacitated individuals; mandates data controllers to ensure privacy protection, breach notification, and accountability in data handling; and introduces provisions for security breach notifications to strengthen transparency and compliance.

Despite these advancements, criticism remains regarding the Act's lack of clarity in defining key technical terms and its failure to specify enforcement mechanisms. Additionally, the designation of POTRAZ as the Data Protection Authority[40] continues to raise concerns over regulatory independence.

Equally, the Cyber and Data Protection Regulations, 2022, provides detailed procedures for compliance with the Data Protection Act. These regulations include:

Licensing requirements for data processors, with a self-assessment tool to determine eligibility; a register of licensed data controllers, managed by the Data Protection Authority; exemptions for entities processing data for non-profit, household, judicial, or personal purposes; mandatory appointment of data protection officers (DPOs) for non-exempt entities, with DPO certification programs conducted alongside POTRAZ; publication requirements for DPO appointments to ensure transparency; restrictions on health data processing, mandating explicit consent except in emergency or legally authorized situations; and a Code of Conduct governing specific data processing activities.

While these regulations provide structure, they have been criticized for being overly restrictive, potentially stifling innovation and adding compliance burdens on businesses.

Other Relevant Legislation include:

- Electronic Transactions and Electronic Commerce Act (2018): Regulates online transactions, requiring service providers to implement security measures and notify data breaches. However, its limited scope for electronic signatures and the absence of clear digital evidence guidelines remain issues.

- POTRAZ Regulations: Provide data protection guidelines for telecom operators, including data retention rules and breach notification obligations. However, excessive regulation is cited as a barrier to innovation in the telecommunications sector.

- National Cyber Security Policy (2020): Addresses cybersecurity, promotes adherence to international standards, and sets incident response guidelines, though it lacks comprehensive alignment with global best practices.

36 Will ZimSwitch Online unlock Zimbabwe's E-Commerce potential? https://dotzedw.com/will-zimswitch-online-unlock-zimbabwes-e-commerce-potential/ accessed 19 July 2024.
37 An Evaluation of the Importance of E-commerce Adoption to the Growth of SMEs in Zimbabwe http://www.ieomsociety.org/harare2020/papers/556.pdf accessed 19 July 2024

38 Section 14 of the Data Protection Act.
39 Section 11 and Section 10 of the Data Protection Act respectively.
40 Designated under S.5.

Zimbabwe's data protection and cybersecurity efforts are enforced through multiple institutions:

- Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ): Serves as the Data Protection Authority, responsible for enforcing compliance with the Data Protection Act. However, concerns persist about its regulatory independence, given its role in overseeing telecommunications.
- Zimbabwe Information and Communication Technologies (ZICT): Promotes privacy best practices within the ICT sector.
- National Cyber Security Centre: Coordinates national cybersecurity efforts, including data protection.
- Zimbabwe Human Rights Commission (ZHRC): Monitors privacy rights and addresses data-related complaints.
- Zimbabwe Republic Police (ZRP): Investigates cybercrimes such as hacking, identity theft, and fraud.

While these institutions provide a framework for enforcement, resource limitations and overlapping mandates hinder their ability to effectively address privacy violations and cyber threats.

Zimbabwe's evolving data protection landscape reflects both progress and challenges. The Data Protection Act provides a clear legal foundation for data privacy. Businesses and government agencies are increasingly adopting privacy policies in response to legislative requirements. Awareness initiatives, such as public consultations, webinars, and workshops, have enhanced public engagement in data protection matters.

However, the lack of clear enforcement mechanisms makes it difficult to hold violators accountable. The dual role of POTRAZ as both telecom regulator and Data Protection Authority raises concerns over conflicts of interest and regulatory efficiency. Limited resources constrain the capacity of enforcement institutions to implement cybersecurity measures effectively. The absence of clear whistleblower protections weakens accountability for data breaches. Overly restrictive licensing requirements for data controllers may hinder business growth and innovation.

