



— PRIVACY SCORECARD REPORT

If You Must Collect It, You Must Protect It

NOV 2025

www.unwantedwitness.org



Written and Compiled by:



Nigeria, Ghana, Botswana,
Rwanda, Tanzania,
Mauritius, Zimbabwe,
Kenya, Uganda



PRIVACY SCORECARD REPORT/2025

If You Must Collect It, You Must Protect It

Nov 2025



**UNWANTED
WITNESS**

"Amplifying Voices, Changing lives"

The Unwanted Witness

Bulange Mengo, Block 381, Plot 26, Nsibambi Village, Sentema Road, P.O.BOX 71314 Clock Tower Kampala – Uganda

Mob: +256-414 697635 Email: info@unwantedwitness.org

Website: unwantedwitness.org

Contents

List of Acronyms	5
List of Respondents Companies	7
About Unwanted Witness.....	11
Acknowledgements	12
Executive Summary.....	13
1. Introduction.....	20
2. Methodology and Criteria.....	22
3. Findings	27
3.1 Overview of the General Compliance Landscape	27
3.1.1 Overall analysis of findings at Country and Sector Level	27
3.2 Highlights of trends/patterns observed across countries, sectors and assessed companies / entities overtime	30
3.3 Overall Assessment of the most used Apps in the countries	82
3.4 Sector-Wise Analysis	130
3.4.1 Country Findings for Telecommunications Sector	130
3.4.2 Country Findings for e -Commerce Sector	151
3.4.3 Country Findings for Online Betting Sector	181
3.4.4 Country Findings for Banks and Finance Sector	208
3.4.5 Country Findings for Insurance Sector	233
3.4.6 Country Findings for e-Government Sector	262
3.4.7 Country Findings for Health Sector	297
3.4.8 Country Findings for Digital Loans Services Sector	325
4. Comparative Review of Data Protection Regimes in Assessed African Countries	359
5. Insights into Challenges, Lessons learned and Best Practices	415
6. Recommendations	427
7. Conclusion	432

Acronyms

%	Percentage
₦	Nigeria Naira
AI	Artificial Intelligence
APC	Association for Progressive Communications
Apps	Applications
AU	African Union
BVNs	Bank Verification Numbers
CCTV	Closed-Circuit Television
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
Co.	Company
CSO	Civil Society Organisations
DCPMIs	Data Controllers and Processors of Major Importance
DPA	Data Protection Act
DPC	Data Protection Commission
DPIs	Data Protection Impact Assessments (corrected to DPIAs below)
DPIAs	Data Protection Impact Assessments
DPPO	Data Protection and Privacy Office
DPO	Data Protection Office
DPO	Data Protection Officer
EAC	East African Community
ECOWAS	Economic Community of West African States
EU	European Union
EU GDPR	The European Union's General Data Protection Regulation
Gov	Government
GPA	Global Privacy Assembly
HIPAA	Health Insurance Portability and Accountability Act
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IDPC	The Information and Data Protection Commission
IECMS	Integrated Electronic Case Management System
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
Ltd	Limited
NADPA	Network of African Data Protection Authorities
NCSA	National Cyber Security Authority
NDPC	Nigeria Data Protection Commission
NDPR	Nigeria Data Protection Regulation
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 the Protection of Privacy and Transborder 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
SADC	Southern African Development Community
SMEs	Small and Medium-sized Enterprises
UW	Unwanted Witness Uganda
ZEC	Zimbabwe Electoral Commission

Respondent Companies

Nigerian Companies

MTN Nigeria
Airtel Nigeria
Globacom Limited
9Mobile
GT Bank (GTCO)
Zenith Bank
UBA Nigeria
Access Bank Nigeria
Mutual Benefits Assurance
Allco Insurance
Leadway Assurance
Sovereign Trust Insurance
Bet9ja
Betway Nigeria
Bet365
Access bet
Jiji Nigeria
Konga
Jumia Nigeria
Kara Nigeria
Nigeria Immigration Service
Independent National Electoral Commission
Federal Inland Revenue Service
Nigeria Customs Service
Lagoon Hospital
Avon Medical
St. Nicholas Hospital
St. Catherine's Specialist Hospital
Ren Money
Branch Nigeria
Fair Money Nigeria
Cabon Nigeria

Botswana Companies

Mascow
Orange
BTC
BoFiNet
Sunbet Botswana
PstBet Botswana
SportPesa Botswana
Bet Xplosion
Botswana Life Insurance
Metropolitan Botswana

Ghanaian Companies

AT Ghana
MTN
Telecel
Glomobile
BetPawa
Betway
1xBet
Soccabet
Eco Bank
GCB
Stanbic
Absa
GRA
Passport Office
SSNIT
Immigration Services
Korle - BU
Komfo Anokye
Nyaho
Trust
Fido
M - Kopa
Izwe
CodisPay
Jumia
Tonaton
Melcom
Kikuu
Enterprise
Star
Hollard
Vanguard

Your Mart
Ubuy Botswana
iStore Botswana
Apex Mart
First National Bank
Absa Botswana
Stanbic Bank Botswana
Standard Chartered Bank
Botswana Unified Revenue Service
Botswana Communications Regulatory

Authority (BCRA)
Hollard
Botswana Insurance Company
tswana
Gaborone Private Hospital
Sidilega Private Hospital
Diagnofirm Medical Laboratories
Sir Ketumile Masire Teaching Hospital

Rwandan Companies

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
Standard Life Rwanda

Mauritius Companies

Emtel Limited
Liquid Telecom
MyT
AtComm
Bank of Baroda
SBM Bank (Mauritius) Limited
Swan Life Limited

1Gov e –Services Portal
Independent Electoral Commission of Bo-

Pachi Micro Solutions
Letshego
Bayport Bostwana
Express Credit Bostwana

Tanzanian Companies

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

Zimbabwean Companies

Econet
TelOne
NetOne
Liquid Telecom Zimbabwe
Stanbic Bank Zimbabwe
NMB Bank
CBZ Bank

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
 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

Empower Bank
 Ubuy Zimbabwe
 Shumba Africa
 Raines Africa
 Tengai Online
 Mrbet
 Pinnacle Sports
 Africabet
 Bezbets
 Ecocash
 Zibuko
 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

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

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 become a leading voice in advocating for internet freedoms, and digital rights, particularly the right to privacy, digital identity, digital inclusion, and freedom of expression.

The organization aims to create a safe and secure digital environment for citizens and promote the responsible use of technology. It aims to empower citizens to use technology in a safe, secure, and effective manner while holding public and private entities accountable for digital rights violations. UW achieves its mission through research, advocacy, and capacity building. UW conducts research to identify digital rights violations, trends, and threats and uses this information to advocate for policy and legal reforms. The organization also provides digital security training and support to human rights defenders, journalists, and vulnerable groups to help them protect themselves online.

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

Vision

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) is profoundly grateful to the essential civil society organizations that have bolstered its efforts and championed its mission. We are particularly thankful for the generous financial support from our development partners, whose funding and technical expertise have been pivotal in enabling the successful annual release of this report.

UW extends special thanks to its Research and Advocacy Unit, highlighting the outstanding work of Ms. Freda Nalumansi and the research team: Mr. Brian Kiira, Ms. Saphirah Kubakurungi, Mr. Harry Mwesigwa, Mr. Nuwe Ahereza Marvin, Ms. Sulel Mercy and Mr. David Kasibante. We also convey our sincere appreciation to the editorial board led by the Executive Director Ms. Dorothy Mukasa, Head of Programmes Mr. Allan Sempala Kigozi, Research and Advocacy Lead Ms. Freda Nalumansi, and IT Manager Mr. John Kauta for their invaluable guidance, including the creation of data collection tools and technical analysis featured in the report. The contributions of other staff members who supported the report's production are also gratefully acknowledged.

Finally, UW thanks the many individuals and organizations that enriched the development process. We are especially appreciative of Price Media for their exceptional graphics and layout expertise, which elevated the report's professional presentation, and for their insightful input during the development and review phases.

Executive Summary

Entering its 5th year, the Unwanted Witness Privacy Scorecard Report marks another milestone in tracking how organisations across public and private sectors safeguard personal data and adhere to data protection obligations. Drawing on local data protection frameworks and global privacy standards, this report examines compliance, highlights progress and uncovers persistent gaps that continue to shape the privacy landscape.

The **2025 assessment** expanded its scope to include **Nigeria, Ghana, and Botswana**, alongside Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda. In total, **286 companies** were assessed, reflecting a 33.56% growth from the 190 recorded in 2024. Participation has risen steadily from 32 companies in one country (2021) to 12 across two countries (2022), 48 across four countries (2023), and 190 across six countries (2024). This growth reflects broader regional coverage and deeper engagement across sectors. The 2025 report builds on previous assessments of data protection and privacy compliance, highlighting the region's evolving digital landscape and growing focus on personal data security, regulatory enforcement, and digital trust.

This assessment adopts a detailed and methodologically sound approach to evaluate data collectors' performance across eight (8) key sectors: telecommunications, e-commerce, online betting, banking and finance, insurance, government agencies/bodies, health, and digital loans. The report examines the extent of compliance with data protection laws, drawing attention to emerging performance trends, sectoral challenges, and best practices. The evaluation is guided by seven (7) key indicators: Registration with the National Regulator, Accessible Privacy Policy, Pre-collection Data Transparency (Data Subject Rights), Third-Party Data Transfer, Robust Data Security Practices, Availability of Transparency Report, and Internal Data Breach Resolution.

The evaluation is structured around several key components: a contextual overview of data protection laws, institutional frameworks, and their enforcement; an in-depth country analysis providing sectoral performance insights drawn from a study of 286 companies and entities; an examination of key compliance indicators; and a discussion of challenges, emerging trends, and lessons learned across different jurisdictions. The report also offers actionable recommendations aimed at strengthening privacy protections.

The study assesses how public and private sector entities manage personal data, revealing persistent gaps in enforcement, regulatory capacity, and public awareness. Although digital services including mobile money, ride-hailing apps, e-commerce, and digital lending platforms continue to expand rapidly, concerns remain around data breaches, unauthorized surveillance, and weak enforcement mechanisms that undermine data protection efforts.

Comprehensive data protection laws are now in force across Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya and Uganda. Among the most recent legislative developments are Zimbabwe (2021), Rwanda and Tanzania (2022), Nigeria (2023), and Botswana (2025), reflecting a broader regional commitment to aligning with global privacy standards and strengthening regulatory oversight of digital ecosystems.

However, despite this important normative progress, implementation remains uneven. Many regulatory authorities are still developing institutional capacity, enforcement mechanisms are maturing, and organisations are at varying stages of compliance. Consequently, the existence of updated legal frameworks does not automatically ensure consistent enforcement or effective protection in practice, particularly where accountability structures, compliance culture and accessible redress mechanisms are still evolving.

Compared to last year's **overall index score** of 40%, the 2025 assessment recorded a slightly high score of **46%**. Kenya maintained its position as the top-performing country, followed by Nigeria, Uganda, and Mauritius. Ghana and Botswana shared the same score, as did Rwanda and Tanzania, while Zimbabwe ranked lowest overall.

At the **sectoral level**, the Banking and Finance sector continued to lead with an overall score of **52%**, up from 42% last year. This was followed by Telecommunications at 46% (up from 39%), Insurance at 44% (up from 40%), and E-commerce, which remained steady at 39%. Digital Loans scored 37%, followed by Online Betting at 36%, Government Agencies at 25%, and finally, the Health sector at 22%.

This year's results demonstrate steady progress in most sectors, with notable improvements in financial and telecommunications services, though overall performance indicates continued challenges in strengthening data protection practices across all industries.

Across the sectors evaluated, the assessment provides a clear picture of how companies and entities are managing privacy and compliance responsibilities. In the telecommunications sector, Airtel Kenya led with a privacy score of 76%, followed by Vodacom Tanzania (74%) and MTN Uganda (70%), both showing notable improvements from last year. Other strong performers included MTN Nigeria (68%), MTN Rwanda (63%), Zuku (60%), 9Mobile (58%), Lycamobile (57%), and Emtel (56%), reflecting steady progress in privacy compliance and user data protection.

Mid-level performers such as Airtel Nigeria (53%) and Safaricom (51%) demonstrated moderate compliance but need to strengthen transparency and user rights protections. In contrast, low performers including Liquid Telecom Zimbabwe (29%), TelOne (27%), Econet Zimbabwe, Glomobile Ghana (25%), and Atcomm (5%), face significant privacy and regulatory risks due to weak data protection measures. Overall, high-scoring firms enjoy stronger consumer trust, lower regulatory exposure, and greater resilience to data breaches, while low-scoring entities risk legal penalties, reputational damage, and customer attrition. The results underscore the uneven maturity of privacy practices across the region and highlight the urgent need for stronger enforcement and organizational accountability in the telecommunications sector.

In the e-commerce sector, Jumia Uganda (63%, up from 40%) and Glovo Kenya (60%) lead in data protection, reflecting significant progress in strengthening privacy and compliance frameworks. They are followed by Jiji Uganda (58%, up from 47%), Jiji Kenya (55%), and Jiji Nigeria (54%), indicating steady improvements across the Jiji group. iStore Botswana (51%) and Jiji Kenya (50%) show moderate adherence to privacy standards, though without notable advancement. Mid-range performers such as Jumia Kenya (44%, down from 47%), Temu Mauritius (44%), and Worths Mauritius Online (42%, down from 46%) exhibit partial implementation of privacy measures but still face gaps in transparency and user data management. At the lower end, Kikuu Ghana (29%), Kara Nigeria (27%), Kikuu Uganda (26%), Vubavuba Rwanda (22%), and Apex Mart (7%) show limited compliance with data protection principles, exposing users to higher privacy risks. Overall, the results reveal a widening gap in privacy maturity within the e-commerce sector. While leading companies demonstrate growing commitment to data protection, many others lag behind, highlighting the need for stronger regulatory enforcement, better governance, and greater investment in privacy management systems.

The online betting sector exhibited significant variation in privacy and data protection performance. Betway Ghana (53%) and Betika Kenya (52%, up from 35%) led the sector, followed by 22Bet Uganda (47%), 1xBet Ghana (47%), and BetPawa Kenya (46%). These improvements indicate growing investment in compliance frameworks and greater attention to user data governance. Mid-tier performers such as Gorilla Games (43%), Fortbet Rwanda, and BetPawa Rwanda (42%) demonstrate moderate progress but continue to face challenges in implementing transparent consent mechanisms and comprehensive privacy controls.

At the lower end, AccessBet (28%), 1xBet Uganda (26%), Steven Hills Mauritius (6%), Totelepepe (6%), and Bet Xplosion Botswana (6%) reflect limited adherence to data protection standards. Such scores suggest weak privacy governance and elevated risks in handling personal and financial data. Overall, the sector shows gradual progress among leading operators but remains constrained by inconsistent compliance maturity, underscoring the need for enhanced regulatory oversight and strengthened internal privacy management systems.

The banking and finance sector showed mixed performance in privacy and data protection. UBA Nigeria (73%) led the sector, followed by NMB Tanzania (68%, up from 36%), Equity Bank Tanzania (67%), Equity Bank Rwanda (66%), and Zenith Nigeria (66%), reflecting strengthened data governance and growing compliance maturity. Mid-range performers such as Ecobank Ghana (58%), Centenary Bank Uganda (57%), Absa Bank Kenya (57%, up from 46%), and CBZ Bank (57%) show steady progress but still face gaps in transparency, consent management, and third-party oversight. Lower scores for Absa Bank Mauritius (41%), Access Bank Rwanda (37%), Bank of Kigali (35%), Empower Bank (32%), and Bank of Baroda Mauritius (31%) point to weaker privacy frameworks and limited readiness for full regulatory compliance. Overall, the results highlight an improving but uneven landscape, with leading banks advancing toward robust data protection standards while others lag, underscoring the need for stronger institutional accountability and regional regulatory alignment.

The insurance sector displayed significant variation in privacy and data protection performance. Jubilee Insurance Uganda (73%) led the sector, followed by UAP Old Mutual (70%, up from 53%), Jubilee Insurance Kenya (66%), Jubilee Allianz General Insurance Mauritius Ltd (65%), and Sicom (62%), reflecting strong progress in data governance and compliance maturity. Mid-range performers such as Mauritius Union Assurance (55%, down from 72%), Britam Tanzania (54%), Old Mutual Rwanda (51%), Britam Uganda (50%), and ICEA Lion Insurance Kenya (50%) demonstrate partial implementation of privacy frameworks but ongoing gaps in transparency and consent management. Lower scores for Vanguard Assurance (11%), BK Insurance Rwanda (10%), NIC Tanzania (8%), Sale Insurance Zimbabwe (6%), and Alliance Zimbabwe (4%) indicate weak privacy controls and elevated compliance risks. Overall, the sector shows encouraging leadership from a few insurers but generally uneven progress, underscoring the need for stronger privacy governance, regulatory alignment, and consistent data protection practices across the region.

Privacy and data protection practices among government agencies show significant variation. Uganda's NIRA led the sector with 51%, followed by eCitizen Kenya (49%), RSSB Rwanda (49%), Ghana Immigration Service (48%), BOCRA Botswana (45%), and KRA Kenya (44%, down from 47%), reflecting moderate adoption of privacy frameworks. Mid-range performers, including UBOS Uganda (43%), MauPass Mauritius (40%), SSNIT Ghana (36%), ETA Kenya (35%), IremboGov Rwanda (35%), and MRA Mauritius (35%), demonstrate partial implementation of privacy controls but ongoing gaps in consent management and data security. Low scores for TCRA Tanzania (8%), IEC Botswana (7%), Electoral Commission Uganda (6%), NCS Nigeria (6%), RRA Rwanda (5%), Tanzania Work Permit Portal (4%), and Uganda Immigration and Passport Office (3%) indicate weak privacy governance and high exposure to data protection risks. Overall, while some agencies are advancing toward better data protection, the sector remains uneven, highlighting the need for stronger regulatory oversight, enhanced governance, and investment in secure, citizen-focused data management systems.

Health facilities demonstrated generally weak compliance with data protection standards. Wellkin Hospital and Clinique Darne led the sector at 61%, followed by IHK Hospital Uganda (59%), Lagoon Hospital (52%), and Dr. Agarwal's Eye Hospital Mauritius (48%), reflecting limited but notable progress in patient data governance. Mid-range performers, including Aga Khan University Hospital (44%), LyfPlus (43%), Nakasero Hospital (38%), Gaborone Private Hospital (36%), and Lubaga Hospital (35%), showed partial adoption of privacy frameworks but continued gaps in consent management and data security. Low scores were widespread, with several hospitals below 15%, including Case Hospital (11%), both Muhimbili National Hospital (Karanda Mission) and Nyaho Medical Centre (8%), and multiple facilities scoring 5% or less, highlighting weak privacy governance and high exposure to data protection risks. Overall, while a few leading hospitals are strengthening data protection practices, the sector remains largely underprepared, emphasizing the need for stronger privacy policies, staff training, and robust enforcement of data protection regulations.

Digital lending platforms exhibited uneven compliance with data protection standards. Renmoney led the sector at 60%, followed by Cim Finance (59%), Branch Nigeria (58%), Bayport Botswana (54%), and Fair Money Nigeria and Fide Ghana (53%), reflecting stronger adoption of data governance practices. Mid-range performers included Branch International Kenya, Lend Plus, M-Kopa Ghana (50%), Zenka and Kiva (49%), Letshego (48%), Fundkiss (46%), and Carbon Nigeria (45%), indicating partial implementation of privacy frameworks but ongoing gaps in consent management and data security. Low scores were observed for Ecocash Zimbabwe (25%), eShagi (20%), Inn Bucks (7%), Zibuko Capital (5%), and MkopoWako and Twiga Loan (4%), highlighting weak privacy controls and elevated risks of unauthorized data access. Overall, while some platforms demonstrate progress in safeguarding customer data, the sector remains largely inconsistent, underscoring the need for stronger privacy policies, robust governance, and regulatory oversight.

On the other hand, over the five-year period, country performance reflects gradual improvement, periodic fluctuations, and differing levels of maturity in data protection implementation. Countries assessed earlier display more visible performance cycles, while newer entrants establish important baselines for future monitoring.

Mauritius (added in 2023) has shown relatively stable but fluctuating performance, recovering to 40.0% in 2025 after a dip in 2024. Zimbabwe, also added in 2023, demonstrates steady incremental growth, rising from 23.1% to 28.0% over three years, signalling gradual institutional strengthening.

Kenya and Uganda exhibit more dynamic trajectories. Kenya peaked in 2023, declined in 2024, and rebounded strongly in 2025, indicating a maturing and resilient system. Uganda followed a similar pattern, with a significant rise in 2023, a temporary drop in 2024, and recovery in 2025.

Rwanda and Tanzania, first assessed in 2024, both recorded modest but positive early gains by 2025, reflecting emerging regulatory capacity. Among 2025 entrants, Nigeria posted a strong baseline score of 44.0%, outperforming several longer-tracked countries, while Ghana and Botswana entered at 36.0%, positioning them in the mid-range of the index.

Overall, the analysis points to steady continental progress, varied reform speeds, and growing alignment with data protection norms, even as consistency and sustained compliance remain ongoing challenges.

While the sectoral performance over the past five years, reflects uneven progress and varying levels of maturity in privacy governance. While some industries show steady improvement, others continue to face structural and compliance gaps, highlighting the need for targeted regulatory intervention.

Telecommunications demonstrates gradual and consistent growth, improving from 35% in 2021 to 46% in 2025, suggesting increasing institutionalisation of privacy practices. In contrast, e-commerce declined sharply after peaking above 50% in 2022, stabilising at 39% in 2024–2025, raising concerns about sustainability amid rapid expansion. Online betting remains volatile, reflecting inconsistent compliance in a high-risk, data-intensive sector.

Banks and financial institutions remain the strongest and most stable performers, recovering to 52% in 2025 after a temporary dip, reflecting mature compliance systems. Insurance shows notable improvement, rising from 23% to 44%, though gaps persist. Government agencies continue to underperform despite modest recovery, while the health sector remains critically weak, reaching only 22% in 2025 despite handling highly sensitive data. Digital loan providers show fluctuating performance, with a 2025 rebound suggesting responsiveness to regulatory pressure.

Overall, no sector consistently exceeds 60%, indicating low overall maturity. Progress appears largely reactive rather than embedded, underscoring the need for sustained capacity building, stronger enforcement, and sector-specific compliance support.

The review of the 20 most widely used mobile applications shows persistent and systemic privacy risks across categories. Social networking apps remain the largest group at 40% (down from 60% last year), followed by file-sharing apps at 10%, with all other categories including mobile banking, email, web browsing, online shopping, betting, productivity, and streaming each accounting for 5%. Despite this shift, privacy protections remain weak across the ecosystem, particularly outside social media.

Fourteen apps were classified as potentially dangerous due to high numbers of embedded trackers and intrusive permissions, up from 10 last year. Tracking is highly concentrated, dominated by Google (45.5% of observed trackers) and Meta (22.7%), meaning over two-thirds of data flows are directed to just two companies. Most apps deploy multiple trackers simultaneously, enabling cross-app aggregation, profiling, and extensive third-party data sharing, often without meaningful user consent.

Recurring issues include excessive data collection, opaque third-party sharing, weak consent mechanisms, inadequate encryption, and limited user control. Commonly requested permissions such as persistent network access, background operation, camera, microphone, location, and device identifiers create cumulative privacy risks when combined over time.

Overall, the findings indicate that mobile app privacy practices remain structurally weak, with layered tracking and broad permissions undermining user autonomy and exposing individuals to profiling, data misuse, and security vulnerabilities. Stronger transparency, data minimisation, and enforcement are urgently needed to safeguard data protection rights.

Advancing effective data protection and safeguarding privacy rights demands collaborative efforts from governments, businesses, regulators, development partners, and civil society. This report emphasizes the need for more enforcement that is robust, greater transparency, and active participation to translate legal frameworks into tangible protections. The following section outlines practical, actionable measures that each stakeholder can implement to strengthen data protection and privacy practices;

Recommendations for Governments

1. Ensure the financial and operational autonomy of Data Protection Authorities (DPAs) through secure funding, transparent appointments, and independence in oversight.
2. Strengthen legal frameworks by incorporating clear breach notification rules, mandatory audits, and defined data retention limits aligned with global standards such as the GDPR and Malabo Convention.
3. Enhance oversight of surveillance by requiring judicial authorization and periodic public reporting to build transparency and public trust.
4. Ratify and domesticate regional data protection treaties like the Malabo Convention and actively participate in EAC, SADC, and AU digital governance initiatives.
5. Promote responsible innovation by establishing frameworks that require Data Protection Impact Assessments (DPIAs) for high-risk AI and digital systems, especially in e-government and health sectors.

Recommendations for Policy Makers

1. Benchmark national and sectoral laws against global best practices such as the GDPR, OECD Guidelines, and AU Model Laws to ensure consistency.
2. Clarify penalty and enforcement provisions through proportional, percentage-based fines that promote compliance without deterring innovation.

3. Integrate data protection principles into broader policy agendas such as digital transformation, e-commerce, and AI governance.
4. Facilitate international and regional cooperation by promoting cross-border data flow agreements, harmonized standards, and joint enforcement mechanisms.

Recommendations for Data Protection Regulators

1. Enhance institutional capacity by securing sustainable funding, expanding skilled personnel, and adopting digital compliance and monitoring tools.
2. Develop and enforce sector-specific regulations addressing dispute resolution, transparency reporting, and compliance mechanisms for high-risk sectors.
3. Expand public awareness through national education campaigns targeting youth, SMEs, and rural communities, and integrate data protection into formal education.
4. Conduct routine, risk-based compliance audits, publish enforcement reports, and maintain public registers of compliant organizations.
5. Collaborate across borders through regional regulator networks to share knowledge and coordinate enforcement on transnational privacy issues.

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

1. Strengthen internal data governance by embedding privacy-by-design, appointing Data Protection Officers, and conducting annual privacy audits.
2. Implement data minimization and security practices including encryption, pseudonymization, and responsible data disposal.
3. Establish transparent breach notification protocols and publish annual privacy and compliance reports.
4. Localize privacy policies to reflect national legal requirements and ensure accessibility in local languages.
5. Foster innovation in compliance by investing in privacy-enhancing technologies (PETs) and participating in regulatory sandboxes.

Recommendations for Data Subjects (Individuals)

1. Exercise legal rights by requesting access, rectification, erasure, portability, and objection under national data protection laws.
2. Stay informed and vigilant about data privacy by engaging with awareness initiatives and reporting non-compliance to regulators.
3. Demand transparency from organizations regarding how personal data is collected, stored, shared, and used.

Recommendations for Civil Society Organizations (CSOs) and the Media

1. Advocate for stronger privacy protections, including expanded rights such as algorithmic transparency and limits on biometric surveillance.
2. Monitor, report, and educate the public on privacy violations through accessible reporting and awareness campaigns.
3. Foster citizen empowerment by promoting digital literacy, encryption use, and responsible civic engagement in privacy advocacy.
4. Convene multi-stakeholder platforms such as privacy observatories or national data protection forums to drive ongoing reform and dialogue.

Recommendations for the Technical Community

1. Provide expert technical input to policymakers and regulators to ensure that data laws are evidence-based and technology-informed.
2. Develop privacy-enhancing technologies (PETs) and tools for secure data management, consent control, and breach detection.
3. Conduct cybersecurity and compliance training for data officers, IT staff, and entrepreneurs to strengthen implementation capacity.
4. Participate in developing regional and international technical standards to align with global privacy and security benchmarks.

Recommendations for Regional and International Mechanisms

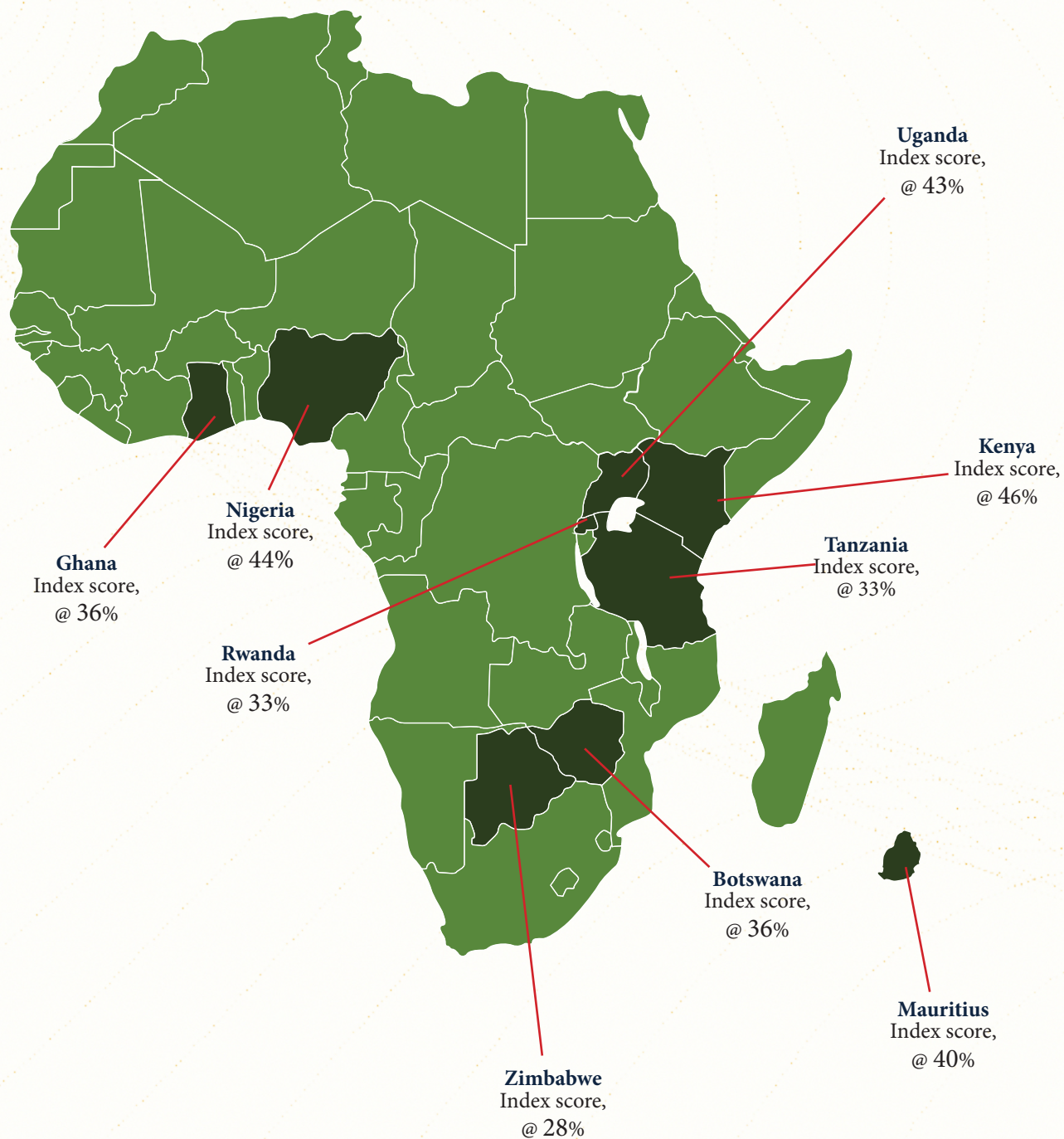
1. Advance regional harmonization by developing common legal and operational data protection benchmarks across Africa.
2. Strengthen regulatory cooperation through peer-review systems and regional data protection taskforces for joint enforcement.
3. Facilitate cross-border data governance through model laws, standard contractual clauses, and mutual adequacy arrangements.
4. Promote knowledge exchange via continental data protection forums and shared capacity-building programs for national DPAs.

Recommendations for Development Partners

1. Support institutional strengthening through funding, capacity-building, and digital tools for regulators, CSOs, and judiciaries.
2. Invest in research and benchmarking to track progress and guide evidence-based reforms in data governance.
3. Promote inclusive, rights-based digital development by integrating privacy safeguards into all digitalization programs.
4. Encourage South–South cooperation and technical exchange to accelerate harmonization and regional learning.

Collectively, these recommendations seek to reinforce institutional independence, strengthen enforcement mechanisms, and entrench a culture of privacy accountability across Africa, ensuring that digital transformation drives not only innovation and economic growth but also inclusion and the protection of fundamental rights. With the inclusion of Nigeria, Ghana, and Botswana in this year's assessment, the analysis provides a broader and more nuanced picture of the evolving data protection landscape across East, West, and Southern Africa. Sustained investment in regulatory capacity, consistent enforcement, and a shared commitment to compliance will be essential to safeguarding personal data and advancing digital rights across the continent.

268 companies / entities were assessed – Overall Index score for each Country:



Key

- Countries that were assessed
- Countries that were not assessed

1. Introduction

As digital transformation accelerates across Africa and beyond, personal data now underpins nearly every aspect of modern life, from commerce and governance to communication and innovation. Safeguarding privacy, a fundamental constitutional right, continues to be a pressing priority for regulators and organizations entrusted with managing personal information. Against this backdrop, the Unwanted Witness Privacy Scorecard Report serves as a comprehensive monitoring tool for assessing how public and private entities comply with national and international data protection and privacy laws. Beyond evaluation, the report provides actionable insights and recommendations to strengthen institutional compliance and accountability.

In 2025, Unwanted Witness broadened its monitoring scope to cover nine African countries: Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda, expanding from six countries in 2024, four in 2023, and two in 2022 and one in the inaugural 2021 edition. This progressive expansion demonstrates the growing recognition of the importance of data protection and privacy across Africa's rapidly digitalizing economies. Building on last year's framework, the 2025 Unwanted Witness Privacy Scorecard Report utilizes the same rigorous methodology to evaluate data collectors and processors across eight critical sectors: telecommunications, e-commerce, online betting, banking and finance, insurance, government agencies, health, and digital lending.

Equally, the 2025 assessment applies the same seven key indicators, to evaluate data protection compliance. These indicators include:

- Registration with the National Regulator
- Accessible Privacy Policy
- Pre-collection Data Transparency (Data Subject Rights)
- Third-Party Data Transfer
- Robust Data Security Practices
- Availability of Transparency Reports
- Internal Data Breach Resolution Mechanisms

The evaluation process follows a rigorous methodology that incorporates peer review and quality validation to ensure accuracy and credibility.

Each organization is assessed against the defined indicators and assigned a score reflecting its overall level of compliance. The results are then classified by indicator and sector, offering a clear and comparative overview of performance across industries and countries.

Only publicly available privacy policies are considered in the scoring process. Internal or unpublished policies, however robust, are excluded to uphold transparency and public accountability. This requirement serves several important functions: it ensures organizations cannot modify internal practices without revising their public commitments, facilitates independent scrutiny of privacy standards, and promotes benchmarking particularly in sensitive areas such as law enforcement data access. This approach also supports peer learning, offers guidance for startups and emerging enterprises, and strengthens collective accountability within the digital ecosystem.

The Privacy Scorecard is intentionally designed to establish ambitious yet practical standards. Each benchmark reflects practices already demonstrated by at least one organization, ensuring that the assessment promotes actionable, scalable improvements rather than theoretical ideals. The criteria are reviewed and refined annually to remain responsive to emerging technologies, evolving policies, and regional regulatory trends.

The overarching goal of the 2025 Privacy Scorecard Report is to produce evidence-based insights that encourage both data controllers and processors to adopt stronger data protection measures, while empowering citizens to demand responsible handling of their personal data. The report further seeks to inform legal and policy reforms, particularly among private sector and non-state actors to enhance compliance and accountability in data governance across Africa.

In total, the 2025 assessment examined 286 organizations across eight sectors, measuring their adherence to national data protection laws and international privacy standards. Using quantifiable indicators, the study captures levels of compliance, documents violations where they occur, and highlights exemplary practices that can serve as models for the region.

Specifically, this year's assessment seeks to:

- Examine the state of personal data protection and privacy in Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda;
- Track changes and progress in compliance among selected organizations over time;
- Evaluate the adherence of data controllers to national and regional data protection laws;
- Identify and document privacy violations or rights abuses by the assessed entities;
- Provide actionable recommendations to strengthen compliance and accountability, particularly among private-sector actors; and
- Offer citizens a practical toolkit to assess compliance and advocate for improved privacy practices.

Building on insights from previous editions, the 2025 Privacy Scorecard continues to track progress in data protection maturity across Africa. With the inclusion of an additional indicator on registration with national regulators and an expanded country scope, this year's report provides a deeper, more comprehensive understanding of the continent's evolving data governance landscape.

2. Methodology And Criteria

The **5th edition** of the UW Scorecard Report offers a snapshot of the privacy practices of **286 private and public companies**, spanning **nine (9) countries** and **eight (8) industries**, all of which manage substantial amounts of personal data due to the size and scope of their operations. The companies assessed increased by 33.56% compared to last year where 190 companies were assessed, 48 companies in 2023 and 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 nine 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 International¹ 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](https://thermarkup.org/blacklight)³ website and [Ghostery](https://www.ghostery.com/)⁴ a browser extension
 7. If the company has any applications, the trackers of the application will be collected with [Exodus](https://reports.exoduc-privacy.eu.org/en/)⁵
 8. The data collector will then locate the company that these trackers belong to with Exodus, [Whotracksme](https://www.whotracksme.com/) 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.

- 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 pro-

¹ 'Data Interception Environment' (Privacy International) at <https://privacyinternational.org/learn/data-interception-environment> accessed 30 October 2025.

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 2025.

³ <https://thermarkup.org/blacklight> at accessed 30 October 2025.

⁴ <https://www.ghostery.com/> at accessed 30 October 2025.

⁵ <https://reports.exoduc-privacy.eu.org/en/> at accessed 30 October 2025.

vision, 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](https://www.qualys.com/ssllabs). 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](https://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 section distils the major insights emerging from the analysis presented in earlier chapters, drawing together the most significant patterns and crosscutting themes revealed by the data. Rather than reiterating individual findings, it highlights the overarching trends that shape how organisations design, implement, and communicate their privacy practices. These consolidated insights provide the analytical backbone for the recommendations that follow, offering stakeholders a clearer understanding of the systemic issues at play and the strategic opportunities for improvement. By interpreting the results collectively, the chapter illuminates the broader implications for regulatory compliance, organisational accountability, and user trust, laying the groundwork for informed decision-making and forward-looking policy development.

3.1 Overview of the general compliance landscape

3.1.1 Evaluation of Findings across Countries and Sectors



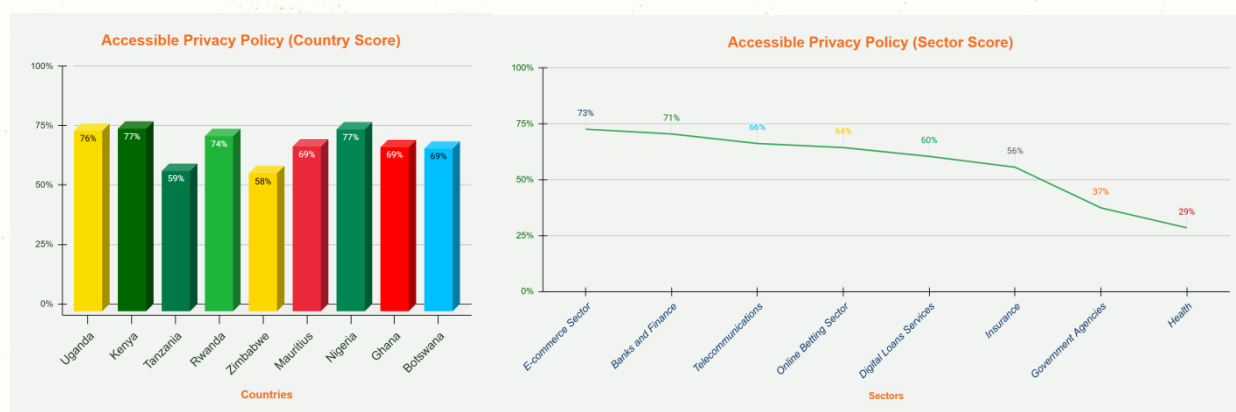
The assessment shows that, much like the previous year, overall performance at the country level continues to fall below the 50% compliance threshold, even though improvements are visible within several sectors. The composite country index rose modestly from 40% to 46%, with Kenya once again achieving the highest score, followed in descending order by Nigeria, Uganda, Mauritius, Ghana, Botswana, Rwanda, Tanzania, and Zimbabwe. Sector-level results, however, reveal more pronounced progress: the Banking and Finance sector maintained its position as the leading performer, climbing to 52% from last year's 42%. Telecommunications followed with 46% (up from 39%), Insurance reached 44% (an increase from 40%), while E-commerce remained stagnant at 39%. Government and Health services continued to register the weakest compliance outcomes. These figures collectively illustrate both the incremental advancements and the persistent structural gaps shaping country and sector trajectories.

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

- a. Registration with the National Regulator** - At the country level, compliance with regulatory registration expanded significantly: whereas only two countries met this requirement last year, the number doubled to four in the current assessment. Overall registration rates rose to 88%, up from 63%, reflecting a broader, but still uneven uptake of formal compliance obligations. Kenya continued to lead, followed by Nigeria at 66%, with Uganda maintaining its previous score of 63% and Ghana reaching 53%. Sectoral performance revealed even sharper contrasts. Banks and Finance, together with the Insurance sector, once again demonstrated the highest levels of regulatory registration, achieving an average of 97%, though slightly below last year's perfect score. In contrast, the Online Betting sector previously scoring 0% made a significant leap to 44%, although it still lagged behind other industries. Telecommunications posted solid gains at 84% (up from 75%), Digital Loans improved substantially to 63% (from 38%), and Government Agencies rose to 50% (from 38%). The Health sector, however, experienced a decline, dropping to 56% from last year's 69%. These figures highlight uneven but generally upward momentum, with some sectors advancing rapidly while others continue to struggle with registration compliance.

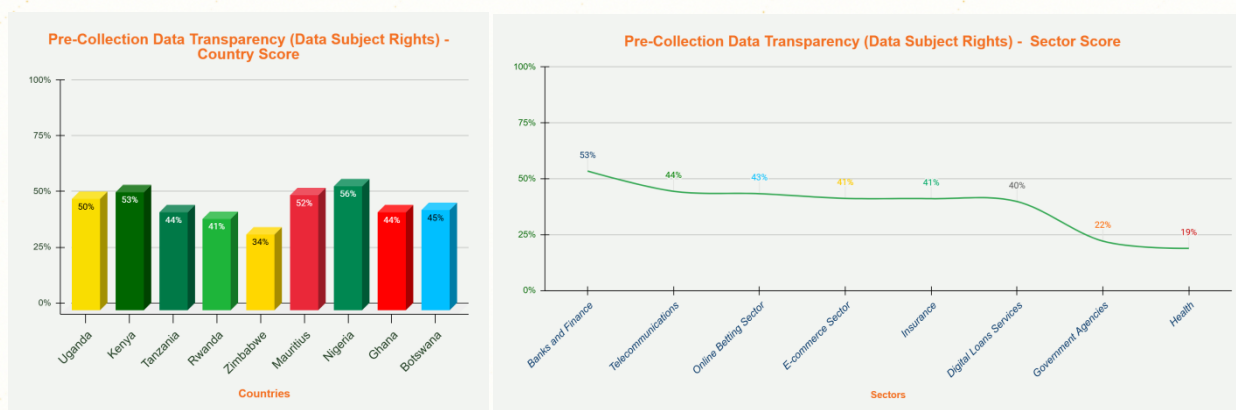


- b. Accessible Privacy Policy** - At the country level, all assessed jurisdictions demonstrated compliance with this indicator, though performance varied considerably. Nigeria and Kenya jointly recorded the highest score at 77%, while the weakest performer reached 58%. Sector-level outcomes revealed a similar pattern of uneven progress. Six of the eight sectors achieved average scores above the 50% threshold, indicating generally improving transparency practices. However, Government Agencies and the Health sector, consistent with last year's results remained the lowest performers, scoring 37% (up from 28%) and 29% (up from 22%) respectively. These persistently low results highlight structural challenges in public sector and health-related privacy communication, despite modest year-on-year improvements.

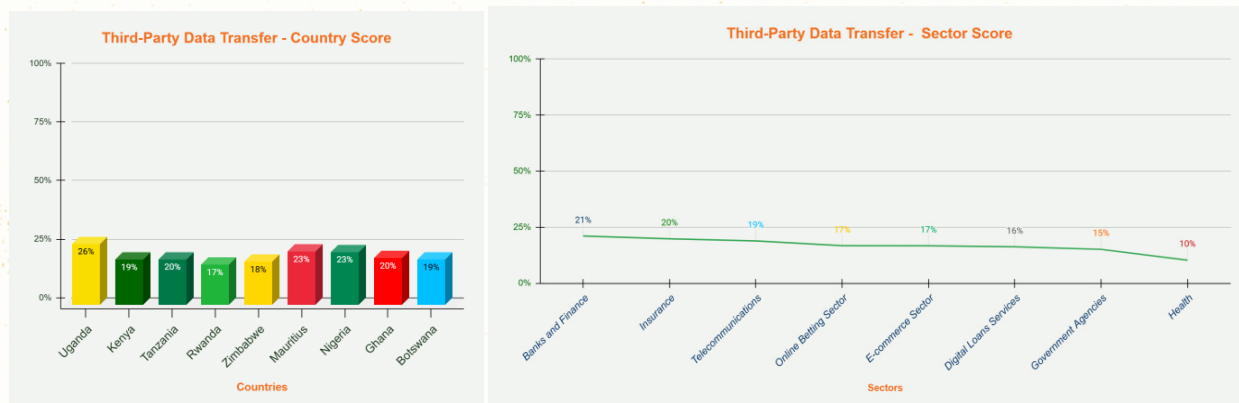


- c. Pre-Collection Data Transparency** - Across all countries assessed, measurable efforts toward meeting this indicator were evident, though performance levels remained modest overall. Nigeria achieved the strongest average score at 56%, a slight improvement from last year's 54%. Kenya followed with 53%, marking a marginal decline from its previous performance, while Mauritius reached 52% (up from 45%) and Uganda 50% (up from 44%). The lowest-performing country scored 34%, improving from last year's 27% but still reflecting significant gaps.

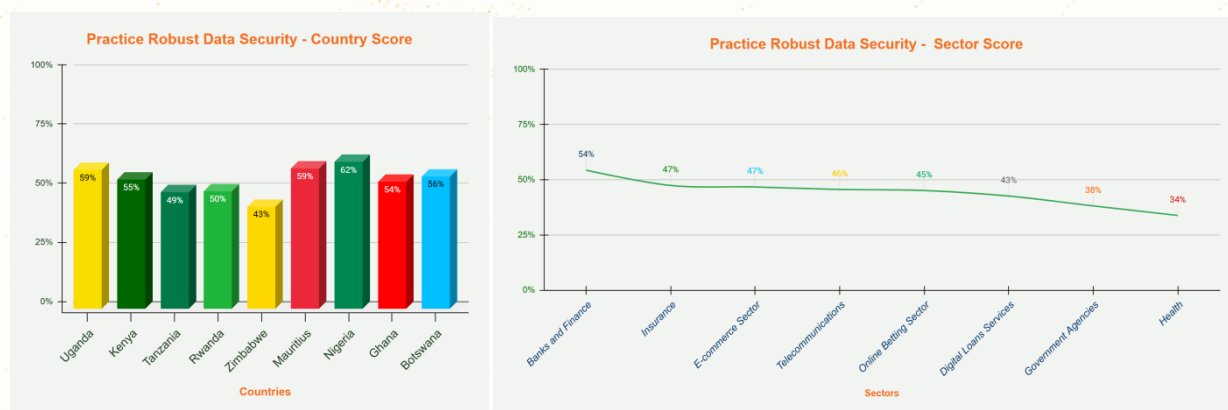
At the sector level, the Banks and Finance sector again emerged as the most compliant, posting an average score of 53% compared with 42% last year. Other sectors including Telecommunications, Online Betting, E-commerce, Insurance, and Digital Loan Services clustered below the 50% mark, indicating uneven alignment with this requirement. The Health sector remained the weakest performer, though it improved from 15% to 19%, signalling incremental progress despite persisting structural challenges.