Equally, efforts were made to engage Zimbabwe's data protection regulator, the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ). The aim was to gain insights into key aspects of data protection regulation, including the registration of data controllers and processors, enforcement actions, institutional capacity, public engagement, and compliance monitoring.

Particularly, Zimbabwe has demonstrated notable progress in strengthening its data protection framework, through the enactment of the Data Protection Act, 2021. POTRAZ has actively implemented oversight mechanisms, developed regulatory guidelines, and engaged stakeholders on privacy rights and compliance obligations. The regulator has also undertaken commendable efforts in sensitization and capacity-building, including awareness-raising campaigns and training programs for Data Protection Officers (DPOs). A significant milestone in this regard was Zimbabwe's hosting of the Unwanted Witness 6th Privacy Symposium Africa in Harare, during which several DPOs were trained and certified, enhancing institutional and sectoral capacity in data protection.

However, unlike the case of Kenya and Uganda, Zimbabwe has yet to establish a publicly accessible register of data controllers and processors, which limits transparency and external accountability. Additionally, despite multiple attempts, direct engagement to obtain updates on enforcement actions, institutional capacity, and regulatory effectiveness proved unsuccessful.

Equally, the limited availability of regulatory data presents several challenges:

1. *Transparency and Accessibility Gaps*: The absence of a publicly accessible register makes it difficult for businesses, civil society, and policymakers to assess compliance trends and understand data protection obligations.
2. *Limited Visibility on Enforcement Actions:* While the Data Protection Act, 2021, includes provisions for enforcement and penalties, little information is publicly available on investigations, sanctions, or compliance rates.
3. *Regulatory Oversight and Capacity:* Without access to data on enforcement activities, there are concerns about whether penalties are consistently applied and whether POTRAZ has the necessary resources to uphold data protection standards effectively.
4. *Public Trust and Awareness:* Although POTRAZ has actively conducted sensitization campaigns and professional training, public confidence in data protection enforcement could be further enhanced by greater regulatory transparency.

5. *Impact on the Privacy Scorecard:* Due to the lack of direct input from the regulator, this assessment relies on publicly available sources, independent research, and sectoral insights. As a result, the Privacy Scorecard may not fully capture Zimbabwe's most recent data protection enforcement actions and compliance trends.

Zimbabwe has taken important steps to advance data protection governance, but further transparency and stakeholder engagement are needed to strengthen accountability. To enhance its regulatory framework, POTRAZ is encouraged to:

- *Establish a publicly accessible register of data controllers and processors*, allowing stakeholders to track compliance efforts.
- *Publish regular enforcement reports*, detailing investigations, penalties, and regulatory interventions to promote accountability.
- *Continue and expand stakeholder engagement*, particularly through professional training and public awareness initiatives similar to the 6th Privacy Symposium Africa.
- *Increase accessibility to compliance data*, ensuring that enforcement trends and regulatory actions are regularly communicated to businesses and individuals.

Zimbabwe has made commendable progress, particularly in awareness-raising, professional training, and regulatory implementation. However, sustained efforts in transparency, accountability, and stakeholder engagement will be essential to strengthen trust in the regulatory system and ensure that data protection laws are effectively enforced.

Furthermore, in response to rising cyber threats, privacy violations, and data breaches, Zimbabwe has taken important legislative and institutional steps to strengthen data protection. However, the effectiveness of these measures hinges on robust implementation, clarity in legal provisions, and sufficient funding for enforcement agencies. To fully realize the benefits of its data protection framework, Zimbabwe must: Enhance independence and capacity of regulatory bodies; simplify compliance requirements for businesses while maintaining strong data security standards; strengthen public awareness and education on data protection rights; and ensure continuous improvement of data protection laws to keep pace with emerging technologies. While challenges remain, continued collaboration between government, businesses, civil society, and individuals will be critical in securing personal data and fostering a trustworthy digital environment in Zimbabwe.