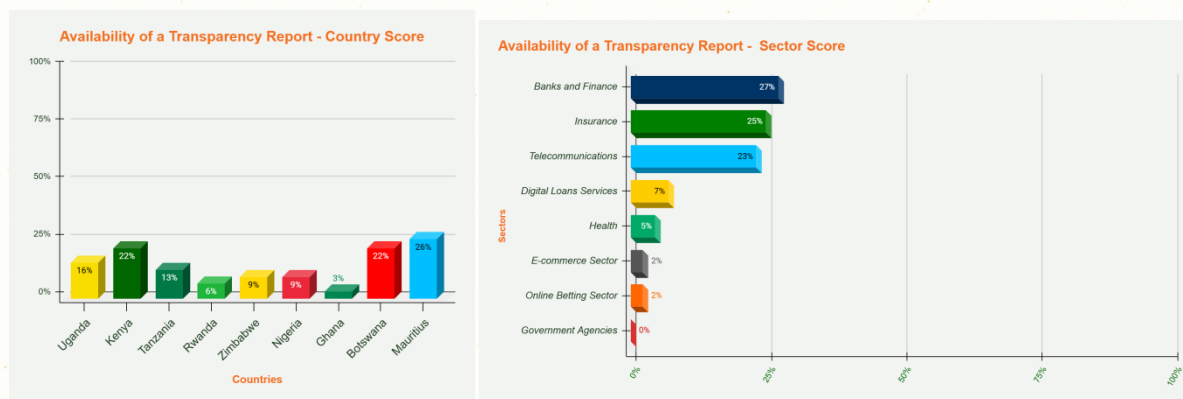
- d. Third-Party Data Transfer** - At both the country and sector levels, the results show that although organisations continued to demonstrate some effort toward meeting this indicator, overall performance remained below the 50% threshold, consistent with last year's pattern. Six out nine countries had demonstrable compliance and Uganda recorded the highest score at 26%, up from 21%, while Nigeria and Mauritius followed closely at 23% each. These figures underscore the persistent challenges in achieving substantive compliance, with progress occurring only in incremental steps.



- e. Practice Robust Data Security** - At the country level, all assessed nations showed increased efforts to comply with the indicator. Nigeria led with the highest score of 62%, improving from 59% last year, followed by Mauritius and Uganda at 59% each (Mauritius up from 57%), and Botswana at 56%. Kenya maintained a consistent score of 55%, while the lowest score remained unchanged at 43%. At the sector level, Banks and Finance once again topped the rankings with a score of 54%, up from 48%, whereas all other sectors continued to score below 50%, highlighting persistent gaps in compliance outside the leading sector.

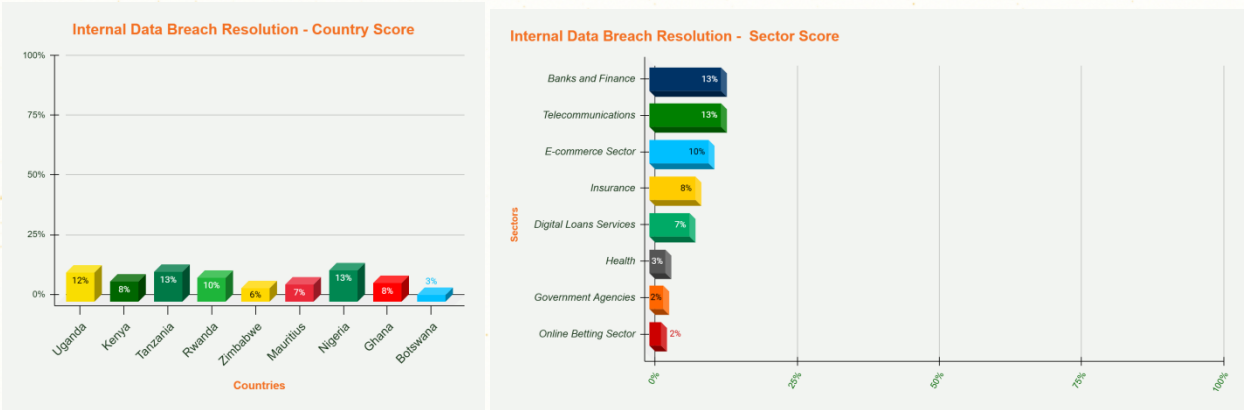


- f. Availability of a Transparency Report** - At both the country and sector levels, compliance with this indicator remained generally low despite noticeable efforts. Mauritius emerged as the highest-performing country, achieving 26%, a substantial increase from 10% last year, followed by Kenya and Botswana at 22% each, Kenya showing significant improvement from 0%. The lowest country score remained at 3%, unchanged from the previous year. At the sector level, Banks and Finance led with 27%, up sharply from 3%, followed by Insurance at 25% (up from 9%) and Telecommunications at 23% (up from 13%). All other sectors recorded scores of 7% or lower, highlighting persistent weaknesses and indicating that targeted interventions are needed to raise compliance across the broader landscape.



- g. Internal Data Breach Resolution** - At both country and sector levels, performance against this indicator remained generally low despite observable compliance efforts. Tanzania and Nigeria led the country rankings with 13% each, Tanzania showing

a notable improvement from 4% and Nigeria up from 11%, followed closely by Uganda at 12%. The lowest country score was 3%, a slight increase from 1% last year. Within sectors, Banks and Finance and Telecommunications topped the performance chart at 13% (up from 7%), followed by e-Commerce at 10% (up from 7%). All remaining sectors scored 8% or below, highlighting persistent gaps in compliance and the need for targeted capacity-building and enforcement strategies to strengthen adherence across the board.

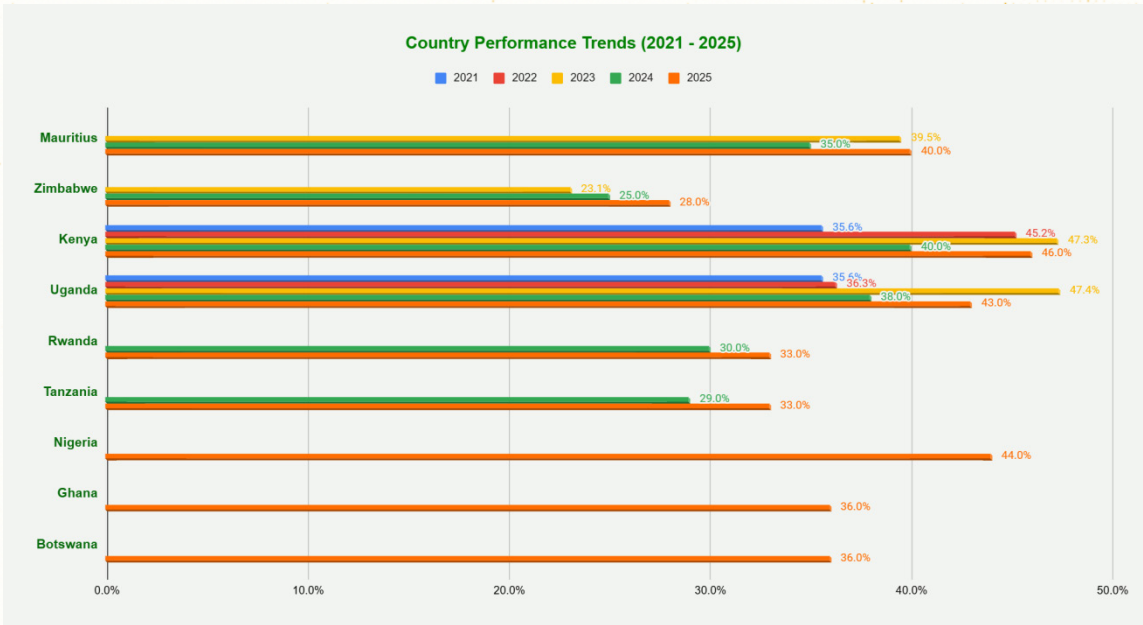


3.2 Highlights of Trends and Patterns across Countries and Sectors

This section presents a synthesis of the notable trends and recurring patterns observed across the assessed countries and sectors. The analysis underscores variations in performance, spotlighting both areas of relative strength and persistent gaps requiring attention. By considering the results from both sectoral and country-level perspectives, we gain a clearer understanding of the underlying factors driving these outcomes, as well as the broader dynamics that shape data protection practices across regions and industries. These insights provide a foundation for targeted interventions, policy refinement, and strategic planning aimed at improving compliance and governance.

3.1.2 Country-Level Performance Over Five Years

A review of the five-year performance trajectory across countries reveals a pattern of gradual improvement, periods of fluctuation, and varied levels of maturity in data protection implementation. Countries added earlier to the Scorecard exhibit more visible performance cycles, while newly assessed countries provide baseline indicators for future monitoring.



Mauritius, included from 2023 onward, demonstrates a somewhat fluctuating yet generally stable performance profile. After a strong entry at 39.5% in 2023, its score dipped to 35.0% in 2024 before recovering to 40.0% in 2025. Although the shifts are modest, the rebound in 2025 suggests renewed momentum in strengthening compliance structures.

Zimbabwe, also added in 2023, shows a steady and incremental improvement across the three assessment cycles. Starting at 23.1% in 2023, Zimbabwe rose to 25.0% in 2024 and further to 28.0% in 2025. While the overall level remains low relative to more established performers, the consistent upward trend signals gradual capacity development and institutional strengthening.

Kenya continues to demonstrate one of the most dynamic performance trajectories. From 35.6% in 2021, the country advanced significantly in 2022 (45.2%) and peaked at 47.3% in 2023. Although Kenya experienced a temporary decline to 40.0% in 2024, it rebounded to 46.0% in 2025. This pattern suggests a maturing system capable of recovery after periods of institutional or operational strain.

Uganda exhibits a similar pattern of fluctuations within an overall upward trajectory. After relatively stable scores in 2021 (35.6%) and 2022 (36.3%), Uganda made a significant jump to 47.4% in 2023. The decline to 38.0% in 2024 mirrors regional challenges noted that year, but the country recovered to 43.0% in 2025, indicating resilience and growing institutional consistency.

Rwanda, added in 2024, entered with a moderate baseline score of 30.0%, improving slightly to 33.0% in 2025. This early ascent reflects strengthening regulatory structures, though significant gaps remain.

Tanzania, also added in 2024, scored 29.0% in its first year and improved to 33.0% in 2025. This trajectory parallels Rwanda's early development curve, pointing to shared regional challenges but also comparably positive initial progress.

Among the countries newly added in 2025, Nigeria emerged as one of the stronger performers with a baseline score of 44.0%, surpassing several countries that have been tracked over the full five-year period. This strong entry underscores Nigeria's ongoing institutional reforms and growing emphasis on data governance.

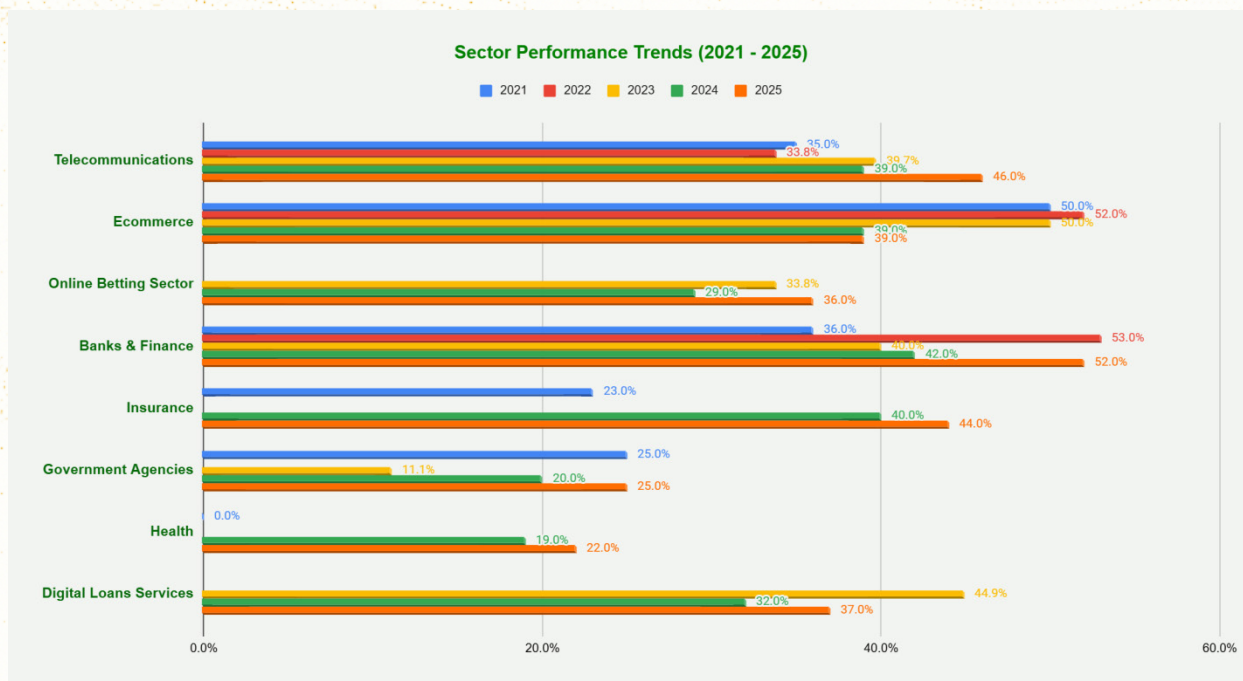
Ghana and Botswana, also assessed for the first time in 2025, entered at 36.0% each. These baseline scores place both countries in the mid-range of the index, providing a foundation for monitoring future improvement and aligning with broader regional trends.

Overall, the five-year analysis reveals a continental landscape marked by gradual improvement, differentiated rates of progress, and increasing alignment with data protection norms. Earlier entrants show more pronounced performance cycles, while newer entrants provide important reference points for future benchmarking. The collective upward trend across nearly all countries suggests growing institutional investment in data protection, even as challenges persist in achieving consistent and sustained compliance.

3.1.3 Sector-Level Performance over Five Years

An examination of sectoral performance over the past five years reveals a landscape marked by uneven progress, sector-specific challenges, and fluctuating levels of maturity in privacy governance. While some industries demonstrate clear and sustained improvements, others continue to exhibit significant structural and compliance gaps, underscoring the need for targeted regulatory and institutional interventions. The telecommunications sector illustrates a pattern of steady advancement. With scores rising from 35% in 2021 to 46% in 2025, telecom operators appear to be gradually formalizing and institutionalizing privacy practices. This upward trajectory, though modest, suggests growing attention to internal controls, transparency mechanisms, and regulatory compliance likely driven by heightened scrutiny and the sector's centrality in digital ecosystems.

The e-commerce sector, which began as a top performer in 2021 and 2022, presents a contrasting picture. After peaking at over 50%, its performance declined sharply from 2023 onwards, stabilizing at 39% in 2024 and 2025. This regression signals weakening adherence to privacy best practices, likely influenced by rapid market expansion, complex data flows, and insufficient governance structures to match operational growth. The stagnation observed in the last two years raises concerns about sustainability of privacy measures within online retail platforms.



Similarly, the online betting sector exhibits volatility, recording a decrease from 33.8% in 2023 to 29.0% in 2024 before recovering to 36% in 2025. Such fluctuations reflect inconsistent embedding of privacy principles within an industry known for intensive data processing and high compliance risk. Regulatory oversight appears insufficient to stabilise these outcomes, suggesting a need for more stringent enforcement mechanisms.

In contrast, banks and financial institutions continue to demonstrate the strongest and most stable compliance performance across all sectors. Despite a temporary dip in 2023, the sector recovered significantly to 52% in 2025, mirroring its earlier peak. This trend reflects long-standing investments in compliance infrastructure, risk management, and data protection frameworks, driven by regulatory requirements and the sector's dependence on public trust.

The insurance sector also shows significant growth, from 23% in 2021 to 44% in 2025 indicating improving internal governance and greater recognition of privacy as an essential component of digital transformation efforts. However, the continued moderate performance suggests that more work is needed to strengthen transparency, consent processes, and safeguards around data sharing.

Despite slight improvements, government agencies remain among the poorest performers. Following a sharp decline to 11% in 2023, the sector made gradual progress, returning to 25% in 2025. This chronic underperformance reflects systemic gaps such as limited institutional capacity, inadequate policy frameworks, and low prioritisation of citizen data protection factors that pose significant risks to public trust and digital service delivery.

The health sector, despite dealing with highly sensitive personal data, continues to score dangerously low. Rising from 0% in 2021 to only 22% in 2025, health institutions still lack robust data protection systems, particularly in the areas of security controls, consent management, and breach preparedness. This exposes patients to substantial risks and signals a pressing need for sector-wide reforms.

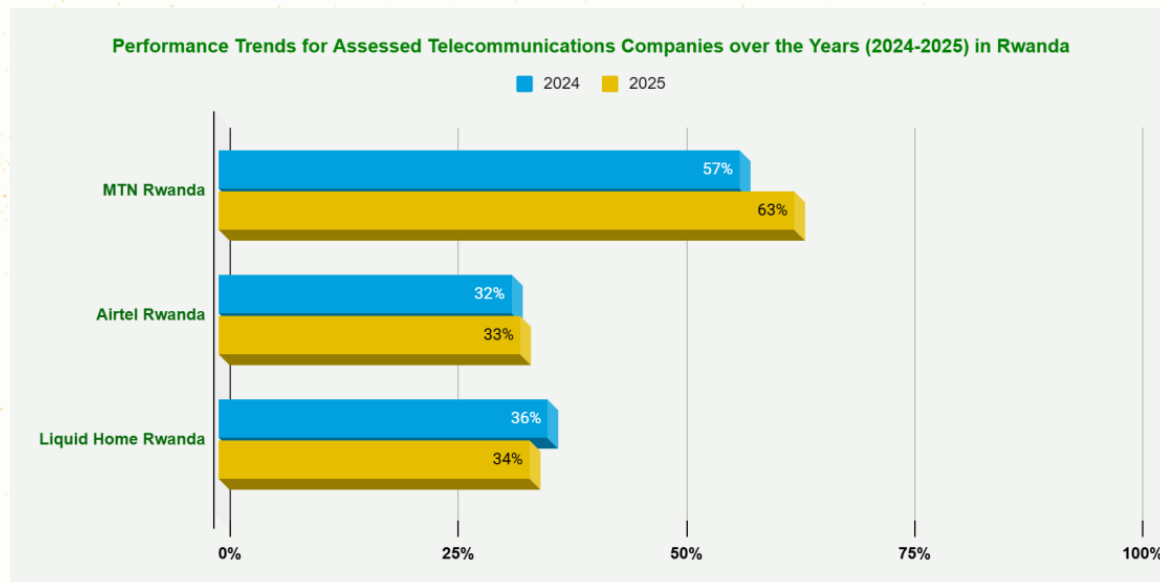
Finally, digital loan service providers reveal a mixed trajectory. After strong performance in 2023, scores dropped sharply in 2024 before partially recovering in 2025. These fluctuations suggest difficulties in aligning business models, often reliant on aggressive data extraction with emerging privacy norms. However, the 2025 rebound indicates increasing responsiveness to regulatory pressure.

Across all sectors, the data highlights a persistent low maturity level in privacy compliance, with no industry consistently exceeding the 60% threshold. The sporadic nature of improvements suggests that progress is largely reactive, driven more by external pressures than by embedded institutional culture. This underscores the need for sustained capacity building, sector-specific guidance, and stronger enforcement mechanisms to ensure privacy protection becomes a fundamental component of organizational practice.

3.1.4 Five-Year Performance of Assessed Companies/Entities

Here, we dive into the five-year performance trajectories (2021–2025) of the evaluated companies and entities. By analysing historical trends and core metrics, this section reveals key patterns, competitive advantages, and priority improvement areas providing actionable insights into compliance drivers and hurdles to empower better decision-making and forward-thinking planning.

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



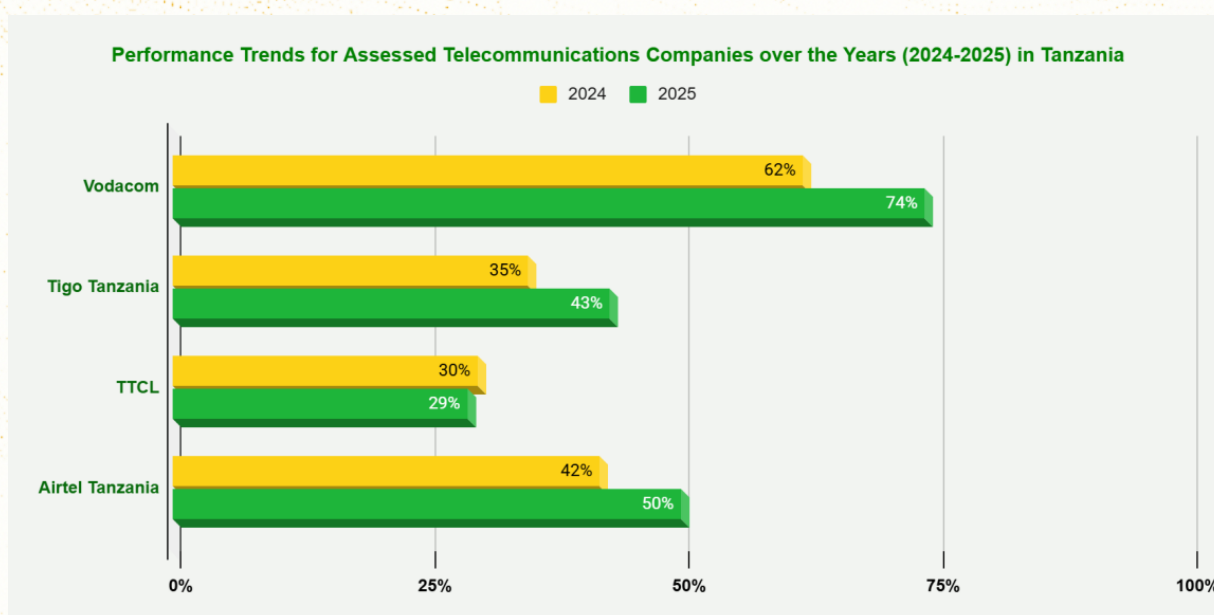
The performance data for Rwandan telecommunications operators highlights varying levels of maturity and progress in privacy and data protection practices. While MTN Rwanda demonstrates clear improvement, Airtel Rwanda and Liquid Home Rwanda show limited gains, suggesting differences in governance, investment, and operational prioritisation.

MTN Rwanda's performance has improved from 57% in 2024 to 63% in 2025. This upward trend indicates a deliberate and structured approach to enhancing privacy and data protection practices, likely involving strengthened policies, governance frameworks, and technical safeguards. MTN Rwanda demonstrates growing privacy maturity, embedding compliance and risk management into operational processes. Continued focus on monitoring, accountability, and privacy by design will help sustain and further improve its performance, reducing regulatory and operational risk.

Airtel Rwanda's performance has remained largely static, increasing slightly from 32% in 2024 to 33% in 2025. This minimal change suggests limited progress in institutionalising privacy practices or enhancing technical safeguards. Airtel Rwanda appears to be at an early stage of privacy maturity. Without strategic investment.