4.5 Data Protection Landscape in Kenya

Kenya's rapid digitization of government services has fueled increased data collection across digital platforms. The country has established an emerging data protection and privacy regime composed of the Constitution of Kenya, the Data Protection Act (DPA) and its supporting regulations, as well as sectoral laws and policies that govern data collection and privacy. Before the enactment of the Data Protection Act in 2019, Kenya lacked a specific law dedicated to data protection.

However, Article 31 of the Constitution of Kenya provides for the internationally recognized right to privacy,[41] which includes the right of individuals not to have: their personal or family information unnecessarily required or revealed and the privacy of their communications infringed upon.

Kenyan courts have upheld this right in various landmark cases, including *Rukia Idris Barri v Mada Hotels Ltd*,[42] which emphasized personality rights, and *Okiya Omtatah Okoiti v Communications Authority of Kenya & Others*,[43] where the court declared a government surveillance system unconstitutional for violating privacy rights.[44]

The Data Protection Act (DPA) is Kenya's primary legal framework for data protection, enacted in 2019 and came into effect in 2020. It aligns with international best practices, such as the EU General Data Protection Regulation (GDPR).[45]

41 See, e.g., Universal Declaration of Human Rights Article 12; United Nations Convention on Migrant Workers Article 14; U.N. Convention of the Protection of the Child Article 16; International Covenant on Civil and Political Rights Article 17; Article 10 of the African Charter on the Rights and Welfare of the Child; Article 4 of the African Union Principles on Freedom of Expression.
42 Rukia Idris Barri v Mada Hotels Ltd[2013] eKLR.
43 Okiya Omtatah Okoiti versus Communication Authority of Kenya and others ,Constitutional Petition no.53 of 2017; [2018] eKLR
44 Ibid.
45 Article 5 and Section 25.

The Act establishes:

- The Office of the Data Protection Commissioner (ODPC) as the regulatory body.
- Registration requirements for data controllers and processors.
- Principles of data protection, including lawfulness, fairness, transparency, data minimization, security, and accountability.
- Rights of data subjects, including: the right to be informed about data processing, the right to access, correct, and delete personal data, the right to object to data processing, the right to data portability.[46]
- Regulations on cross-border data transfers, ensuring data sent outside Kenya meets equivalent protection standards.[47]
- Legal provisions for penal sanctions and fines for non-compliance.

Despite its comprehensive nature, challenges persist in its enforcement, compliance, and the need for further regulatory clarity.

Equally, the Access to Information Act,[48] enacted pursuant to Article 35 of the Constitution, grants citizens the right to access their personal data, subject to certain limitations related to national security and legal compliance.

It mandates public and private entities to disclose information, enhancing transparency and accountability.

Furthermore, the Computer Misuse and Cybercrimes Act[49] addresses cyber-related offenses, including unauthorized access, identity theft, impersonation, fraudulent use of electronic data, and unlawful disclosure of passwords or access codes. While not solely focused on data protection, it safeguards personal data from cyber threats.

Additionally, Kenya Information and Communications Act (KICA)[50] is the primary statute governing telecommunications and digital communications. It mandates the Communications Authority of Kenya (CA) to regulate the sector[51] and ensure compliance with privacy laws. Key provisions include: Section 27 empowers the minister to make privacy-related regulations; Section 31 prohibits interception of private communications; Section 46 protects the right to privacy in broadcasting services and Regulation 3 (2010 Consumer Protection Regulations) guarantees consumers' right to privacy.

Other Sectoral Laws contributing to data protection include:

- The National Security Intelligence Service Act[52] – Requires judicial oversight for surveillance activities.[53]
- The Public Health Act, [54] Health Act,[55] and HIV/AIDS Prevention and Control Act[56] – Regulate medical data processing.
- The Central Bank of Kenya Act and Prudential Guidelines[57] – Protect financial data privacy.
- The National Payment System Act[58] and Consumer Protection Act[59] – Safeguard consumer data across various sectors.

46 Section 23.
47 Section 48, section 49.
48 Act No. 31 of 2016, Laws of Kenya.
49 Act No.5 of 2018, Laws of Kenya.
50 Chapter 411A, Laws of Kenya.
51 Part 2 of the Kenya Information and Communications Act amended by the Kenya Information and Communications (Amendment) Act, 2013.
52 Chapter 205, Laws of Kenya.
53 Section 22 of the National Security Intelligence Service Act.
54 Chapter 242, Laws of Kenya.
55 Act No.21 of 2017, Laws of Kenya.
56 Act No 14 of 2006, Laws of Kenya.
57 Chapter 491, Laws of Kenya.
58 Act No 39 of 2011, Laws of Kenya.
59 Act No 46 of 2012, Laws of Kenya.

Institutionally the ODPC is the government agency responsible for enforcing the Data Protection Act. Established in 2019,[60] it operates under the Ministry of ICT, Innovation, and Youth Affairs. The ODPC's core functions include: Regulating and enforcing compliance with data protection laws; maintaining a register of data controllers and processors; investigating complaints and conducting data protection impact assessments; educating the public on data privacy rights; and issuing penalties and administrative fines for non-compliance.

The Communications Authority of Kenya (CA) oversees the telecommunications sector and enforces compliance with KICA and sector-specific data protection regulations. It ensures: Protection of consumer privacy, compliance with the National ICT Policy Guidelines, 2020 and secure telecommunications infrastructure to safeguard data privacy.

The Central Bank of Kenya (CBK) regulates financial data protection, ensuring: Banks comply with consumer data protection guidelines, payment service providers follow cybersecurity measures and risk assessments cover customer privacy risks.

The Digital Health Agency (DHA), under the Digital Health Act,[61] manages health data protection. It: Oversees health information systems and data exchange frameworks; ensures secure collection and processing of health data and promotes interoperability of health data systems.[62]

While the DHA's role complements the ODPC, concerns have arisen about potential overlaps in regulatory authority.

As part of this assessment, efforts were made to engage Kenya's data protection regulator, the ODPC. The goal was to obtain firsthand insights into key regulatory aspects, including registration, enforcement actions, institutional capacity, public engagement, and monitoring efforts. However, direct outreach to obtain specific data and detailed status updates on enforcement and monitoring efforts proved unsuccessful. This notwithstanding, Kenya has made notable strides in advancing its data protection framework comprising the Data Protection Act and supporting regulations, sectoral regulations ensuring compliance across telecommunications, finance, and health sectors; and independent regulatory authority (ODPC) to enforce data protection laws. Additionally, the ODPC has demonstrated proactive engagement through public awareness initiatives, enforcement actions, and regulatory guidance. The ODPC equally, should be commended for maintaining a publicly accessible register of data controllers and processors, which enhances transparency and allows stakeholders to track compliance.

However, at the same time there key challenges in form of weak enforcement due to resource constraints within the ODPC; gaps in regulatory clarity, particularly regarding cross-border data transfers and exemptions; non-compliance by public and private entities, slowing the Act's full realization; and concerns over surveillance practices, with some government initiatives potentially infringing on privacy rights. Moreover, the lack of direct responses from the ODPC made it difficult to assess the full scope of enforcement effectiveness and implementation progress.

Furthermore, the absence of direct input from the ODPC on enforcement actions and institutional capacity raises several concerns:

1. *Limited Access to Enforcement Data* - While Kenya's ODPC has taken enforcement actions, including issuing compliance notices and penalties, detailed information on case resolutions and regulatory priorities remains limited. A more structured and consistent reporting mechanism could enhance confidence in enforcement efforts.

2. *Regulatory Oversight Gaps* - Without clear and updated enforcement data, there are concerns about whether penalties and corrective actions are being applied consistently and whether the ODPC has the necessary resources and capacity to effectively uphold Kenya's Data Protection Act, 2019.