Liquid Home Rwanda exhibits a slight decline in performance, from 36% in 2024 to 34% in 2025. This decrease indicates challenges in maintaining or updating existing privacy practices. The decline may reflect operational gaps, insufficient oversight, or limited integration of privacy considerations into business processes. Liquid Home Rwanda's performance signals emerging risk in privacy governance. To improve, the organisation needs to prioritise consistent implementation of privacy policies, strengthen technical and organisational safeguards, and ensure privacy by design is embedded into service delivery and operational processes.

In sum, MTN Rwanda leads in privacy and data protection maturity, showing measurable improvement. In contrast, Airtel Rwanda remains largely stagnant, and Liquid Home Rwanda exhibits slight regression. Collectively, these trends suggest that while MTN Rwanda is progressing toward stronger compliance and operational security, Airtel and Liquid Home Rwanda need focused interventions to stabilise and advance their privacy practices.



The data from 2024 to 2025 shows distinct differences in privacy and data protection maturity among major Tanzanian telecom operators. The trends highlight progress, stagnation, and areas of potential risk exposure.

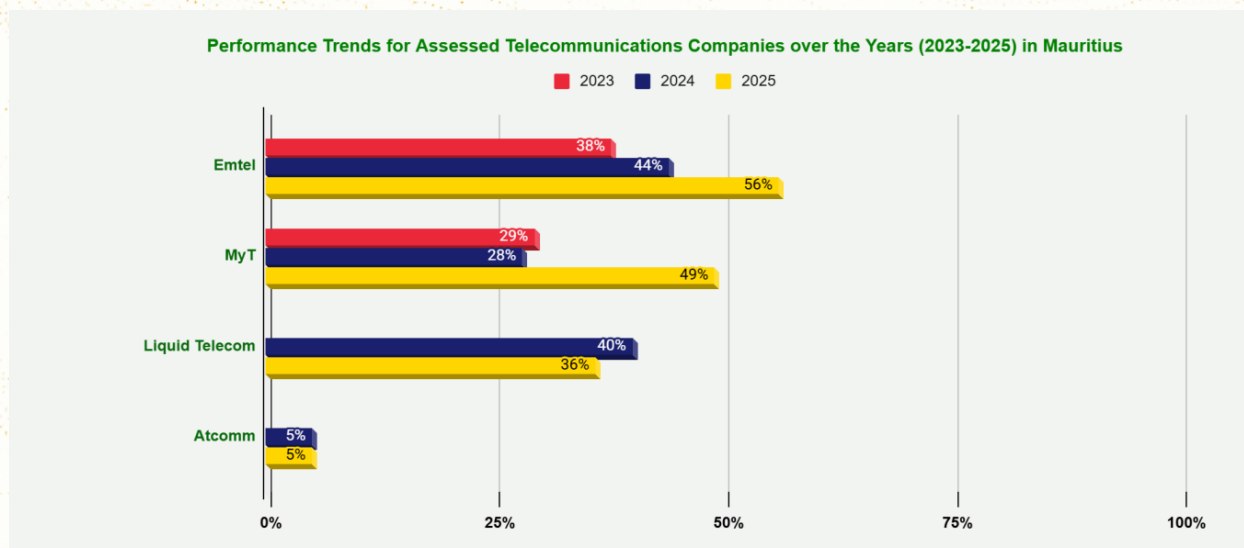
Vodacom demonstrates strong and consistent improvement, increasing from 62% in 2024 to 74% in 2025. This upward trajectory reflects deliberate investments in governance, technical safeguards, and regulatory compliance. The performance indicates a mature privacy posture with effective implementation of privacy principles across lawfulness, data security, accountability, and privacy by design. Vodacom leads the market in privacy maturity. Sustaining this performance will require ongoing monitoring, proactive adaptation to regulatory changes, and continued embedding of privacy practices into all operations.

Tigo Tanzania improved moderately from 35% in 2024 to 43% in 2025. The growth reflects incremental enhancement of privacy and data protection practices, likely through strengthened policies, security measures, and governance oversight. However, the overall score indicates that Tigo still operates at a moderate level of maturity, with further work required to consistently meet regulatory expectations. Tigo should continue to strengthen accountability structures, implement robust technical safeguards, and ensure privacy by design is integrated into service delivery to maintain progress and reduce operational risk.

TTCL shows a slight decline from 30% in 2024 to 29% in 2025. This trend indicates challenges in sustaining prior controls or in adapting privacy frameworks to evolving operational and regulatory demands. The low and declining performance signals limited embedding of privacy principles and weak governance structures. TTCL faces significant privacy and compliance risk. Urgent investment in governance, technical safeguards, and systematic monitoring is required to prevent further deterioration and to improve institutional privacy maturity.

Airtel Tanzania demonstrates steady improvement, rising from 42% in 2024 to 50% in 2025. The upward trend reflects deliberate efforts to strengthen privacy governance, enhance technical and organisational safeguards, and improve alignment with regulatory requirements. Airtel Tanzania is building a moderate level of privacy maturity. Continued focus on embedding privacy by design, enhancing oversight, and ensuring consistent application across operations will be critical to sustaining improvements.

Vodacom Tanzania leads the market with strong privacy maturity and consistent progress. Airtel Tanzania shows steady improvement, while Tigo Tanzania is moderately advancing. TTCL remains stagnant with a slight decline, indicating emerging privacy and compliance risks.



Emtel demonstrates a consistent and sustained improvement in privacy performance, increasing from approximately 38% in 2023 to 44% in 2024 and reaching 56% in 2025. This upward trajectory reflects a structured and deliberate approach to strengthening privacy and data protection practices, rather than isolated or reactive interventions. The progression indicates that privacy controls are increasingly embedded within organisational processes and decision-making frameworks. The 2024 assessment correctly identified Emtel as improving but not yet fully aligned with higher international privacy standards. The 2025 results confirm that these gaps are being actively addressed, positioning Emtel as the most mature organisation among its peers in terms of privacy governance.

From a lawfulness, fairness, and transparency perspective, Emtel's steady improvement suggests increasing maturity in lawful processing mechanisms, clearer and more consistent privacy notices, and more robust management of consent and customer communications across the organisation. With regard to data security and integrity, the sustained upward trend points to the ongoing strengthening of technical and organisational safeguards, supported by improved risk management practices and incident preparedness. The absence of significant performance volatility indicates that security controls are not only implemented but also effectively maintained and periodically reviewed.

Emtel's performance also reflects strong accountability and governance, evidenced by consistent year-on-year improvement, defined roles and responsibilities, and clear management ownership of privacy risks. Furthermore, the results indicate growing alignment with privacy by design and default, with privacy considerations increasingly integrated into system development, service design, and operational processes.

MyT's privacy performance exhibits volatility over the assessment period, followed by a marked improvement in 2025. After a marginal decline from approximately 29.3% in 2023 to 28.0% in 2024, the organisation recorded a significant increase to 49% in 2025. The decline observed in 2024 highlighted challenges in maintaining momentum in privacy compliance and keeping pace with evolving regulatory and operational demands. The sharp rebound in 2025 indicates that corrective actions were implemented in response to identified weaknesses. While this improvement is notable, the abrupt nature of the increase suggests a remediation-driven approach rather than a sustained, incremental maturity model. As such, MyT's privacy posture has improved substantially, but its long-term sustainability remains dependent on continued governance, monitoring, and institutionalisation of controls.

From a lawfulness, fairness, and transparency perspective, the 2024 decline points to earlier difficulties in maintaining compliant processing practices and adapting to regulatory change. The improvement in 2025 suggests corrective measures, including updates to privacy notices, processing records, and consent management mechanisms; however, the scale and speed of progress indicate that consistent application across all operations may still be maturing.

In relation to data security and integrity, the 2025 performance increase reflects accelerated strengthening of technical and organisational safeguards, potentially through enhanced controls, policies, and monitoring capabilities. While these measures reduce immediate risk exposure, their reactive implementation underscores the need for sustained investment and ongoing effectiveness testing. With respect to accountability and governance, MyT appears to be transitioning toward stronger ownership of privacy risks. Nevertheless, year-on-year performance volatility indicates that governance structures, assurance processes, and management oversight are not yet fully embedded. Alignment with privacy by design and default is improving, but privacy considerations may still be applied retrospectively rather than being consistently integrated into the design of new systems, products, and initiatives.

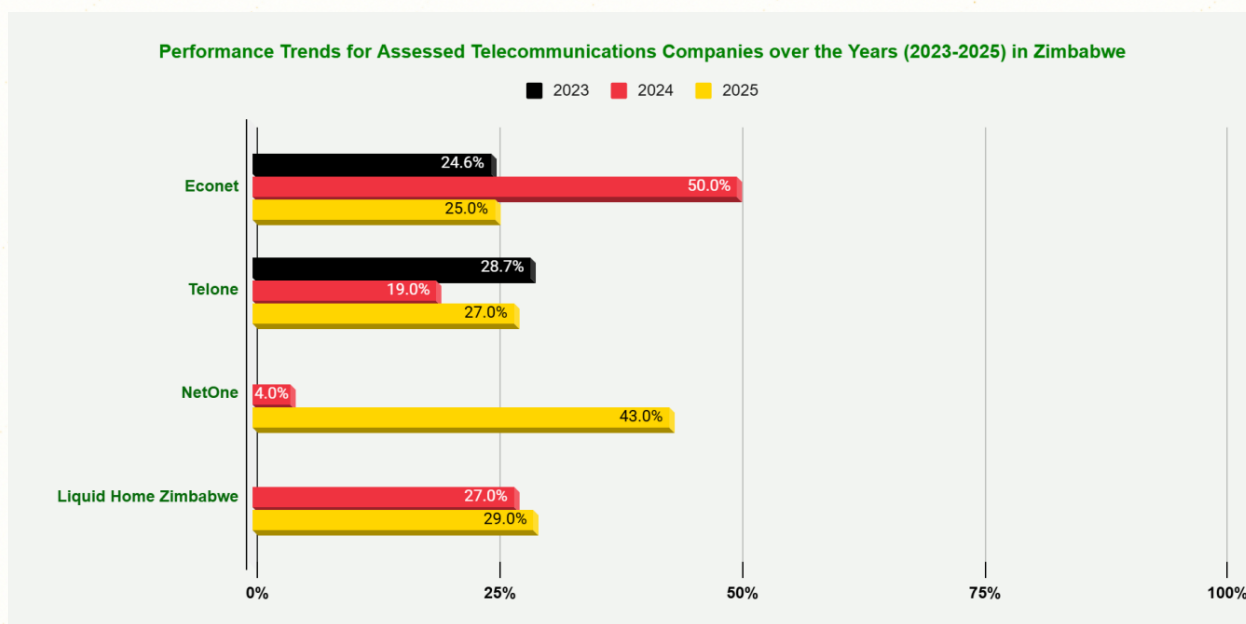
Liquid Telecom demonstrates a moderate level of privacy capability followed by a decline in performance in 2025, decreasing from approximately 40% in 2024 to 36% in 2025. While earlier results indicated a reasonable baseline, the downward trend suggests growing challenges in sustaining and evolving existing privacy and data protection controls in line with increasing operational complexity and regulatory expectations. This pattern indicates the potential emergence of *privacy debt*, whereby controls exist but are not sufficiently updated, resourced, or consistently enforced. Without targeted intervention, this decline is likely to translate into elevated compliance and operational risk.

From a lawfulness, fairness, and transparency perspective, the decline may reflect difficulties in maintaining alignment between processing activities, contractual arrangements, and applicable regulatory requirements as the organisation's operations evolve. This increases the risk of inconsistencies in how personal data is processed and communicated to data subjects. In terms of data security and integrity, the reduction in performance points to potential gaps in the maintenance, testing, and periodic review of technical and organisational safeguards. While security controls may be in place, the trend suggests that they may not be keeping pace with changes in systems, data volumes, or the evolving threat landscape. With respect to accountability and governance, the downward trajectory indicates possible weaknesses in oversight, clarity of roles and responsibilities, and prioritisation of privacy risk management. Alignment with privacy by design and default also appears to be weakening, particularly where privacy considerations are not systematically incorporated into system upgrades, process changes, or service expansions.

Atcomm's privacy performance remains consistently low, with no measurable improvement between 2024 and 2025, both recorded at approximately 5%. This sustained stagnation indicates minimal progress in developing or implementing privacy and data protection measures and reflects a very low level of privacy maturity. Compared to industry peers, Atcomm remains at an early stage of privacy capability, exposing the organisation to significant regulatory, operational, and reputational risks.

From a lawfulness, fairness, and transparency perspective, the lack of improvement suggests insufficient formalisation of lawful processing bases, limited or unclear privacy notices, and weak mechanisms for communicating with data subjects. In relation to data security and integrity, the persistently low performance strongly indicates inadequate technical and organisational safeguards, significantly increasing the likelihood of data breaches, data loss, or unauthorised access. Atcomm also demonstrates limited alignment with accountability and governance principles, with little evidence of defined roles and responsibilities, management oversight, or structured privacy risk management. Furthermore, there is minimal indication of privacy by design and default, with privacy considerations unlikely to be embedded into system development, operational processes, or service delivery.

In sum, performance over the years demonstrates that sustained improvement and principle-based governance are key determinants of privacy maturity. Emtel shows strong and consistent alignment with core privacy principles, MyT has made notable but reactive gains, Liquid Telecom exhibits early signs of control erosion, and Atcomm remains significantly exposed. These trajectories provide a clear basis for prioritising risk mitigation efforts and regulatory engagement heading into 2026.



The performance trends observed across the four operators between 2023 and 2025 reveal divergent trajectories in maturity, consistency, and sustainability of organisational practices. While some operators demonstrate progress and responsiveness, others exhibit volatility or persistent weaknesses that raise concerns regarding the robustness of their underlying frameworks.

Econet's performance shows a mixed trajectory over the assessment period. After a significant improvement from 24.6% in 2023 to 50.0% in 2024, the score declined sharply to 25.0% in 2025. Last year's analysis correctly identified Econet's 2024 improvement as a strong signal of enhanced practices, likely driven by focused investments in compliance, security controls, and policy refinement. However, the subsequent decline in 2025 suggests that these improvements may not have been fully institutionalised.

The drop indicates potential challenges in sustaining momentum, such as inconsistent implementation across business units, resource reallocation, or reduced governance oversight. While Econet demonstrated the capacity to improve rapidly, the volatility points to a need for stronger operationalisation, continuous monitoring, and embedded governance to ensure that gains are durable rather than episodic. Econet's practices appear capable but insufficiently stabilised.

Without reinforcing accountability and ongoing assurance mechanisms, performance gains may continue to fluctuate, exposing the organisation to compliance and operational risk.

Telone's performance reflects a steady downward trend followed by only partial recovery. After declining from 28.7% in 2023 to 19.0% in 2024, Telone recorded a modest improvement to 27.0% in 2025. Last year's analysis highlighted the 2024 decline as a significant concern, signalling potential underinvestment in frameworks, weak compliance execution, or emerging risk exposures.

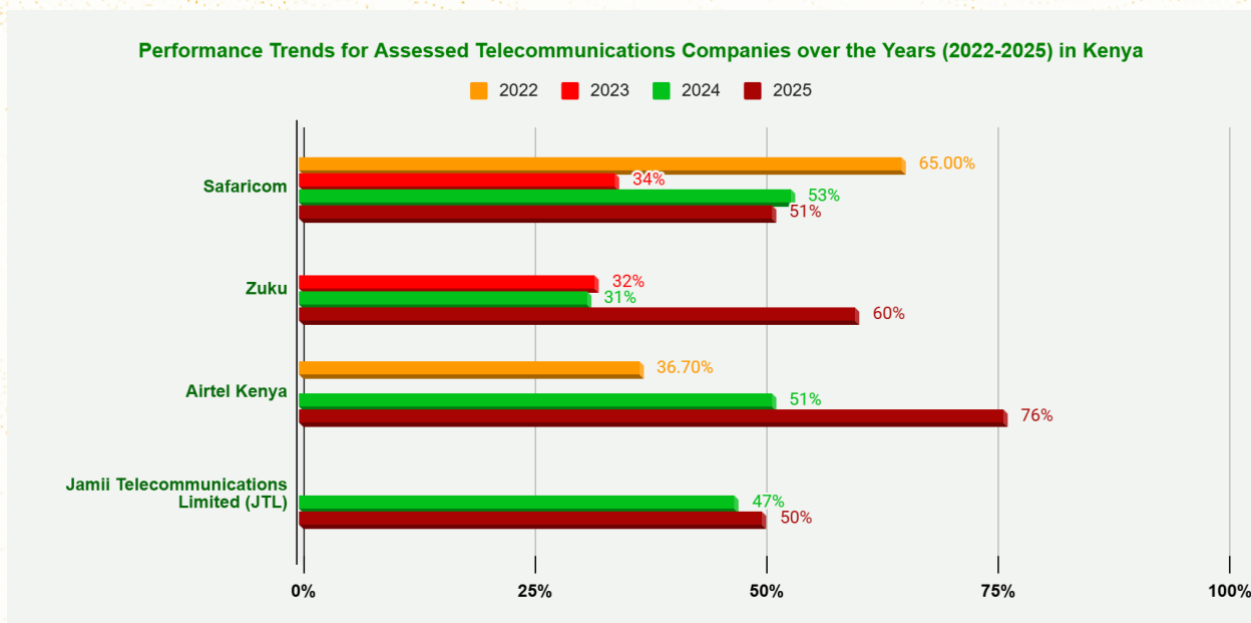
The 2025 improvement suggests that corrective actions may have been initiated in response to these concerns. However, the recovery merely returns Telone to approximately its 2023 level, rather than demonstrating clear progression. This pattern indicates reactive remediation rather than sustained enhancement of practices. Telone appears to be addressing immediate gaps but has yet to demonstrate consistent advancement. Continued focus is required on strengthening governance, resourcing, and long-term capability development to avoid recurring cycles of decline and recovery.

NetOne exhibits the most dramatic change across the period. From a very low score of 4.0% in 2024, the company recorded a substantial increase to 43.0% in 2025. While 2023 data is unavailable, the magnitude of the 2025 improvement strongly suggests a significant intervention, such as the introduction of new controls, frameworks, or leadership-driven initiatives.

Although this rebound is noteworthy, the scale and speed of improvement raise questions about maturity and consistency. Such rapid gains often reflect foundational remediation rather than fully embedded practices, and their effectiveness will depend on sustained implementation and oversight. NetOne has made meaningful progress in addressing critical weaknesses, but its practices remain at a transitional stage. The primary risk lies in ensuring that recent improvements are embedded, tested, and maintained over time.

Liquid Home Zimbabwe shows gradual but modest improvement across the period, increasing from 27.0% in 2024 to 29.0% in 2025. While 2023 data is not available, the limited year-on-year growth suggests incremental change rather than transformation. This steady but low-level performance indicates the presence of baseline practices, but also points to constrained momentum, possibly due to limited scope, resources, or prioritisation. Compared to peers showing either strong recovery or significant fluctuation, Liquid Home Zimbabwe appears relatively stable but underdeveloped. Without more decisive investment and strategic focus, Liquid Home Zimbabwe risks stagnation. Incremental improvement alone may be insufficient to meet rising regulatory and operational expectations.

Last year's analysis accurately identified Econet as an improver and Telone as an organisation facing setbacks. The 2025 data adds nuance to this assessment: Econet's gains have proven difficult to sustain, while Telone has stabilised but not yet progressed. The emergence of NetOne as a rapidly improving performer introduces a new dynamic, while Liquid Home Zimbabwe remains largely unchanged at a low-to-moderate level. Overall, the data highlights that sustained performance is more indicative of mature practices than short-term gains. Organisations demonstrating volatility face heightened risk that improvements are not embedded, while those showing limited movement risk falling behind evolving expectations. To improve outcomes, all operators must prioritise consistent governance, continuous monitoring, and long-term institutionalisation of practices rather than relying on periodic corrective efforts.



The performance trends across Safaricom, Zuku, Airtel Kenya, and Jamii Telecommunications Limited (JTL) highlight varying levels of maturity, consistency, and responsiveness in privacy and data protection practices. While some operators demonstrate steady improvement, others show volatility or delayed progress, which has implications for operational resilience and regulatory compliance.

Safaricom's performance has fluctuated over the past four years. After peaking at 65% in 2022, the score declined to 53% in 2024 before stabilizing at 51% in 2025. Last year's analysis acknowledged the company's strong historical performance and ongoing efforts to enhance its data protection frameworks. The slight decline from 2022 indicates potential operational or regulatory challenges, but the overall improvement since 2023 reflects continued commitment to safeguarding user data.

The observed trend suggests that while Safaricom has a mature privacy posture, sustaining high performance requires ongoing governance, monitoring, and adaptation to regulatory changes, particularly given the large volumes of personal and financial data it handles. Safaricom demonstrates a strong privacy framework but must maintain continuous oversight to prevent minor dips from becoming systemic issues.

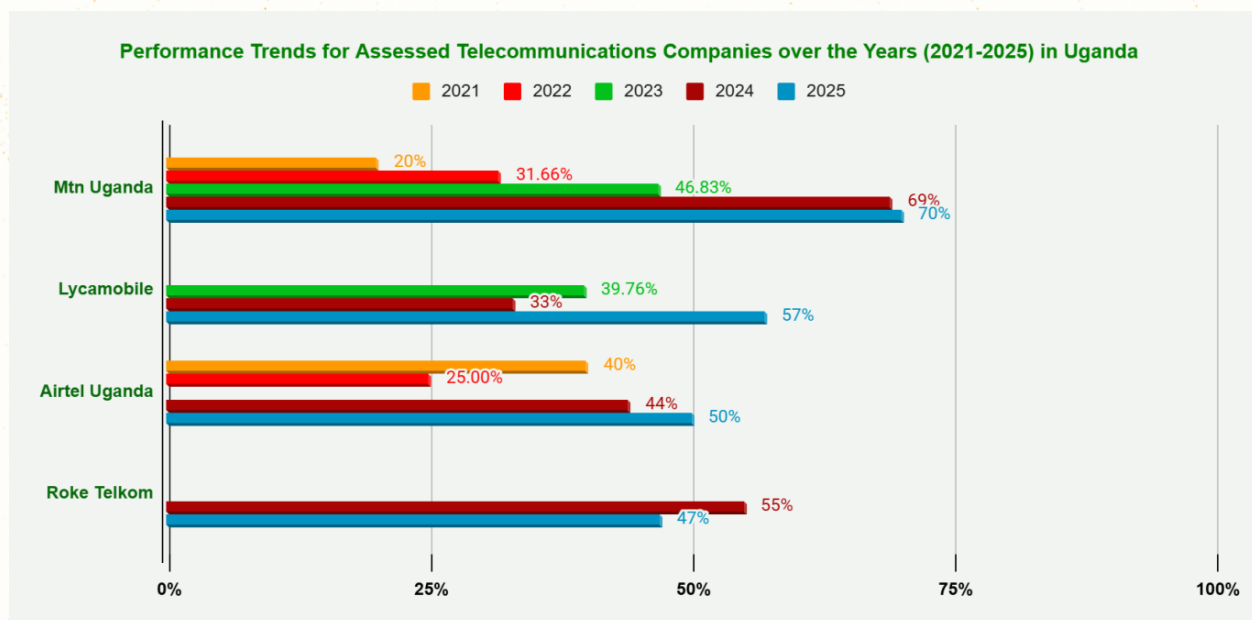
Zuku's performance shows a remarkable rebound in 2025, rising to 60% from 31% in 2024 and 31.9% in 2023. Previously, last year's analysis noted the company's stagnation and low privacy maturity. The 2025 improvement indicates that Zuku has likely implemented corrective measures, such as enhanced policies, technical controls, or governance mechanisms.

Despite this rapid progress, the dramatic nature of the improvement suggests remediation-driven change rather than fully embedded practices. The sustainability of these gains will depend on consistent application of controls, regular monitoring, and integration of privacy by design principles. Zuku has taken significant steps to strengthen its privacy posture, but attention is needed to institutionalize these changes and ensure long-term compliance and operational resilience.