3. *Public Trust and Awareness:* While Kenya has made efforts in public education, greater accessibility to enforcement data would further strengthen public trust in the ODPC's ability to safeguard data privacy rights and provide effective recourse mechanisms.

4. *Impact on the Privacy Scorecard:* Due to the lack of direct engagement with the regulator, this assessment relied on publicly available sources, independent research, and sectoral insights. As a result, the privacy scorecard may not fully capture the latest enforcement trends or compliance levels in Kenya.

60 Section 5(1) Data Protection Act.
61 Section 5.
62 David Indeje, Kenya's Digital Health Act: A Leap Forward in Data Governance, KICTANET, October 24, 2023, <https://www.kictanet.or.ke/kenyas-digital-health-act-a-leap-forward-in-data-governance> (accessed August 10, 2023).

Kenya has set a strong foundation in data protection, particularly in transparency through its public register and active awareness campaigns. To further enhance regulatory trust and effectiveness, the ODPC is encouraged to:

- *Expand the publication of enforcement reports*, including details on investigations, compliance trends, and sanctions imposed.
- *Engage more openly with stakeholders*, including businesses, civil society, and the public, to provide clarity on regulatory expectations and enforcement priorities.
- *Enhance accessibility of compliance data*, ensuring businesses and individuals can easily track enforcement actions and emerging regulatory developments.

Kenya's leadership in data protection within the region is commendable, but sustained efforts in transparency, accountability, and proactive stakeholder engagement will be essential to strengthening enforcement and public confidence in the regulatory framework.

4.6 Data Protection Landscape in Uganda

Despite having a predominantly young population, Uganda lags in technological advancement. The country's internet penetration rate stands at 43%, hindered by limited infrastructure and disparities in skills, innovation, and inclusiveness.[63] While Uganda performs well in digital policy and regulation, awareness of data privacy rights and access to enforcement mechanisms remain low.

The Right to Privacy is a Constitutional guaratee in Article 27, prohibiting interference with a person's home, correspondences, communication, or property.

To uphold this right, Uganda enacted the Data Protection and Privacy Act (DPPA) in 2019, operationalized by the Data Protection and Privacy Regulations, 2021. Data Protection and Privacy Act (DPPA), 2019 codifies key principles of lawful and fair data collection, storage limitations, data security, and restrictions on cross-border data transfers. Particularly, Section 7(1) prohibits the collection or processing of personal data without prior consent;[64] Section 3 requires data to be processed transparently and securely while, Regulations, 2021establish standard forms for filing complaints, objecting to data collection, and reporting security breaches.[65]

Other sector-specific laws supporting data protection include:[66]

- The Access to Information Act, 2005 governs data access and disclosure.
- The Regulation of Interception of Communications Act, 2010 regulates government surveillance.
- The Computer Misuse Act, 2011 (as amended) criminalizes cyber offenses such as unauthorized access and identity theft.
- The Registration of Persons Act, 2015 mandates digital identification and personal data collection.

Institutionally National Information Technology Authority - Uganda (NITA-U), established under the NITA-U Act, 2009, is the designated national data protection authority. The DPPA further established the Personal Data Protection Office (PDPO) under NITA-U to oversee compliance and enforcement.[67]

Functions of NITA-U and the PDPO include; ensuring compliance with the DPPA by data controllers and processors, investigating data breaches and determining necessary actions, maintaining a national register of data processors and controllers, and conducting public awareness campaigns to educate citizens on data rights.[68]

63 https://www.undp.org/uganda/blog/ugandas-digital-transformation-journey.
64 In this case of Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746 Personal data was defined as the name of a person or identification of him by some other means, for instance by giving his telephone number or information regarding his working conditions or hobbies. This case elaborately defines personal data as a foundation to data privacy and protection.
65 Regulation 10(5), Regulation 32(3) and Regulation 39(3) of the Data Protection and Privacy Regulations, 2021.
66 https://www.dlapiperdataprotection.com/index.html?t=law&c=UG.
67 Section 4 of the Data Protection and Privacy Act, 2019.
68 https://www.dataguidance.com/notes/uganda-data-protection-overview

Notwithstanding its mandate, as part of this assessment, efforts were made to engage with Uganda's national data protection regulator - the National Information Technology Authority - Uganda (NITA-U) and its Personal Data Protection Office (PDPO), to obtain firsthand information on key areas such as registration, enforcement actions, institutional capacity, regulatory frameworks, public engagement, and monitoring efforts.

NITA-U faces significant challenges and gaps in enforcement.

- Regulatory Independence Concerns: The PDPO operates under NITA-U, a government agency, raising concerns about potential political influence in enforcement decisions. A more independent regulatory body would strengthen oversight and accountability.

- Resource Constraints: NITA-U faces financial and staffing limitations, which may affect its ability to conduct proactive audits, investigations, and risk-based monitoring of data controllers and processors.

- Lack of clarity on withdrawal of consent – The DPPA does not clearly define how a data subject may withdraw consent, limiting individuals' control over their data.

Notwithstanding the above challenges, there have been efforts toward data protection and public Awareness which are highlighted below:

Government Initiatives in the form of Data Protection and Privacy 2024 Campaign that was launched by the Ministry of ICT and National Guidance under the slogan, *"Stop, Think, Own Your Privacy"*, to promote responsible personal data use.[69] As well as Digital ID System Oversight where in March 2023, the High Court allowed civil society intervention in a case against the National Identification Registration Authority (NIRA), emphasizing the human rights implications of biometric data collection.

Landmark legal cases pertaining to *SafeBoda Data Breach Investigation (2023)* where NITA-U ruled that SafeBoda unlawfully shared users' personal data, marking a precedent for enforcing privacy laws.[70] As well as Access Now & ARTICLE 19 v. Ugandan Government (2023) where civil society organizations challenged the mandatory biometric digital ID system, advocating for better privacy safeguards.[71]

Further more, civil society particularly CIPESA, Unwanted Witness, and ARTICLE 19 played a crucial oversight role in the year under review by advocating for stronger policies and transparency in data protection, raising awareness of digital privacy rights among Ugandans and challenging government surveillance programs that infringe on privacy.

Overall, Uganda exhibits, a progressive legal framework with the DPPA and supporting regulations; growing awareness campaigns by both government and civil society organizations and judicial recognition of digital rights through court rulings. However, challenges remain in the form of weak enforcement mechanisms, limiting the effectiveness of privacy protections; insufficient funding for NITA-U, hindering comprehensive oversight; political interference, affecting the autonomy of the data protection authority; and low digital literacy, reducing citizens' ability to assert their rights.

Uganda has laid a strong legal foundation for data protection, but implementation gaps remain. To enhance privacy protections, Uganda must:

- Strengthen NITA-U's independence to minimize external influences.

- Increase funding and technical capacity for effective enforcement.

- Expand public education programs to improve digital literacy on data rights.

- Align national laws with international best practices, including ratification of the African Union Convention on Cyber Security and Personal Data Protection.

By addressing these challenges, Uganda can bridge the gap between policy and practice, ensuring that the right to privacy is effectively upheld in its evolving digital landscape.

69 https://infrastructure.go.ug/2024-data-protection-campaign-launched-by-the-ministry-of-ict-to-protect-individual-privacy/
70 https://www.dataguidance.com/notes/uganda-data-protection-overview
71https://www.accessnow.org/press-release/uganda-digital-identity-system-human-rights-warnings/?utm_source=perplexity

5. RECOMMENDATIONS

Based on the findings of this report, it is evident that while significant progress has been made in privacy and data protection across various jurisdictions, particularly Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya and Uganda; critical gaps remain in legal frameworks, institutional oversight, enforcement mechanisms, and public awareness. To address these challenges and strengthen data governance, the following recommendations are proposed. These recommendations are categorized according to key stakeholders, ensuring that each entity involved in data protection plays its role in fostering a secure and privacy-conscious digital ecosystem.