Airtel Kenya has shown a consistent upward trajectory, improving from 36.7% in 2022 to 51% in 2024 and further to 76% in 2025. Last year's analysis highlighted the positive trend and commitment to aligning practices with best-in-class standards. The continued growth indicates that Airtel Kenya is systematically addressing gaps in its privacy and data protection framework, including technical safeguards, policy updates, and compliance mechanisms. The steady progression suggests that privacy considerations are increasingly embedded into operational processes, risk management practices, and governance structures. Airtel Kenya demonstrates strong and improving privacy maturity. Sustaining this trajectory will require ongoing investment in security controls, employee awareness, and regulatory alignment to maintain trust and competitive advantage.

JTL shows gradual improvement, rising from 47% in 2024 to 50% in 2025. While 2023 and earlier data are not fully available, the modest growth indicates that foundational practices are in place, but momentum remains limited. The incremental progress suggests that improvements are likely operational or compliance-driven rather than reflective of a comprehensive strategic privacy framework. JTL's privacy posture is developing but remains relatively nascent. Greater emphasis on formal governance structures, technical safeguards, and integration of privacy by design will be necessary to achieve parity with leading operators.

Last year's assessment accurately identified Safaricom as strong but facing minor challenges, Zuku as stagnant, and Airtel Kenya as improving steadily. The 2025 data adds nuance: Zuku demonstrates a marked rebound, Airtel Kenya continues its strong upward trend, Safaricom shows minor decline but retains high maturity, and JTL exhibits modest incremental improvement. Overall, the data underscores that sustained privacy performance reflects embedded governance and operationalisation, while rapid gains may signal remediation efforts that require consolidation. Safaricom and Airtel Kenya demonstrate mature and improving practices, Zuku shows significant catch-up progress, and JTL remains in an early development stage. All operators should continue prioritizing compliance, security, and governance to ensure sustainability, regulatory alignment, and customer trust.



The performance trends among the major telecommunications providers in Uganda reveal significant differences in maturity, consistency, and responsiveness in privacy and data protection practices. Some operators demonstrate steady progress, while others show volatility, reflecting differing approaches to governance, operationalisation, and compliance.

MTN Uganda has shown strong and consistent improvement over the assessment period, increasing from 20% in 2021 to 31.66% in 2022, 46.83% in 2023, 69% in 2024, and reaching 70% in 2025. Last year's analysis highlighted MTN Uganda's rapid rise as a clear indication of significant investment in data protection policies, compliance, and technical safeguards. The continued improvement in 2025 reinforces the view that MTN Uganda has embedded privacy considerations into operational processes, governance structures, and risk management practices. The organisation demonstrates high privacy maturity, capable of handling sensitive user information in alignment with regulatory expectations.

MTN Uganda's practices are robust and maturing, but sustaining high performance will require continuous monitoring, adaptation to regulatory developments, and ongoing reinforcement of governance mechanisms.

Lycamobile exhibits a volatile trajectory. After improving from 25% in 2022 to 39.76% in 2023, its score declined sharply to 33% in 2024, before rebounding to 57% in 2025. Last year's analysis identified the 2024 drop as a signal of challenges in maintaining privacy and security practices, potentially due to inconsistent implementation, limited investment, or gaps in compliance.

The 2025 rebound indicates that corrective actions were implemented, likely targeting governance, technical safeguards, and compliance frameworks. However, the abrupt nature of the increase suggests that improvements are remediation-driven and may not yet be fully institutionalised across all operations. Lycamobile is capable of making significant improvements but must focus on embedding controls and monitoring mechanisms to ensure sustained privacy maturity and compliance.

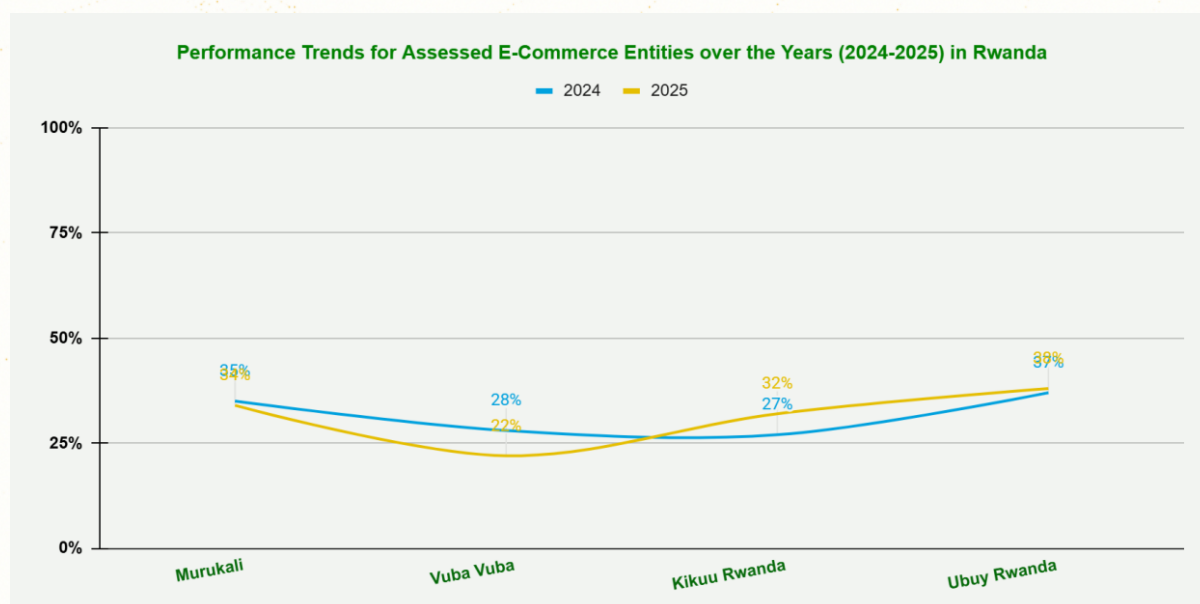
Airtel Uganda demonstrates steady progress, improving from 40% in 2021 to 44% in 2024, and reaching 50% in 2025. The upward trend indicates systematic enhancement of privacy policies, security measures, and governance structures. While the company's performance lags behind MTN Uganda, it reflects deliberate and incremental investment in privacy practices. Airtel Uganda is developing a moderate level of privacy maturity. Continued focus on embedding privacy by design, strengthening technical safeguards, and reinforcing governance is needed to maintain momentum and achieve parity with leading operators.

Roke Telkom shows variable performance, scoring 55% in 2024 but declining to 47% in 2025. This decline suggests challenges in sustaining improvements, potentially due to operational changes, governance lapses, or emerging risks in data protection. The downward movement underscores the need for strengthened oversight, consistent implementation of technical safeguards, and periodic review of privacy frameworks. Roke Telkom demonstrates the potential for high privacy performance but must stabilise its practices to avoid fluctuations that could expose the organisation to regulatory, operational, and reputational risks.

Last year's assessment highlighted MTN Uganda as the most progressive, Lycamobile as declining, and Airtel Uganda as steadily improving. The 2025 data largely confirms these observations while showing that Lycamobile has achieved a substantial recovery and that Roke Telkom's performance has weakened slightly. The data highlights that sustained privacy performance requires consistent governance, institutionalised practices, and proactive monitoring. MTN Uganda stands out as the most mature operator, Airtel Uganda shows steady progress, Lycamobile demonstrates remediation-driven improvement, and Roke Telkom faces volatility. All operators must prioritise embedding privacy by design, strengthening technical safeguards, and ensuring continuous compliance to maintain trust and meet regulatory expectations.

All the companies assessed should prioritise institutionalising privacy governance, embedding privacy by design, strengthening technical safeguards, and maintaining ongoing monitoring to ensure compliance, protect customer data, and enhance stakeholder trust in 2026.

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



The 2024–2025 data for Rwandan e-commerce and telecom operators highlights mixed trends in privacy and data protection maturity. While some companies maintain stable performance, others show declines or moderate improvement, reflecting varying levels of governance, technical safeguards, and regulatory alignment.

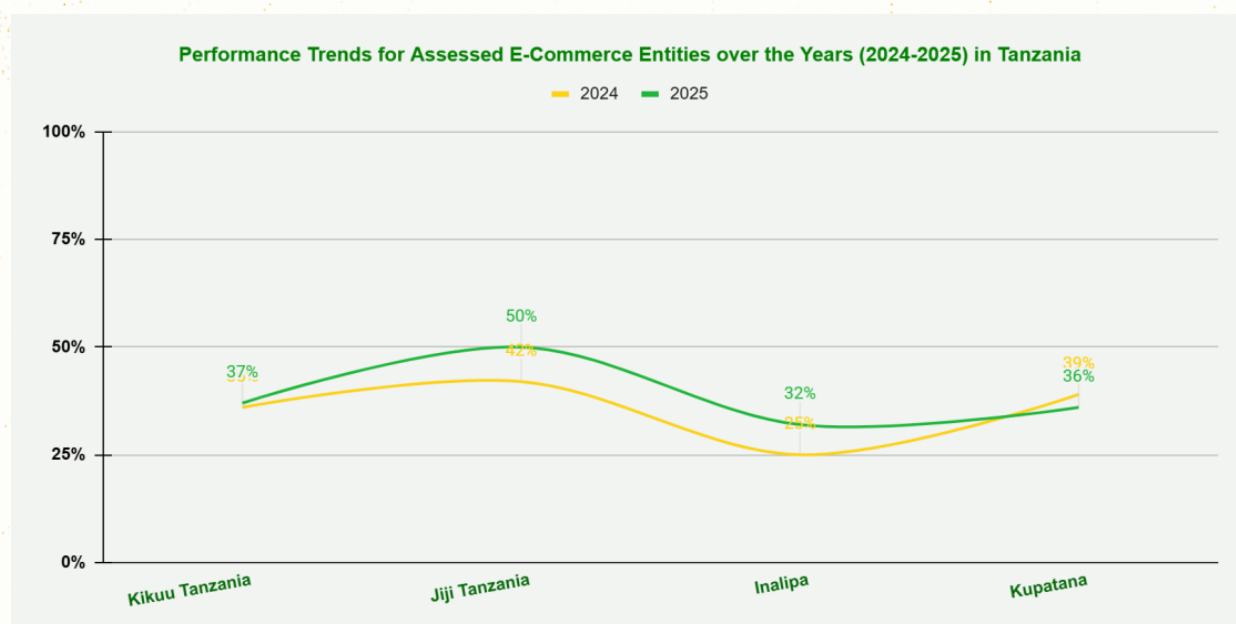
Murukali shows a slight decline from 35% in 2024 to 34% in 2025. This minor drop indicates challenges in maintaining or consistently applying privacy and data protection measures. While some baseline controls are likely in place, governance and operational integration of privacy principles may be limited. Murukali should prioritise strengthening accountability, embedding privacy by design into operational processes, and reinforcing technical safeguards to prevent further decline and reduce regulatory and operational risk.

Vuba Vuba experienced a notable decrease from 28% in 2024 to 22% in 2025. This downward trend suggests emerging gaps in privacy governance, technical controls, and compliance practices. The performance indicates limited maturity and potential vulnerability to data breaches or regulatory scrutiny. Immediate attention is required to implement robust privacy policies, improve data security measures, and establish stronger governance structures to enhance institutional privacy maturity.

Kikuu Rwanda shows moderate improvement, increasing from 27% in 2024 to 32% in 2025. This upward trend suggests that targeted interventions or corrective actions were undertaken to strengthen privacy governance and technical safeguards. However, the overall performance remains at a moderate level, indicating that further institutionalisation of privacy practices is needed. Kikuu Rwanda should continue to embed privacy by design, formalise governance structures, and systematically monitor compliance to sustain and build upon gains.

Ubuy Rwanda maintains a relatively stable performance, increasing slightly from 37% in 2024 to 38% in 2025. The stability indicates ongoing, albeit limited, attention to privacy and data protection practices. While the company shows moderate maturity, incremental improvements suggest a need for more structured governance and consistent application of privacy principles across operations. Ubuy Rwanda should focus on strengthening technical safeguards, enhancing transparency with customers, and embedding privacy into all operational processes to improve long-term compliance and reduce risk exposure.

Among these companies, Ubuy shows the highest and most stable privacy maturity, followed by Kikuu with moderate improvement. Murukali's performance is slightly declining, and Vuba Vuba demonstrates the largest deterioration. Overall, these trends highlight a need for greater governance, accountability, and embedding of privacy by design across the sector to ensure compliance, protect customer data, and mitigate operational and reputational risks.



The data from 2024 to 2025 for Tanzanian e-commerce platforms shows varying degrees of progress in privacy and data protection maturity. The trends indicate differences in governance, technical safeguards, and compliance implementation across companies.

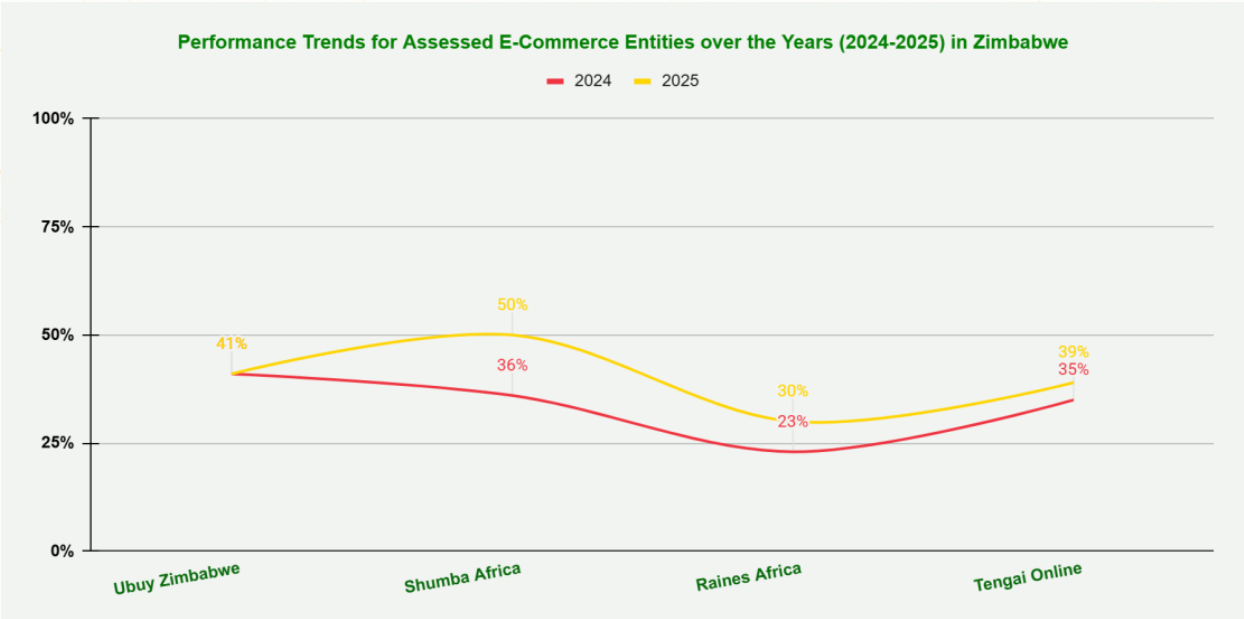
Kikuu Tanzania demonstrates slight improvement from 36% in 2024 to 37% in 2025. The incremental gain suggests modest efforts to strengthen privacy governance and operational safeguards. However, the overall performance remains at a moderate level, indicating that privacy principles may not yet be fully embedded into business processes. Kikuu Tanzania should focus on reinforcing accountability mechanisms, integrating privacy by design into operations, and continuously monitoring compliance to sustain and enhance privacy maturity.

Jiji Tanzania shows a more pronounced improvement from 42% in 2024 to 50% in 2025. This upward trend suggests deliberate interventions to enhance privacy policies, technical safeguards, and regulatory compliance. The improvement reflects growing maturity in managing personal data and aligning with privacy principles. Jiji Tanzania is moving toward stronger privacy maturity. Continued focus on governance, data security, and embedding privacy in system design will be critical to maintain this trajectory and mitigate future risks.

Inalipa experiences a significant increase from 25% in 2024 to 32% in 2025. This improvement indicates that corrective actions were likely implemented to address identified privacy gaps. Despite the progress, the score remains relatively low, suggesting that privacy practices are still at an early stage of maturity. Inalipa must prioritise embedding privacy by design, strengthening technical safeguards, and formalising governance structures to ensure sustainable compliance and reduce operational risk.

Kupatana shows a slight decline from 39% in 2024 to 36% in 2025. The decrease suggests challenges in maintaining previous privacy controls or in adapting them to changing operational and regulatory demands. While some governance and technical measures may be in place, their effectiveness appears inconsistent. Kupatana needs to stabilise privacy governance, reinforce accountability, and enhance security and compliance processes to prevent further decline and strengthen customer trust.

Among Tanzanian e-commerce platforms, Jiji Tanzania demonstrates the strongest improvement and emerging privacy maturity. Kikuu Tanzania shows modest gains, while Inalipa is making progress from a low base. Kupatana exhibits a slight decline, indicating potential gaps in governance and operationalisation of privacy principles. These platforms should prioritise embedding privacy by design, strengthening technical and organisational safeguards, and implementing robust monitoring and governance mechanisms to ensure sustainable data protection practices and compliance with regulatory standards in 2026.



The performance data for Ubuy Zimbabwe, Shumba Africa, Raines Africa, and Tengai Online indicates varying levels of maturity and momentum in complying with data protection laws and embedding effective privacy practices. Overall, the assessment reflects a mix of stabilisation, improvement, and persistent low maturity, underscoring uneven adoption of compliance frameworks and operational safeguards.

Ubuy Zimbabwe maintains a stable performance at 41% in both 2024 and 2025. Last year’s analysis highlighted a slight decline from 46.4% in 2023 to 41% in 2024, raising concerns about the company’s ability to sustain earlier gains. The unchanged score in 2025 suggests that while further deterioration has been avoided, progress has largely plateaued. This stability indicates that Ubuy Zimbabwe has established foundational compliance measures, such as basic privacy policies, data handling procedures, and security controls. However, the absence of improvement suggests limited advancement in strengthening accountability, enhancing transparency, or adapting practices to evolving regulatory expectations. Ubuy Zimbabwe remains relatively better positioned than many peers but risks falling behind if it does not move beyond baseline compliance. To strengthen alignment with data protection laws, the company should prioritise continuous improvement, stronger governance oversight, and deeper integration of privacy by design into its platform and operations.

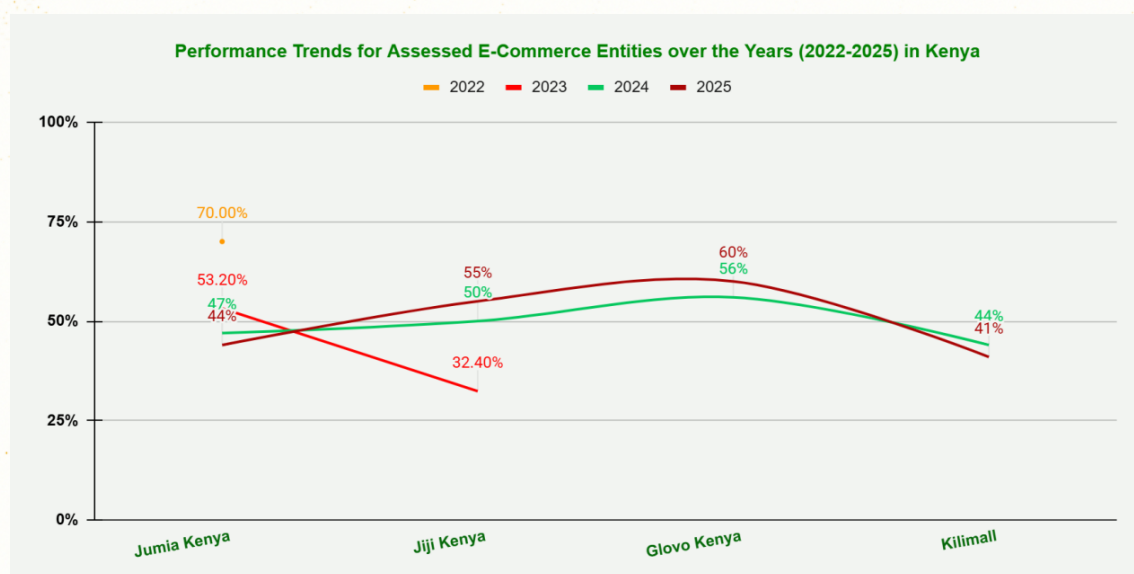
Shumba Africa shows a strong upward trajectory, improving from 36% in 2024 to 50% in 2025. Last year’s analysis correctly identified the 2023–2024 improvement as evidence of focused efforts to address privacy and compliance gaps. The continued growth in 2025 confirms that these efforts have not only been sustained but expanded. The improvement suggests enhanced attention to lawful processing, clearer privacy notices, better data security measures, and more structured compliance processes. While Shumba Africa previously lagged behind Ubuy Zimbabwe, it has now overtaken it, indicating meaningful progress in privacy maturity. Shumba Africa is transitioning from basic compliance toward a more structured privacy framework. To maintain momentum, the company should institutionalise governance mechanisms, formalise accountability, and ensure consistent application of controls as its platform scales.

Raines Africa improves from 23% in 2024 to 30% in 2025. Although the increase is notable, performance remains low in absolute terms. This pattern suggests early-stage remediation efforts, possibly including the introduction of privacy policies or initial security controls, but limited operational maturity. The low score indicates ongoing weaknesses in compliance with data protection laws, particularly in areas such as transparency, data subject rights management, and technical safeguards. Raines Africa faces elevated compliance and operational risk. Without accelerated investment in governance structures, staff awareness, and security controls, the company is likely to struggle to meet regulatory expectations and protect customer data effectively.

Tengai Online demonstrates moderate improvement, increasing from 35% in 2024 to 39% in 2025. This upward trend indicates incremental enhancement of privacy and data protection practices. However, progress remains cautious, sug-

gesting that improvements may be tactical rather than driven by a comprehensive compliance strategy. While some controls and policies may be in place, the overall performance suggests that privacy practices are not yet fully embedded into business processes or platform design. Tengai Online is moving in the right direction but remains vulnerable to compliance gaps. Continued focus on strengthening governance, embedding privacy by design, and improving security controls will be essential to achieving sustainable compliance.

Last year's analysis identified Ubuy Zimbabwe as relatively strong but declining and Shumba Africa as an improving organisation. The 2025 data refines this picture: Ubuy Zimbabwe has stabilised but not advanced, while Shumba Africa has continued to improve and now demonstrates stronger relative maturity. Raines Africa and Tengai Online add further context, highlighting that much of the sector still operates at a low to moderate level of compliance. The Zimbabwe e-commerce sector shows uneven progress in compliance with data protection laws and privacy practices. Shumba Africa emerges as the strongest improver, Ubuy Zimbabwe remains stable but risks stagnation, Tengai Online shows gradual progress, and Raines Africa remains at an early stage of maturity. Across the sector, sustained compliance will depend on moving beyond baseline controls toward embedded governance, stronger accountability, and privacy by design to ensure long-term regulatory alignment and customer trust.



The performance trends across Jumia Kenya, Jiji Kenya, Glovo Kenya, and Kilimall illustrate differing levels of maturity and consistency in complying with data protection laws and embedding privacy practices within e-commerce operations. The results point to a sector characterised by both regression from previously high standards and notable improvement driven by targeted remediation efforts.