The recommendations focus on:

- Governments enhancing legal and regulatory frameworks, ensuring financial and operational autonomy for data protection authorities, and aligning national laws with international best practices.
- Policy Makers benchmarking against international best practices, clarifying legal penalties, and facilitating international cooperation.
- National Regulators (DPOs, NCSAs) strengthening enforcement through compliance audits, developing clear regulations, and expanding public awareness campaigns.
- Data Controllers and Processors (Businesses and Tech Providers) implementing robust compliance measures, publishing transparency reports, and appointing data protection officers.
- Data Subjects (Individuals) exercising privacy rights, staying informed about personal data protection, and holding businesses accountable.
- Civil Society Organizations (CSOs) and Media advocating for stronger privacy protections, monitoring and reporting violations, and promoting digital security tools.
- Technical Community providing expert insights in policy development, innovating privacy-enhancing technologies, and conducting cybersecurity training.

Specific, actionable steps that each of these key stakeholders can take to enhance data protection and privacy are outlined below;

Recommendations for Governments

1. *Ensure Financial and Operational Autonomy* - Establish independent data protection offices (DPOs) with adequate financial resources to function effectively and impartially.
2. *Strengthen Legal Frameworks* - Amend data protection laws to provide clear guidelines on audits, data retention, and breach notification procedures aligned with international best practices (e.g., GDPR, Malabo Convention).
3. *Enhance Oversight of Surveillance Practices* - Implement strict judicial oversight for government surveillance and ensure transparency in surveillance programs.
4. *Ratify International Data Protection Treaties* - Countries like Tanzania should sign and ratify the African Union Convention on Cyber Security and Personal Data Protection to strengthen their commitment to privacy.

Recommendations for Policy Makers

1. *Benchmark Against Global Best Practices* - Align national data protection laws with international standards such as GDPR and OECD privacy guidelines.
2. Clarify Penalty Provisions - Ensure data protection laws specify clear penalties (e.g., percentage-based fines) to enhance enforcement without discouraging investment.
3. *Facilitate International Cooperation* - Promote cross-border collaboration on data protection to address global challenges in data governance.

Recommendations for Data Protection Regulators

1. *Develop and Enforce Regulations* -Address legal gaps by introducing regulations on dispute resolution, appellate procedures, and mandatory transparency reporting.
2. *Expand Public Awareness Campaigns* - Conduct large-scale sensitization initiatives targeting schools, businesses, and rural communities to educate citizens about their data rights.
3. *Establish a Digital Register* - Maintain a public registry of compliant data controllers and processors for easy verification by businesses and consumers.
4. *Conduct Random Compliance Audits* - Implement periodic audits to ensure organizations adhere to data protection laws and ethical data governance practices.

Recommendations for Data Controllers and Processors (Businesses and Tech Providers)

1. *Enhance Compliance Measures* - Adopt strong data security measures and publish annual transparency reports to demonstrate commitment to privacy.
2. *Implement Data Minimization Practices* - Limit data collection to only what is necessary and ensure secure storage and timely disposal.
3. *Appoint Data Protection Officers* - Mandate internal DPOs to oversee compliance with legal requirements and ethical data governance.
4. *Establish Breach Notification Procedures* - Report data breaches promptly to the regulatory authority and affected individuals.

Recommendations for Data Subjects (Individuals)

1. *Exercise Privacy Rights* - Utilize legal channels to report non-compliance and enforce privacy rights through complaints to data protection authorities or legal action.
2. *Stay Informed* - Educate themselves on personal data rights and best practices for protecting their information online.
3. *Demand Transparency*- Hold businesses and service providers accountable by requesting information on how their data is collected, stored, and used.

Recommendations for Civil Society and the Media

1. *Advocate for Stronger Privacy Protections* - Lobby for amendments in data protection laws to include enhanced rights for data subjects, such as the right to be forgotten and algorithmic accountability.
2. *Monitor and Report Violations* - Investigate and document privacy breaches and raise awareness through media campaigns.
3. Promote Digital Security Tools - Encourage the use of encryption, anonymization, and circumvention tools to enhance personal data security.

Recommendations for the Technical Community

1. *Provide Technical Expertise in Policy Development* - Offer insights on the impact of emerging technologies on data privacy to guide lawmaking.
2. *Develop Privacy-Enhancing Technologies* - Innovate tools that help individuals control their data and enhance security.
3. *Conduct Cybersecurity Training* - Equip businesses and individuals with skills to safeguard personal data against cyber threats.

By implementing these recommendations, stakeholders across different sectors can contribute to a more secure and privacy-conscious digital ecosystem, fostering trust, compliance, and sustainable innovation in data governance.

6. CONCLUSION

The evolving digital landscape across East Africa and beyond underscores the critical need for robust data protection and privacy frameworks. While countries like Kenya, Rwanda, Tanzania, Mauritius, and Zimbabwe have made significant progress in establishing legal and institutional mechanisms to safeguard personal data, challenges remain in enforcement, compliance, and public awareness.

Kenya, despite being a leader in the region's digital economy, continues to grapple with regulatory gaps, non-compliance, and weak enforcement of its Data Protection Act. The rise of emerging technologies such as Artificial Intelligence (AI), blockchain, and the Internet of Things (IoT) necessitates stronger regulatory oversight, aligning with international best practices, including the GDPR and the African Union Convention on Cyber Security and Personal Data Protection.

For Rwanda, ethical data governance is paramount in its rapidly digitalizing economy. Ensuring that privacy, dignity, and autonomy are upheld requires the active participation of government, the private sector, civil society, and citizens. This report has evaluated Rwanda's Data Privacy and Protection Law, identifying both strengths and areas for improvement, particularly in compliance and enforcement across different sectors.

Tanzania has demonstrated a commitment to data privacy through its Personal Data Protection and Privacy Act, but challenges in its legal and institutional frameworks hinder full implementation. Strengthening these frameworks by incorporating international legal obligations, particularly through the Malabo Convention, would enhance Tanzania's data protection regime.

Mauritius has taken commendable steps in aligning its Data Protection Act (DPA) 2017 with international standards, but translating this framework into effective protections remains a challenge. Inconsistencies in data collection, lack of transparency, and insufficient public awareness have impeded progress. To address these gaps, Mauritius must focus on legislative refinements, institutional strengthening, enforcement mechanisms, and public education. A comprehensive data breach response framework and active engagement in global data protection forums would further solidify its position as a regional leader in data protection.

Zimbabwe's Data Protection Act, though relatively new, has introduced significant measures to protect data subjects. There is an increasing recognition of data privacy rights across various sectors, with businesses and government agencies adopting privacy policies. However, challenges persist, including the lack of transparency reports and weak internal data breach resolution mechanisms. Strengthening compliance frameworks and promoting greater accountability are essential to fostering a more secure digital ecosystem.

As digital economies continue to expand, cross-stakeholder collaboration is essential to ensuring that data protection is not just a legal requirement but a practical reality. Governments must strengthen regulatory oversight, businesses must prioritize compliance and transparency, and civil society must demand accountability and advocate for user rights.

The protection of personal data is not just a legal obligation but a fundamental human right. Countries in the region have the opportunity to enhance digital trust, drive innovation, and foster economic growth by continuously refining their data protection laws and enforcement mechanisms. Moving forward, sustained efforts in policy development, international cooperation, and public engagement will be crucial in shaping a secure and privacy-conscious digital future.

Privacy Scorecard Report 2024

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