Jumia Kenya continues to experience a downward trajectory in performance. After a strong score of 70.0% in 2022, performance declined to 53.2% in 2023, 47% in 2024, and further to 44% in 2025. Last year's analysis identified the decline from 2022 to 2024 as a signal that Jumia was struggling to maintain its earlier high standards of privacy and data protection. The continued decline in 2025 confirms that these challenges persist. While Jumia Kenya still operates at a moderate level of compliance, the trend suggests growing difficulty in sustaining effective governance, consistently applying security controls, or adapting privacy practices to evolving regulatory and operational demands. Jumia Kenya faces an increasing risk of privacy debt, where legacy controls are no longer sufficient. To strengthen compliance, the company must reassess its privacy governance, reinforce accountability, and ensure that privacy by design is consistently applied across its platform and third-party integrations.

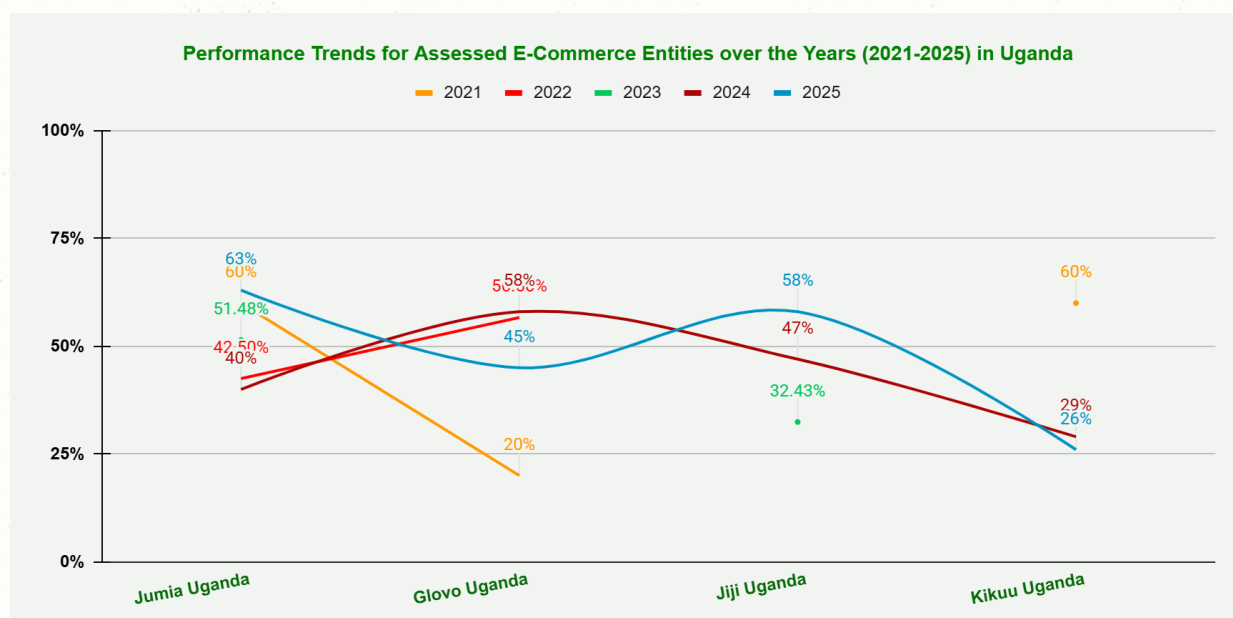
Jiji Kenya demonstrates a strong and sustained improvement. Following a low base of 32.4% in 2023, performance increased to 50% in 2024 and further to 55% in 2025. Last year's analysis correctly characterised the 2024 increase as a significant step forward, and the 2025 results confirm that this improvement has been sustained rather than reversed. This upward trend suggests meaningful progress in aligning with data protection requirements, including clearer privacy notices, better handling of personal data, and strengthened security and compliance processes. Jiji Kenya is transitioning toward a more mature compliance posture. Continued investment in governance structures, monitoring, and embedding privacy by design will be critical to consolidating gains and reducing long-term regulatory and operational risk.

Glovo Kenya shows consistent improvement, increasing from 56% in 2024 to 60% in 2025. Although earlier data is not available, the upward trend indicates strengthening compliance practices and increasing maturity in privacy governance. The relatively high score suggests stronger alignment with data protection laws, particularly in operational controls,

transparency, and security measures, which is especially important given the platform's reliance on real-time location and transactional data. Glovo Kenya is comparatively well positioned within the sector. To sustain this position, it should continue proactive compliance monitoring and ensure that privacy considerations remain embedded in product development and partnerships.

Kilimall records a slight decline from 44% in 2024 to 41% in 2025. This downward movement, while modest, suggests challenges in maintaining existing privacy and compliance controls. The performance indicates moderate maturity but limited progress toward stronger or more comprehensive privacy practices. Kilimall may face growing compliance risk if current controls are not strengthened. Targeted improvements in governance, data security, and accountability will be necessary to stabilise performance and enhance compliance with data protection laws.

Last year's analysis highlighted Jumia Kenya's declining performance and Jiji Kenya's significant improvement. The 2025 data reinforces these conclusions: Jumia's decline has continued, while Jiji has built on its gains. The inclusion of Glovo Kenya and Kilimall provides additional context, showing that while some platforms are progressing toward stronger compliance, others are struggling to maintain or improve their privacy posture. The Kenya e-commerce sector exhibits divergent levels of compliance and privacy maturity. Jiji Kenya and Glovo Kenya show positive and sustained progress, while Jumia Kenya and Kilimall face challenges in maintaining or strengthening their privacy practices. Overall, the data underscores the importance of continuous governance, accountability, and privacy by design to ensure sustained compliance with data protection laws and to maintain consumer trust in an increasingly data-driven market.



The performance of Jumia Uganda, Glovo Uganda, Jiji Uganda, and Kikuu Uganda over the assessment period reflects divergent trajectories in privacy maturity and compliance with data protection laws. The data highlights patterns of recovery, volatility, sustained improvement, and persistent decline across the sector.

Jumia Uganda demonstrates a marked recovery in 2025, improving significantly from 40% in 2024 to 63% in 2025. Last year's analysis identified a concerning decline from 51.48% in 2023 to 40% in 2024, suggesting challenges in maintaining effective privacy and data protection controls. The 2025 rebound indicates that corrective actions were likely implemented to address previously identified gaps. While the improvement is substantial, the historical volatility from 2021, down to 42.5% in 2022, followed by fluctuations through 2024 suggests that privacy practices have not been consistently embedded. Jumia Uganda has demonstrated the capacity to strengthen compliance when prioritised, but sustaining this improvement will require institutionalising governance mechanisms, ensuring continuous monitoring, and embedding privacy by design across platform operations and partnerships.

Glovo Uganda's performance shows variability. After improving from 56.66% in 2022 to 58% in 2024, the score declined to 45% in 2025. Last year's analysis correctly identified Glovo Uganda as showing positive momentum in strengthening privacy practices. The 2025 decline, however, indicates challenges in sustaining these gains.

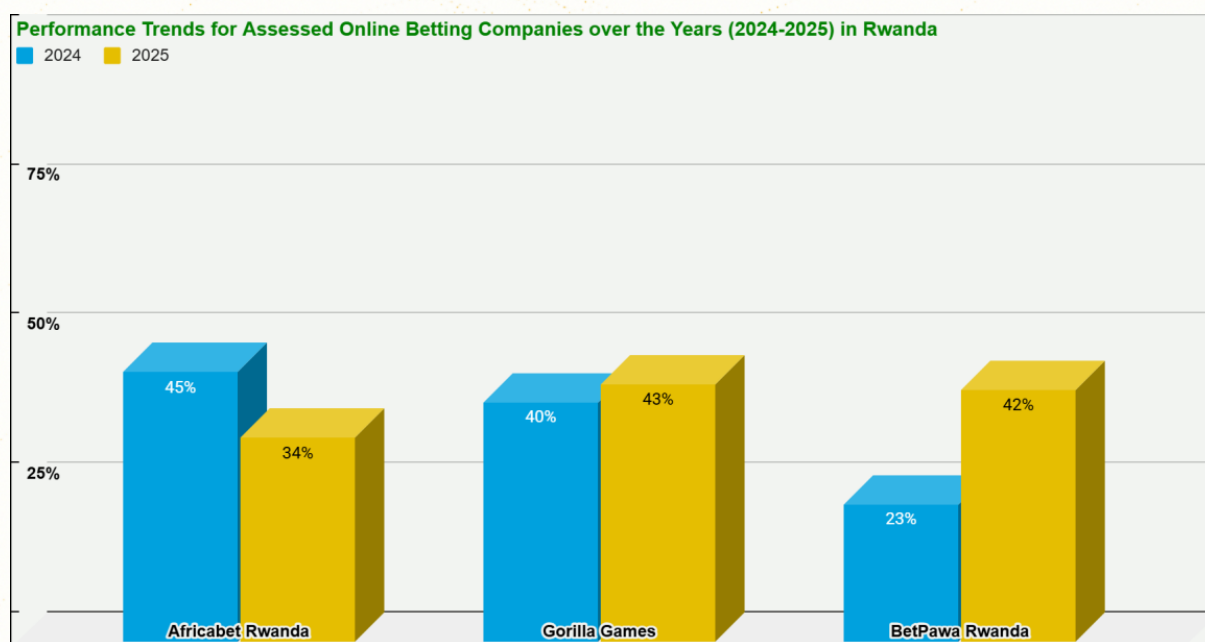
Given Glovo's reliance on location, transactional, and behavioural data, even modest declines in performance can have significant compliance implications. Glovo Uganda faces emerging privacy risk if improvements are not stabilised. The company should reinforce accountability, regularly review security controls, and ensure privacy considerations remain central to operational and technological changes.

Jiji Uganda continues to demonstrate consistent improvement, increasing from 32.43% in 2023 to 47% in 2024 and further to 58% in 2025. Last year's analysis characterised Jiji Uganda as an improving organisation, and the 2025 results confirm that this progress has been sustained. The upward trend indicates strengthening compliance with data protection laws, likely through clearer transparency mechanisms, improved handling of personal data, and enhanced security practices. Jiji Uganda is transitioning toward a more mature privacy posture. Continued focus on embedding privacy by design, strengthening governance, and maintaining compliance oversight will be critical to consolidating gains and mitigating future regulatory risk.

Kikuu Uganda remains the weakest performer in the group, declining further from 29% in 2024 to 26% in 2025. Last year's analysis raised serious concerns following the sharp drop from 60% in 2021 to 29% in 2024. The continued decline in 2025 confirms persistent challenges in maintaining basic privacy and data protection controls. This pattern suggests limited governance, weak technical safeguards, and insufficient alignment with evolving data protection requirements. Kikuu Uganda faces significant compliance, operational, and reputational risk. Urgent intervention is required, including the establishment of basic governance structures, implementation of minimum security safeguards, and alignment with statutory data protection obligations.

Last year's analysis highlighted Glovo Uganda's improvement, Jiji Uganda's positive trajectory, and declines at Jumia Uganda and Kikuu Uganda. The 2025 data refines this picture: Jumia Uganda has staged a strong recovery, Jiji Uganda has continued its upward trend, Glovo Uganda has experienced a setback, and Kikuu Uganda's position has further deteriorated. The Uganda e-commerce sector exhibits high variability in privacy maturity and compliance. Jiji Uganda and Jumia Uganda demonstrate strong recent performance, though with differing levels of historical stability. Glovo Uganda shows moderate maturity but faces sustainability challenges, while Kikuu Uganda remains at high risk due to persistently low performance. Across the sector, sustained compliance with data protection laws will depend on embedding governance, accountability, and privacy by design into core business operations rather than relying on reactive remediation.

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



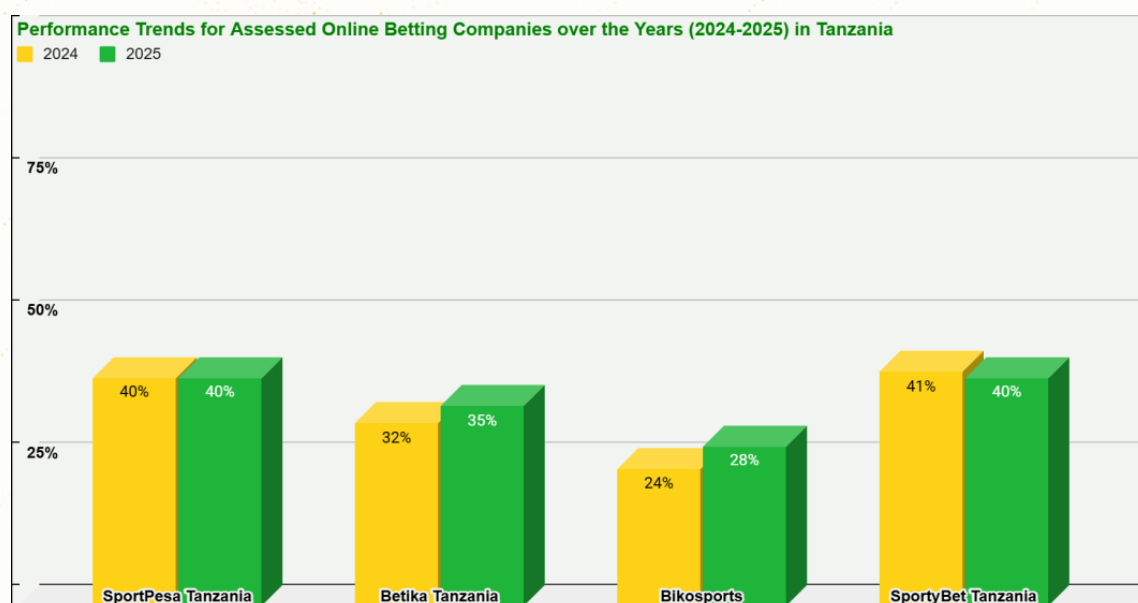
The performance of Africabet Rwanda, Gorilla Games, and BetPawa Rwanda over the assessment period highlights uneven levels of privacy maturity and differing approaches to compliance with data protection laws within the online betting sector. Given the sensitive personal and financial data processed in this sector, these trends have direct implications for regulatory, operational, and reputational risk.

Africabet Rwanda shows a notable decline in performance, dropping from 45% in 2024 to 34% in 2025. The 2024 score suggested a moderate level of privacy capability, with some governance and security controls in place. The subsequent decline indicates challenges in sustaining these measures or adapting them to evolving regulatory and operational requirements. This regression may reflect weaknesses in maintaining lawful processing practices, transparency with users, or consistent enforcement of security controls as the business scales. Africabet Rwanda faces increasing compliance risk. To reverse this trend, the organisation should reinforce governance oversight, ensure regular review and updating of privacy controls, and embed privacy by design into platform changes and customer engagement processes.

Gorilla Games demonstrates moderate improvement, increasing from 40% in 2024 to 43% in 2025. This upward movement suggests incremental strengthening of privacy and data protection practices, potentially through clearer policies, improved transparency mechanisms, or enhanced security controls. While the improvement is positive, the overall score indicates that privacy maturity remains at a developing stage rather than fully embedded across operations. Gorilla Games is moving in a positive direction but should accelerate efforts to formalise accountability structures, strengthen technical safeguards, and ensure continuous compliance monitoring to achieve sustainable alignment with data protection laws.

BetPawa Rwanda records a significant improvement, rising sharply from 23% in 2024 to 42% in 2025. This substantial increase suggests targeted remediation efforts in response to previously identified compliance gaps. Although the improvement meaningfully reduces immediate compliance risk, the scale and speed of change indicate that these enhancements may still be relatively new and not yet fully institutionalised. BetPawa Rwanda has made important progress toward compliance, but long-term sustainability will depend on embedding governance mechanisms, maintaining robust security controls, and integrating privacy by design into core systems and business processes.

Thus, BetPawa Rwanda emerges as the strongest improver, Gorilla Games shows steady but modest progress, and Africabet Rwanda exhibits regression that raises compliance concerns. These trends underscore the uneven maturity of privacy practices across the sector. The findings highlight the need for online betting operators in Rwanda to move beyond reactive compliance and adopt structured, continuous privacy governance. Sustained compliance with data protection laws will require strong accountability, regularly updated technical and organisational safeguards, and the systematic application of privacy by design. Without these measures, operators remain exposed to regulatory enforcement, operational disruption, and erosion of customer trust.



The performance data for SportPesa Tanzania, Betika Tanzania, Bikosports, and SportyBet Tanzania reflects generally low to moderate privacy maturity across the online betting sector, with limited year-on-year movement. The trends suggest that while some operators have established baseline compliance measures, broader institutionalisation of privacy governance remains uneven.

SportPesa Tanzania maintains a stable performance at 40% in both 2024 and 2025. The absence of improvement or decline indicates that the company has implemented basic privacy and data protection controls but has not significantly advanced its compliance posture over the assessment period. The flat trend suggests that existing measures such as privacy policies, basic security controls, and data handling procedures may be in place but are not being strengthened or expanded in response to evolving regulatory and operational requirements. SportPesa Tanzania faces moderate compliance risk. To improve alignment with data protection laws, the company should move beyond baseline controls by strengthening governance oversight, enhancing technical safeguards, and embedding privacy by design into platform development and customer engagement processes.

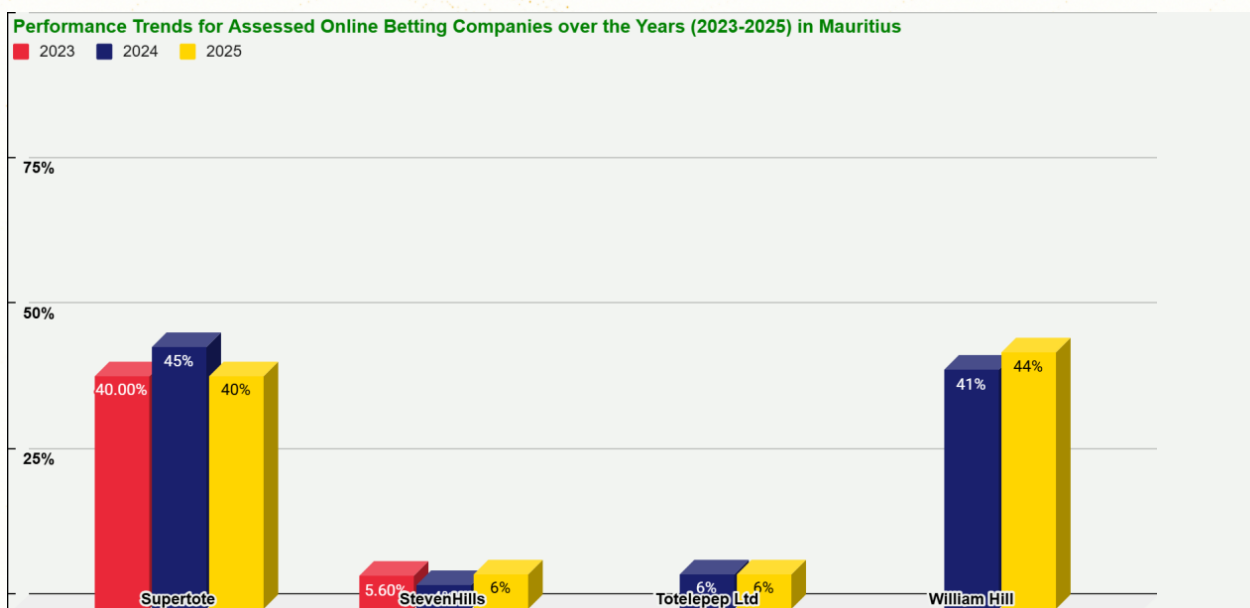
Betika Tanzania shows modest improvement, increasing from 32% in 2024 to 35% in 2025. This upward trend suggests incremental efforts to enhance privacy practices, possibly through improved transparency mechanisms, policy updates, or enhanced security measures. Despite the improvement, overall performance remains relatively low, indicating that privacy and data protection practices are still at an early to mid-stage of maturity. Betika Tanzania is progressing in the

right direction but remains exposed to regulatory and operational risk. Sustained investment in accountability structures, security controls, and continuous compliance monitoring will be necessary to consolidate gains and ensure longer-term compliance.

Bikosports demonstrates a gradual improvement from 24% in 2024 to 28% in 2025. While the increase is positive, the low absolute scores indicate significant gaps in compliance with data protection laws. The performance suggests limited implementation of core privacy principles, including lawful processing, transparency, and data security, raising concerns given the sensitive financial and personal data processed in the betting context. Bikosports faces elevated compliance risk. Urgent attention is required to establish foundational privacy governance, implement minimum technical and organisational safeguards, and align operations with statutory data protection requirements.

SportyBet Tanzania remains relatively stable, recording a slight decline from 41% in 2024 to 40% in 2025. Although the change is marginal, it suggests challenges in sustaining prior improvements or in adapting privacy practices to changing operational demands. The performance indicates moderate maturity but limited progression toward stronger compliance frameworks. SportyBet Tanzania should focus on stabilising and strengthening its privacy controls, improving governance and oversight, and ensuring privacy considerations are systematically integrated into system updates and business processes.

Across the Tanzanian online betting sector, performance remains largely static at low to moderate levels of compliance. SportPesa Tanzania and SportyBet Tanzania demonstrate baseline maturity but limited progression, Betika Tanzania shows modest improvement, and Bikosports remains at an early stage of compliance. The findings underscore the need for betting operators in Tanzania to move beyond basic compliance and adopt more structured, proactive privacy governance. Sustained compliance with data protection laws will require embedding accountability, strengthening technical safeguards, and applying privacy by design across platforms. Without such measures, operators remain exposed to regulatory enforcement, operational disruption, and erosion of customer trust in an increasingly scrutinised and data-intensive sector.



The performance data for Supertote, StevenHills, Totelepep Ltd, and William Hill highlights sharp contrasts in privacy maturity and compliance with data protection laws across the online betting sector. The trends reveal limited progress, persistent low compliance among some operators, and moderate but uneven improvement among others.

Supertote's performance shows moderate fluctuation rather than sustained improvement. After scoring 40% in 2023, the company improved to 45% in 2024, as noted in last year's analysis, before declining back to 40% in 2025. The earlier assessment correctly identified the 2024 increase as a positive but modest step toward improved compliance. The regression in 2025 suggests that the improvements observed in 2024 were not fully institutionalised. This pattern indicates reliance on short-term remediation rather than embedded governance and continuous privacy risk management. Supertote maintains a baseline level of compliance but remains exposed to regulatory and operational risk. To achieve sustainable alignment with data protection laws, the organisation must strengthen accountability structures, maintain up-to-date security controls, and embed privacy by design into core systems and customer interactions.

StevenHills continues to demonstrate persistently poor performance, with scores remaining critically low at 5.6% in 2023, 4% in 2024, and only marginally improving to 6% in 2025. Last year's analysis highlighted significant and systemic gaps in privacy practices, and the 2025 data confirms that these issues remain largely unaddressed. The consistently low

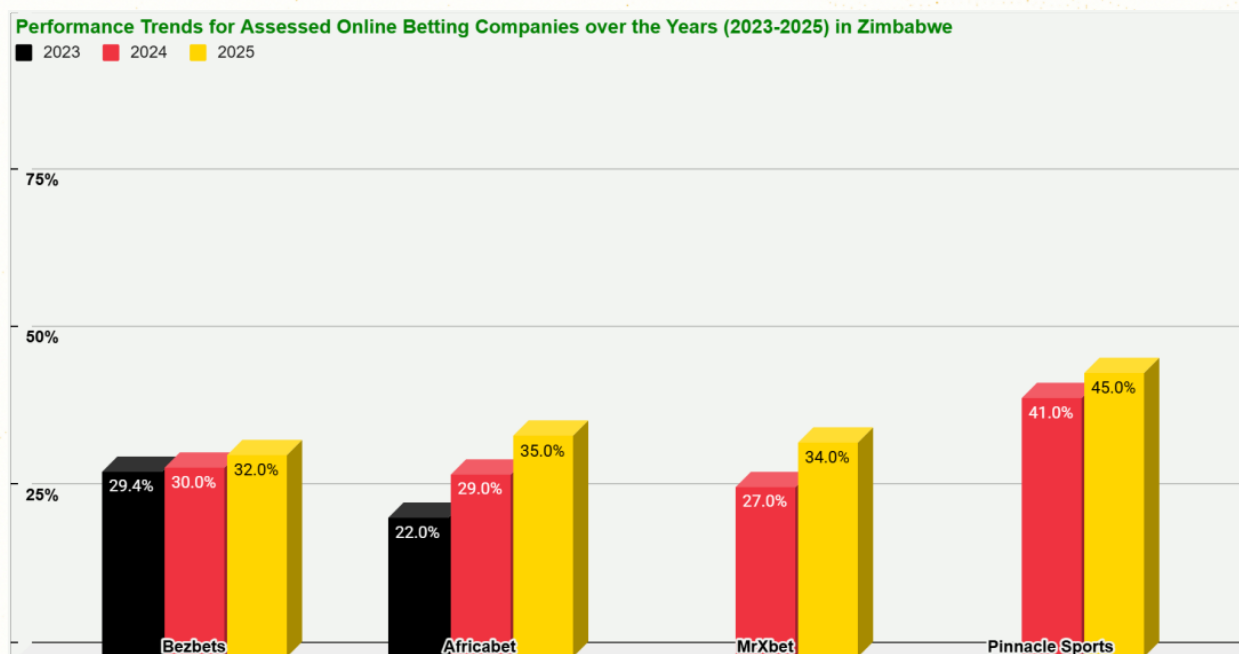
scores indicate minimal compliance with fundamental data protection principles, including lawful processing, transparency, data security, and accountability. StevenHills faces severe regulatory, operational, and reputational risk.

Immediate intervention is required to establish even basic compliance with data protection laws. Without urgent implementation of governance structures and security safeguards, the organisation remains highly vulnerable to enforcement action and data breaches.

Totelepep Ltd records consistently low performance, scoring 6% in both 2024 and 2025. Although historical data for 2023 is unavailable, the flat and extremely low scores indicate negligible progress in establishing privacy and data protection controls. The absence of improvement suggests that privacy compliance is not being prioritised and that foundational requirements, such as clear privacy notices, lawful processing frameworks, and minimum security measures are largely absent. Totelepep Ltd is at an early and high-risk stage of privacy maturity. Urgent investment is required to meet statutory data protection obligations, implement minimum safeguards, and reduce exposure to regulatory sanctions and consumer harm.

William Hill demonstrates moderate and consistent improvement, increasing from 41% in 2024 to 44% in 2025. While earlier data is not available, the upward trend suggests strengthening governance, improved security controls, and better alignment with data protection requirements. Compared to other operators in the sector, William Hill shows relatively stronger privacy maturity, though its performance still indicates room for further enhancement to meet higher industry and regulatory standards. William Hill is comparatively well positioned but must continue to enhance governance oversight, transparency mechanisms, and privacy by design practices to maintain compliance in a highly regulated and data-intensive sector.

Last year's analysis identified Supertote as showing modest improvement and StevenHills as persistently non-compliant. The 2025 data confirms these conclusions: Supertote's gains were not sustained, while StevenHills remains critically weak. The inclusion of Totelepep Ltd reinforces concerns about systemic low compliance in parts of the sector, while William Hill provides evidence that gradual, structured improvement is achievable. The online betting sector continues to exhibit significant disparities in compliance with data protection laws and privacy practices. William Hill and, to a lesser extent, Supertote demonstrate moderate compliance, though sustainability remains a concern. StevenHills and Totelepep Ltd remain at critically low levels of privacy maturity, posing substantial regulatory and reputational risks. Across the sector, long-term compliance will depend on moving beyond reactive measures toward embedded governance, consistent security controls, and privacy by design to protect customer data and meet evolving regulatory expectations.



The performance data for Bezbets, Africabet, MrXbet, and Pinnacle Sports indicates gradual improvement across much of the online betting sector, albeit from a low baseline. While some operators are making incremental progress, overall privacy maturity remains limited, and compliance risks persist due to the sensitive personal and financial data processed in this sector.

Bezbets demonstrates a slow but consistent improvement over the assessment period, increasing from 29.4% in 2023 to 30.0% in 2024 and 32.0% in 2025.

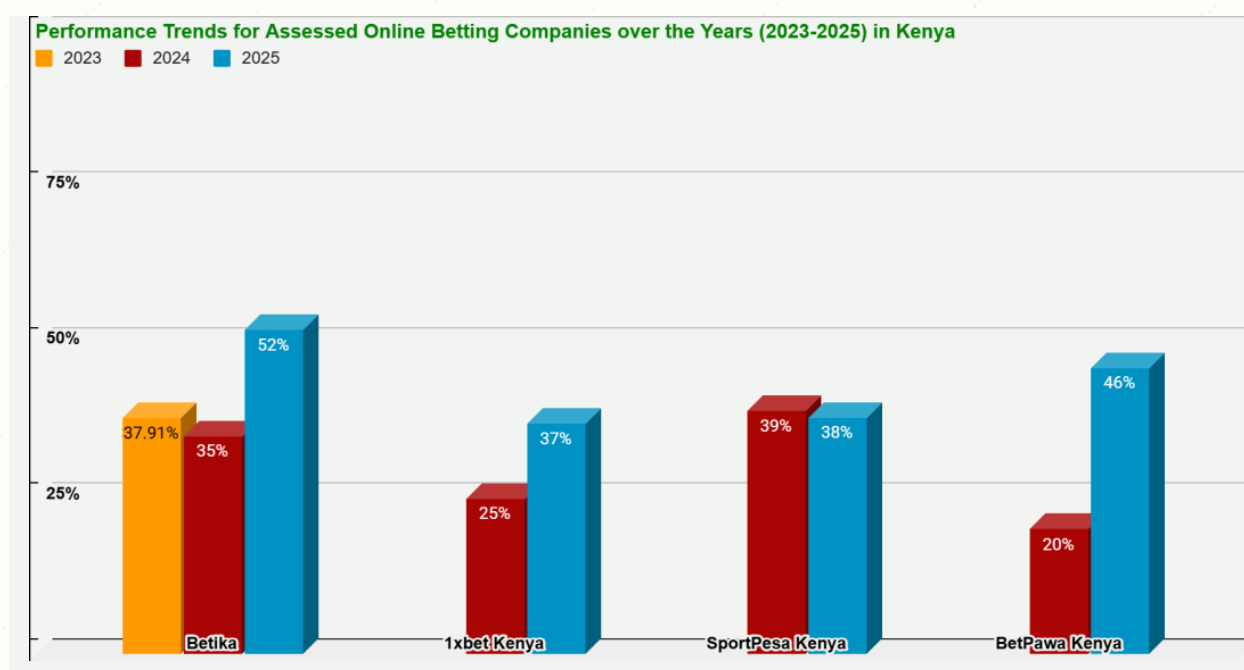
Last year's analysis correctly identified only marginal progress between 2023 and 2024, and the 2025 data confirms that improvement has continued, though at a gradual pace. The trend suggests that Bezbets has begun addressing certain privacy and data protection gaps, possibly through policy updates or basic security enhancements. However, the overall performance remains low, indicating that privacy governance, accountability, and technical safeguards are not yet sufficiently embedded. Bezbets remains exposed to moderate-to-high compliance risk. To move beyond incremental gains, the organisation must invest in structured governance frameworks, strengthen technical and organisational security measures, and ensure continuous compliance monitoring aligned with data protection laws.

Africabet shows a notable improvement from 22.0% in 2023 to 29.0% in 2024 and further to 35.0% in 2025. Last year's analysis highlighted meaningful progress but emphasised that significant gaps remained. The continued improvement in 2025 confirms that Africabet has sustained its remediation efforts. Despite this progress, the absolute score indicates that privacy practices are still developing and may not yet be consistently applied across all operations. Africabet has reduced immediate compliance risk but remains below industry best practice. Sustained improvement will require institutionalising accountability, enhancing transparency, and embedding privacy by design into systems and customer interactions.

MrXbet records an improvement, rising from 27.0% in 2024 to 34.0% in 2025. While earlier data is not available, the magnitude of the increase suggests focused corrective action to strengthen privacy and data protection practices. The improvement likely reflects enhancements in security controls, privacy policies, or compliance processes, though the overall score indicates that maturity remains moderate at best. MrXbet is on a positive trajectory but must ensure that improvements are sustained through formal governance structures, ongoing risk assessments, and consistent operational application of privacy principles.

Pinnacle Sports demonstrates a stronger and most consistent performance in this group, improving from 41.0% in 2024 to 45.0% in 2025. While earlier data is unavailable, the upward trend indicates comparatively higher privacy maturity and more established compliance mechanisms. Despite leading peers, the score suggests that further enhancement is needed to fully align with evolving regulatory expectations and best practices. Pinnacle Sports is comparatively well positioned but should continue strengthening governance oversight, technical safeguards, and privacy by design practices to maintain compliance in a high-risk, data-intensive environment.

Last year's analysis concluded that Bezbets and Africabet had made only modest progress, with both remaining at low levels of compliance. The 2025 data refines this assessment: Bezbets continues to improve slowly, while Africabet has made more meaningful gains. The inclusion of MrXbet and Pinnacle Sports provides additional context, demonstrating that stronger progress is achievable, though not yet widespread across the sector. The online betting sector continues to exhibit incremental but uneven progress in compliance with data protection laws and privacy practices. Pinnacle Sports and Africabet show the strongest upward trajectories, while Bezbets and MrXbet remain at relatively early stages of maturity. Across all operators, long-term compliance will depend on moving beyond ad hoc remediation toward embedded governance, robust security controls, and systematic application of privacy by design to protect customer data and meet regulatory expectations.



The performance of Betika, 1xBet Kenya, SportPesa Kenya, and BetPawa Kenya shows divergent trajectories in privacy maturity and compliance with data protection laws. While some operators have made significant progress in strengthening their privacy practices, others continue to demonstrate volatility or remain at relatively low levels of compliance, reflecting uneven sector-wide maturity.

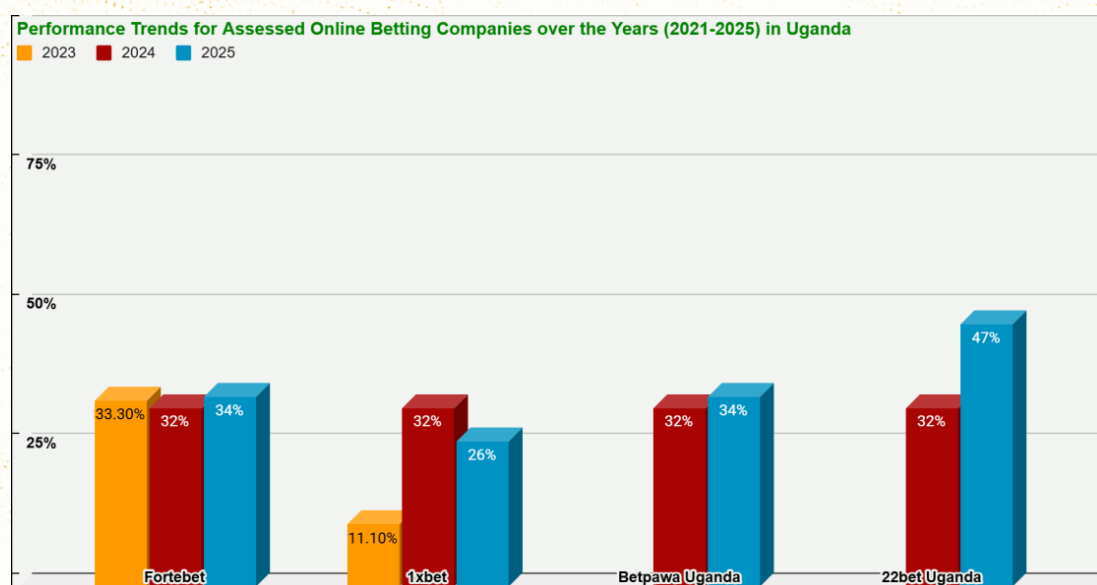
Betika demonstrates a recovery and marked improvement in 2025. After declining slightly from 37.91% in 2023 to 35% in 2024, Betika's score increased significantly to 52% in 2025. Last year's analysis highlighted challenges in maintaining momentum and the need for strengthened data protection measures. The 2025 results indicate that these gaps have been actively addressed. The scale of improvement suggests focused efforts to enhance governance, transparency, and security controls, potentially including clearer privacy notices, improved consent management, and stronger technical safeguards. Betika has materially reduced its compliance risk and is transitioning toward moderate privacy maturity. To sustain this progress, the organisation should continue embedding accountability structures and privacy by design into its platforms and operational processes.

1xBet Kenya shows steady improvement, increasing from 25% in 2024 to 37% in 2025. While earlier data is unavailable, the upward trend indicates ongoing remediation of privacy and data protection gaps. Despite this progress, the overall score suggests that privacy practices remain developing and may not yet be consistently applied across all business operations. 1xBet Kenya is moving in a positive direction but remains exposed to compliance risk. Sustained improvement will depend on formalising governance mechanisms, strengthening security controls, and ensuring continuous compliance monitoring.

SportPesa Kenya exhibits relative stability, with a slight decline from 39% in 2024 to 38% in 2025. While the change is marginal, it suggests challenges in advancing privacy maturity beyond a moderate baseline. The stagnation indicates that existing controls may not be evolving in line with regulatory expectations or operational complexity. SportPesa Kenya faces a risk of compliance stagnation. To avoid regression, the organisation should prioritise periodic review of privacy controls, enhanced governance oversight, and deeper integration of privacy considerations into system updates and customer engagement processes.

BetPawa Kenya demonstrates the significant improvement among the assessed operators, rising sharply from 20% in 2024 to 46% in 2025. This substantial increase suggests targeted remediation efforts to address previously identified compliance gaps. While encouraging, the magnitude of improvement indicates that these measures may still be relatively recent and require sustained institutionalisation. BetPawa Kenya has significantly reduced its immediate compliance risk and is approaching moderate privacy maturity. Continued focus on governance, accountability, and privacy by design will be critical to sustaining compliance with data protection laws.

Last year's analysis focused primarily on Betika, identifying a slight decline and the need for stronger privacy measures. The 2025 data confirms that Betika has responded effectively to these concerns, achieving a substantial improvement. The inclusion of additional operators highlights broader sector trends: while meaningful progress is achievable, as demonstrated by Betika and BetPawa Kenya, sustainability and consistency remain key challenges for others. Overall, there is improvement but uneven compliance with data protection laws. Betika and BetPawa Kenya emerge as strong improvers, while 1xBet Kenya shows steady progress. SportPesa Kenya remains relatively stable but risks stagnation without renewed focus. To achieve sustainable privacy maturity, all operators must move beyond reactive compliance and embed strong governance, robust security safeguards, and privacy-by-design principles across their platforms and business operations.



The performance of Fortebet, 1xBet, BetPawa Uganda, and 22Bet Uganda illustrates divergent levels of privacy maturity across the sector. While some operators demonstrate incremental or significant improvement, others show stagnation or volatility, underscoring uneven compliance with data protection laws in a high-risk, data-intensive environment.

Fortebet's performance remains largely stable but flat, recording 33.30% in 2023, declining slightly to 32% in 2024, and improving marginally to 34% in 2025. Last year's analysis correctly identified limited progress and a lack of meaningful advancement in privacy practices. The 2025 result confirms that Fortebet has maintained baseline controls but has not yet transitioned to a more mature, governance-driven privacy framework. Improvements appear incremental rather than transformative. Fortebet faces ongoing compliance risk due to slow progress. To strengthen alignment with data protection laws, the organisation should prioritise formal governance structures, regular privacy risk assessments, and stronger technical and organisational safeguards.

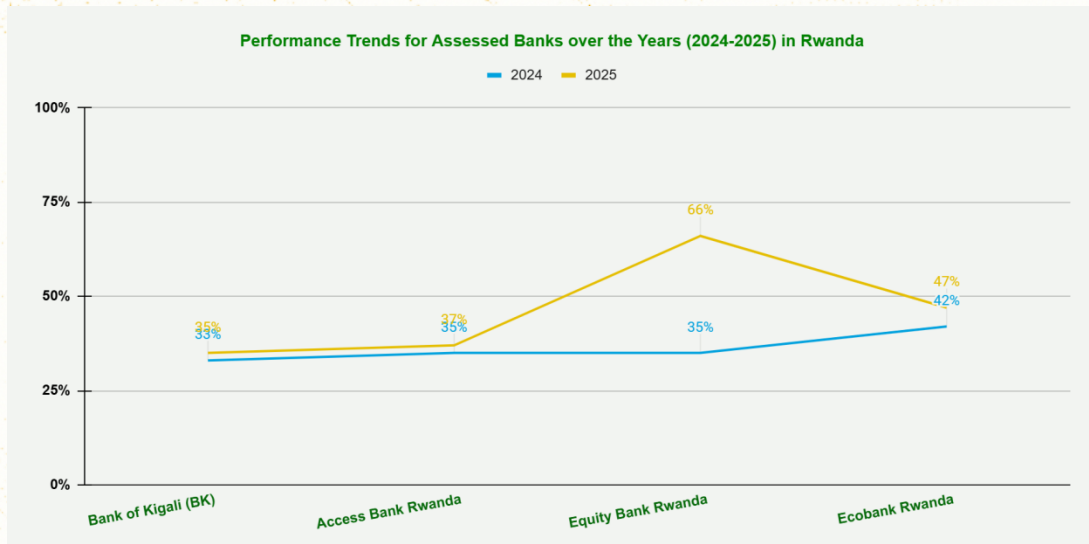
1xBet demonstrates a mixed trajectory. Following a sharp improvement from 11.10% in 2023 to 32% in 2024, the score declined to 26% in 2025. Last year's analysis characterised 1xBet's 2024 performance as a significant improvement, and the 2025 data suggests that these gains were not fully sustained. This regression indicates potential weaknesses in institutionalising privacy controls or maintaining compliance momentum after initial remediation efforts. 1xBet's volatility signals elevated compliance and enforcement risk. The organisation must focus on embedding accountability, ensuring consistent application of privacy controls, and maintaining ongoing compliance oversight rather than relying on short-term corrective actions.

BetPawa Uganda shows steady improvement, increasing from 32% in 2024 to 34% in 2025 (with no earlier data available). While the improvement is modest, it suggests continued effort to strengthen privacy and data protection practices. The trajectory indicates emerging maturity, though overall performance remains at a developing stage. BetPawa Uganda is progressing in the right direction but must accelerate efforts to formalise governance, strengthen security controls, and integrate privacy by design into systems and operational processes to reduce compliance risk.

22Bet Uganda demonstrates the strongest improvement among the assessed operators, increasing significantly from 32% in 2024 to 47% in 2025. This sharp rise suggests targeted and effective remediation of previously identified gaps in privacy governance and data protection controls. While encouraging, the scale of improvement suggests that these measures may still be relatively recent and require sustained oversight to ensure durability. 22Bet Uganda has materially reduced its immediate compliance risk and is approaching moderate privacy maturity. Continued focus on institutionalising controls, governance oversight, and continuous monitoring will be critical to sustaining compliance with data protection laws.

Last year's analysis concluded that Fortebet showed stagnation while 1xBet made substantial progress. The 2025 data refines this assessment: Fortebet remains largely unchanged, while 1xBet's gains have partially reversed, highlighting sustainability challenges. The inclusion of BetPawa Uganda and 22Bet Uganda demonstrates that meaningful progress is achievable when remediation efforts are effectively implemented and prioritised. Overall, the Uganda online betting sector shows uneven progress toward compliance with data protection laws. 22Bet Uganda emerges as the strongest improver, while BetPawa Uganda demonstrates gradual advancement. Fortebet and 1xBet remain exposed to compliance risks due to stagnation and volatility, respectively. To achieve sustainable privacy maturity, operators must move beyond reactive remediation and adopt embedded governance, robust security safeguards, and privacy-by-design principles across their platforms and business operations.

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



The performance of Bank of Kigali (BK), Access Bank Rwanda, Equity Bank Rwanda, and Ecobank Rwanda reflects varying levels of privacy maturity within Rwanda's banking and financial services sector. Given the highly sensitive nature of financial and identity data processed by these institutions, differences in performance have direct implications for regulatory compliance, customer trust, and systemic risk.

Bank of Kigali shows a modest but positive improvement, increasing from 33% in 2024 to 35% in 2025. This gradual progression suggests incremental strengthening of privacy and data protection controls, potentially through policy refinements or limited enhancements to governance and security practices. However, the overall score remains relatively low for a leading national financial institution, indicating that privacy controls may not yet be fully embedded across all systems and processes. BK remains exposed to moderate compliance risk. To align with regulatory expectations and sector best practices, the bank should prioritise stronger governance oversight, regular privacy risk assessments, and deeper integration of privacy by design into digital banking platforms and operational processes.

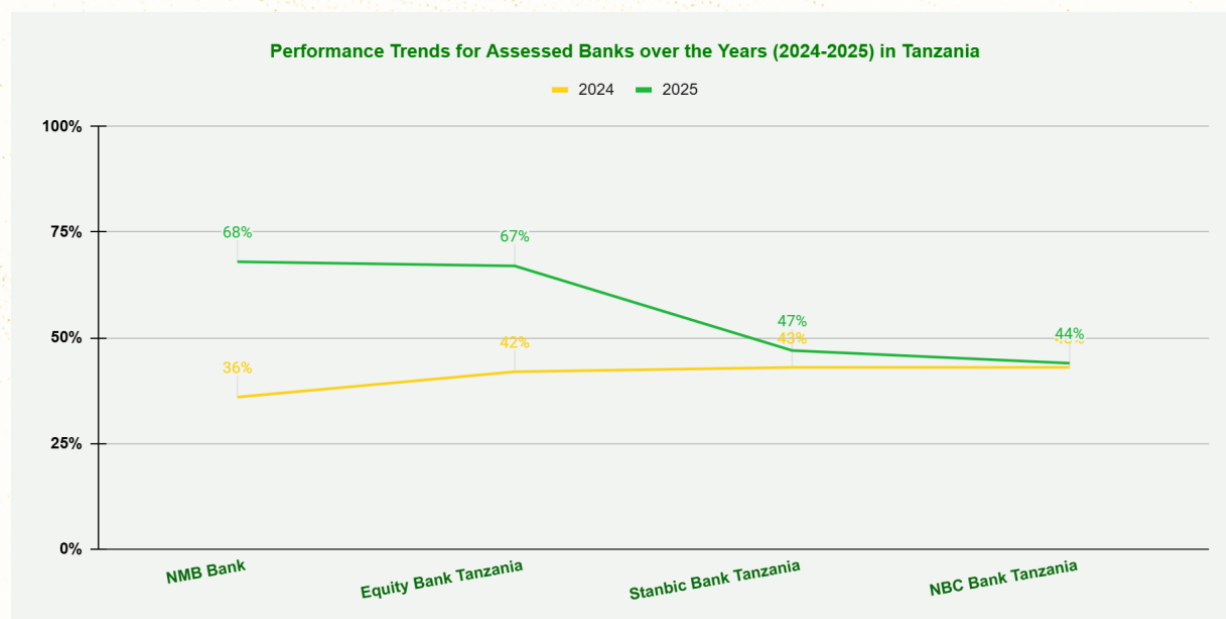
Access Bank Rwanda demonstrates steady improvement, rising from 35% in 2024 to 37% in 2025. While the increase is modest, it indicates continued efforts to address gaps in privacy governance and data protection practices. Despite this progress, the bank's overall performance suggests that privacy maturity is still developing and may rely on reactive compliance measures rather than fully institutionalised controls. Access Bank Rwanda should accelerate its privacy maturity by formalising accountability structures, enhancing technical safeguards, and ensuring consistent implementation of data protection requirements across business units.

Equity Bank Rwanda records a significant improvement, increasing sharply from 35% in 2024 to 66% in 2025. This substantial gain suggests a focused and effective effort to strengthen privacy governance, security controls, and compliance mechanisms. The magnitude of improvement indicates that Equity Bank has likely implemented structured governance frameworks, improved transparency and customer rights management, and enhanced technical and organisational safeguards. Equity Bank Rwanda has materially reduced its compliance risk and now demonstrates comparatively strong privacy maturity within the sector. Continued monitoring, periodic audits, and sustained leadership oversight will be essential to maintaining this level of compliance.

Ecobank Rwanda shows consistent improvement, increasing from 42% in 2024 to 47% in 2025. This upward trend reflects ongoing enhancements to privacy and data protection practices, positioning the bank at a moderate level of maturity relative to peers. While progress is evident, the score suggests that further work is needed to fully embed privacy by design and ensure consistent application across all systems and customer touchpoints. Ecobank Rwanda is on a positive trajectory but should continue strengthening governance, technical safeguards, and cross-border data management practices to meet evolving regulatory and operational demands.

Within the Rwanda banking sector, Equity Bank Rwanda emerges as the clear leader in privacy performance, demonstrating rapid advancement toward stronger compliance with data protection laws. Ecobank Rwanda occupies a middle position with steady progress, while Bank of Kigali and Access Bank Rwanda show slower, incremental improvement and remain at earlier stages of privacy maturity. The findings highlight uneven privacy maturity across Rwanda's banking and financial services sector. While significant progress is achievable as demonstrated by Equity Bank Rwanda other institutions remain exposed to compliance, operational, and reputational risks due to slower adoption of robust pri-

privacy governance. To ensure sustainable compliance with data protection laws, banks must move beyond incremental improvements and embed strong accountability, advanced security controls, and privacy-by-design principles into all digital and operational processes.



The performance of NMB Bank, Equity Bank Tanzania, Stanbic Bank Tanzania, and NBC Bank Tanzania demonstrates varying levels of privacy maturity and markedly different trajectories in strengthening compliance with data protection and privacy requirements. Given the sensitivity of financial, identity, and transactional data handled by banks, these trends are significant indicators of regulatory readiness and institutional resilience.

NMB Bank shows a substantial improvement, increasing sharply from 36% in 2024 to 68% in 2025. This marked progression suggests a deliberate and structured effort to strengthen privacy governance and data protection controls. The scale of improvement indicates that NMB Bank has likely implemented enhanced accountability mechanisms, strengthened security safeguards, and improved management of lawful processing and customer transparency obligations. NMB Bank has significantly reduced its privacy-related compliance risk and now demonstrates comparatively strong alignment with data protection requirements. Sustaining this position will require continued governance oversight, regular audits, and integration of privacy by design into digital banking and system upgrades.

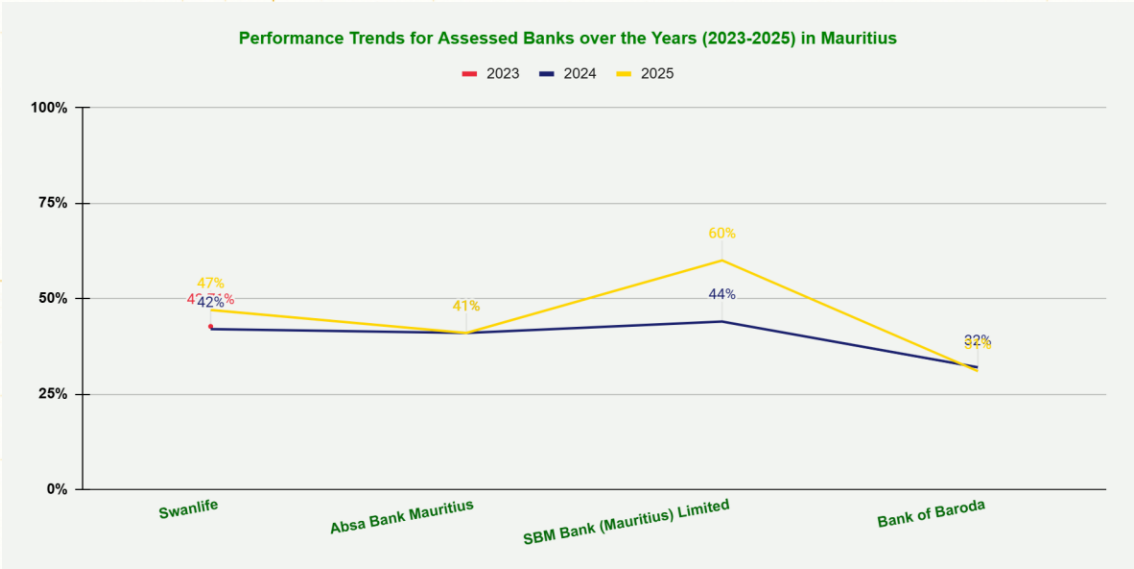
Equity Bank Tanzania also demonstrates strong improvement, rising from 42% in 2024 to 67% in 2025. This trajectory indicates focused investment in privacy and data protection practices, potentially including improved governance structures, clearer privacy notices, and enhanced technical and organisational safeguards. The consistency and scale of improvement suggest that privacy considerations are becoming more embedded in operational and strategic decision-making. Equity Bank Tanzania is approaching a higher level of privacy maturity and is well positioned from a regulatory compliance perspective. Continued attention to cross-border data handling, vendor management, and privacy-by-design implementation will be critical to maintaining this progress.

Stanbic Bank Tanzania shows modest improvement, increasing from 43% in 2024 to 47% in 2025. This incremental change suggests that while foundational privacy controls are in place, progress toward higher maturity is gradual. The relatively moderate score indicates that enhancements may be focused on maintaining baseline compliance rather than advancing toward best practice. Stanbic Bank Tanzania faces moderate compliance risk if progress remains slow. To strengthen its privacy posture, the bank should prioritise stronger governance accountability, regular privacy risk assessments, and deeper integration of privacy controls into operational and digital initiatives.

NBC Bank Tanzania demonstrates minimal improvement, moving marginally from 43% in 2024 to 44% in 2025. This near-static performance suggests challenges in advancing privacy maturity beyond existing controls. While baseline compliance may be maintained, the lack of meaningful progress raises concerns about the bank's ability to adapt to evolving regulatory expectations and technological complexity. NBC Bank Tanzania remains exposed to ongoing compliance and operational risk. Strengthening privacy governance, investing in security enhancements, and embedding privacy by design into system changes will be necessary to avoid stagnation and potential regulatory scrutiny.

Thus, NMB Bank and Equity Bank Tanzania emerge as clear leaders, demonstrating significant advancement in privacy and data protection maturity. Stanbic Bank Tanzania occupies a middle position with gradual improvement, while NBC

Bank Tanzania shows signs of stagnation that warrant closer attention. The findings highlight divergent levels of privacy maturity across Tanzania’s banking sector. While some institutions have demonstrated that rapid and meaningful improvement is achievable, others risk falling behind due to incremental or static progress. Sustainable compliance with data protection laws will require banks to move beyond baseline controls and embed strong governance, robust technical safeguards, and privacy-by-design principles across all systems, products, and customer interactions.



The performance of Swanlife, Absa Bank Mauritius, SBM Bank (Mauritius) Limited, and Bank of Baroda reflects differing levels of privacy maturity and varying trajectories in strengthening compliance with data protection laws. Given the sensitivity of personal, financial, and identity data handled by these institutions, the observed trends have direct implications for regulatory exposure, operational resilience, and customer trust.

Swanlife demonstrates overall stability with gradual improvement. After recording 42.71% in 2023 and 42% in 2024, the score increased to 47% in 2025. Last year’s analysis correctly observed stability and limited progress between 2023 and 2024. The 2025 improvement indicates that Swanlife has begun to strengthen its privacy and data protection practices beyond a maintenance level. This improvement suggests enhanced governance attention, possible refinement of privacy policies, and incremental strengthening of security and compliance controls. Swanlife has reduced its compliance risk and is transitioning toward moderate privacy maturity. Continued focus on embedding privacy by design, strengthening accountability, and regularly reviewing controls will be necessary to sustain this positive trajectory.

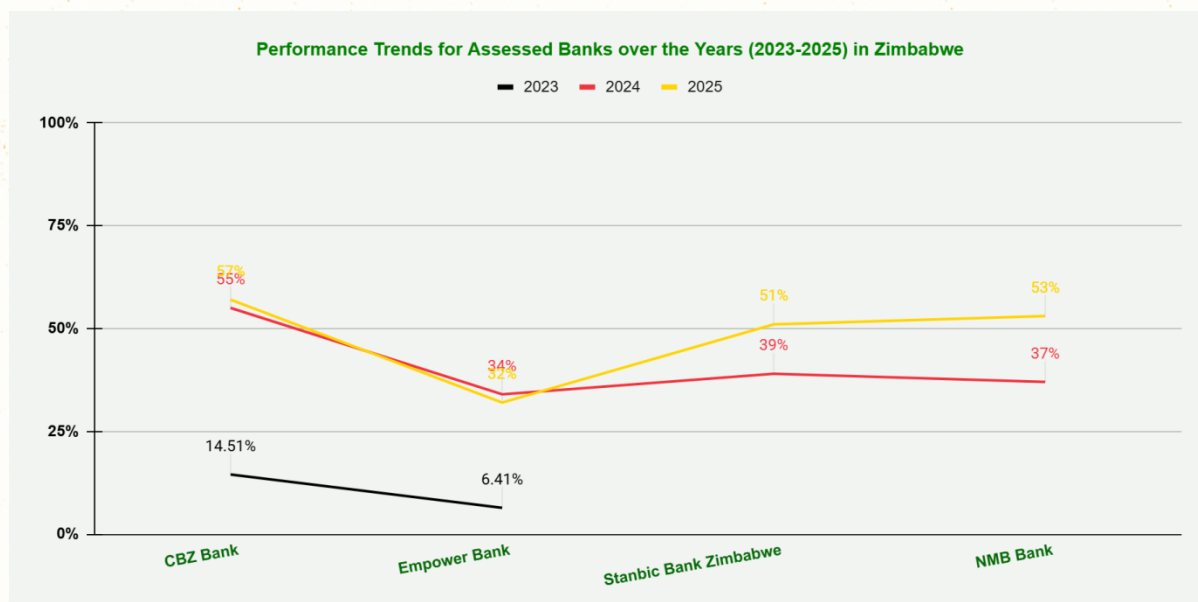
Absa Bank Mauritius shows static performance, maintaining a score of 41% in both 2024 and 2025. While this consistency suggests the presence of baseline privacy and data protection controls, it also indicates limited progress in advancing privacy maturity. The lack of improvement may reflect a focus on maintaining minimum compliance rather than proactively strengthening governance and security frameworks. Absa Bank Mauritius remains exposed to moderate compliance risk. To improve alignment with evolving data protection requirements, the bank should prioritise enhanced governance oversight, periodic privacy risk assessments, and deeper integration of privacy considerations into digital transformation initiatives.

SBM Bank demonstrates a significant improvement, increasing from 44% in 2024 to 60% in 2025. This substantial gain indicates a focused and effective effort to address gaps in privacy governance, security controls, and compliance mechanisms. The scale of improvement suggests stronger accountability structures, improved transparency, and enhanced technical and organisational safeguards. SBM Bank has materially strengthened its compliance posture and now demonstrates comparatively high privacy maturity within the sector. Sustaining this position will require continuous monitoring, staff awareness, and ongoing alignment with regulatory developments.

Bank of Baroda shows slight regression, decreasing marginally from 32% in 2024 to 31% in 2025. While the change is small, it suggests challenges in maintaining or evolving existing privacy controls. The persistently low score indicates that privacy practices remain underdeveloped relative to sector peers. Bank of Baroda faces elevated compliance and operational risk. Targeted intervention is needed to strengthen governance, improve security measures, and formalise privacy management processes to achieve baseline compliance and reduce exposure.

Last year’s analysis focused on Swanlife’s stable performance and limited improvement between 2023 and 2024. The 2025 data confirms this assessment while also demonstrating that Swanlife has since made measurable progress.

The inclusion of other institutions highlights a broader sectoral picture, with SBM Bank showing that significant advancement is achievable, while Absa Bank Mauritius and Bank of Baroda illustrate the risks of stagnation or regression. The Mauritius financial services sector exhibits uneven privacy maturity, ranging from strong improvement to stagnation and slight decline. SBM Bank (Mauritius) Limited emerges as the sector leader in advancing compliance with data protection laws, while Swanlife shows positive momentum. Absa Bank Mauritius and Bank of Baroda face ongoing compliance risks due to static or declining performance. To ensure sustainable compliance and maintain customer trust, financial institutions must move beyond maintaining baseline controls and embed robust governance, advanced security safeguards, and privacy-by-design principles across all operations.



The performance of CBZ Bank, Empower Bank, and Stanbic Bank Zimbabwe over the assessment period highlights differing levels of privacy maturity and varying trajectories in strengthening compliance with data protection and privacy requirements. Given the sensitivity of financial and identity data processed by banks, these trends are strong indicators of regulatory readiness and operational resilience.

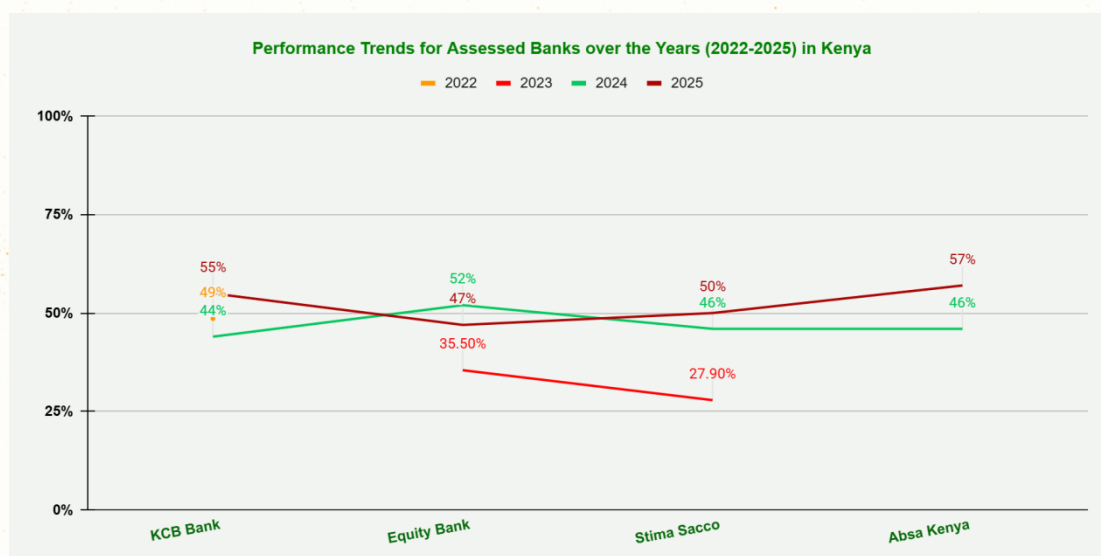
CBZ Bank demonstrates sustained and significant improvement across the period. After recording a low baseline of 14.51% in 2023, the bank increased sharply to 55% in 2024 and further improved to 57% in 2025. Last year's analysis correctly identified the 2024 result as a substantial leap in privacy and data protection maturity. The 2025 data confirms that these gains have been maintained and marginally strengthened. This trajectory suggests that CBZ Bank has moved beyond one-off remediation and is beginning to embed privacy governance, accountability mechanisms, and stronger security controls into its operations. CBZ Bank has materially reduced its compliance risk and now demonstrates moderate to strong alignment with data protection laws. Continued investment in governance oversight, privacy by design, and regular compliance assurance will be necessary to sustain and further enhance this position.

Empower Bank shows mixed performance. The bank improved significantly from 6.41% in 2023 to 34% in 2024, reflecting initial efforts to address major privacy and compliance gaps. However, the score declined slightly to 32% in 2025, indicating challenges in sustaining momentum or institutionalising controls. Last year's analysis noted progress but emphasised the bank's low overall maturity. The 2025 results reinforce this assessment, suggesting that improvements may have been reactive rather than fully embedded. Empower Bank remains exposed to elevated compliance and operational risk. To progress meaningfully, the bank must strengthen governance structures, formalise accountability, and invest in consistent application and monitoring of privacy and security controls across its operations.

Stanbic Bank Zimbabwe demonstrates strong and consistent improvement, increasing from 39% in 2024 to 51% in 2025 (with no 2023 data available). The upward trend suggests focused efforts to enhance privacy governance, security safeguards, and compliance practices. The scale of improvement indicates movement toward a more mature and structured privacy framework, though further advancement is needed to reach higher benchmarks. Stanbic Bank Zimbabwe has reduced its compliance risk and is progressing toward stronger privacy maturity. Continued emphasis on privacy by design, staff awareness, and ongoing compliance monitoring will be essential to sustain this positive trajectory.

Last year's analysis highlighted CBZ Bank's dramatic improvement and Empower Bank's initial progress from a very low baseline. The 2025 data confirms CBZ Bank's continued upward trajectory and reveals sustainability challenges for Empower Bank. The inclusion of Stanbic Bank Zimbabwe provides additional context, demonstrating that consistent

and structured improvement is achievable within the sector. Overall, the trends show meaningful but uneven progress in compliance with data protection laws and privacy practices. CBZ Bank emerges as the strongest performer with sustained improvement, while Stanbic Bank Zimbabwe shows solid upward momentum. Empower Bank, despite initial gains, remains at an early stage of privacy maturity and faces continued compliance risk. To ensure sustainable compliance and maintain customer trust, banks must move beyond reactive remediation and embed strong governance, robust security controls, and privacy-by-design principles across all operations.



The performance of KCB Bank, Equity Bank, Stima Sacco, and Absa Kenya over the past few years demonstrates a mix of improvement, recovery, and short-term fluctuations, reflecting differing levels of maturity in data protection practices and compliance with privacy regulations.

KCB Bank's score improved to 55% in 2025, up from 44% in 2024 and 49% in 2022, reflecting a significant recovery from the slight dip observed in 2024. Last year's analysis highlighted a minor decline and the need for stronger consistency in privacy measures. The 2025 results show that the bank has strengthened its data protection frameworks, implemented more robust controls, and responded effectively to regulatory and operational gaps. KCB Bank is demonstrating a clear commitment to safeguarding customer data and aligning with data protection laws. To maintain this momentum, the bank should continue enhancing governance, monitoring compliance, and integrating privacy-by-design into digital services.

Equity Bank scored 47% in 2025, a decrease from 52% in 2024, but still above 35.5% in 2023, indicating that while the bank has faced a slight short-term decline, it remains on an upward trajectory compared to historical performance. Last year, the bank was recognized for significant improvement in privacy practices. Equity Bank's slight dip may reflect transitional challenges in implementing new privacy frameworks or addressing emerging regulatory requirements. The bank should focus on consolidating gains, reinforcing compliance protocols, and ensuring continuous monitoring of data protection practices to prevent future declines.

Stima Sacco recorded 50% in 2025, improving from 46% in 2024 and 28% in 2023. This reflects a sustained upward trend in enhancing privacy compliance.

Last year's analysis highlighted meaningful improvements, and the current data confirms continued progress. Stima Sacco's consistent improvement demonstrates a growing institutional commitment to data protection. Continued investments in staff training, security infrastructure, and regular privacy audits will be critical for sustaining and further advancing its compliance maturity.

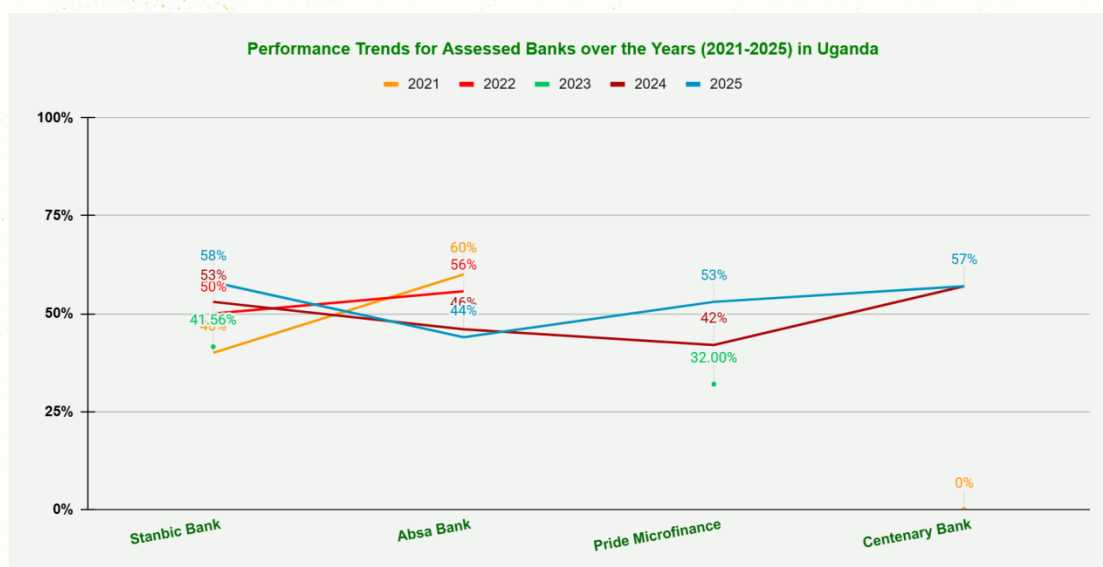
Absa Kenya shows a strong upward trend, moving from 46% in 2024 to 57% in 2025, recovering from historical fluctuations and aligning closely with top-performing peers. This is the first year Absa Kenya is included in this dataset, providing a benchmark for privacy maturity in the sector. The notable improvement indicates that Absa Kenya has made significant strides in addressing gaps in its privacy frameworks, implementing stronger security measures, and complying with regulatory requirements. Maintaining this trajectory will require ongoing monitoring, governance, and integration of data protection into business processes.

Overall, the data shows that all four institutions are improving or recovering from previous declines, with varying rates of progress:

- KCB Bank – strong recovery and increasing compliance maturity.
- Equity Bank – slight short-term decline but overall better than historical performance.
- Stima Sacco – sustained and steady improvement.
- Absa Kenya – rapid and significant improvement, demonstrating strong commitment to privacy practices.

The overall trend in the sector suggests growing awareness of data protection obligations and an increasing alignment with privacy regulations. Institutions that maintain and enhance governance frameworks, invest in security infrastructure, and adopt privacy-by-design principles will likely see continued improvements, reducing regulatory risk and increasing customer trust.

The performance of Stanbic Bank, Absa Bank, Pride Microfinance, and Centenary Bank from Uganda over the assessment period reflects varying levels of privacy maturity and differing abilities to sustain compliance with data protection laws. The data shows a mix of long-term improvement, short-term volatility, and stabilisation at moderate levels of maturity, with direct implications for regulatory exposure and customer trust.



Stanbic Bank demonstrates a clear and sustained upward trajectory. After recording 41.56% in 2023, the bank improved to 53% in 2024 and further to 58% in 2025. Although performance declined from 50% in 2022 to 41.56% in 2023, the subsequent recovery confirms that the bank has taken deliberate steps to strengthen its privacy and data protection practices. Last year's analysis identified Stanbic Bank as improving but still consolidating its gains. The 2025 results confirm that these improvements have been sustained and further embedded. Stanbic Bank has significantly reduced its compliance risk and is approaching a mature level of alignment with data protection requirements. Continued governance oversight, regular privacy risk assessments, and integration of privacy by design into digital banking initiatives will be critical to maintaining this trajectory.

Absa Bank's performance reflects long-term decline followed by stabilisation. After strong results in 2021 (60%) and 2022 (55.70%), the score declined to 46% in 2024 and further to 44% in 2025. Last year's analysis highlighted a drop from earlier high performance while noting that Absa Bank remained at a moderate level of compliance.

The 2025 results confirm that while the decline has slowed, the bank has not yet regained its earlier level of privacy maturity. Absa Bank faces moderate compliance risk due to performance erosion over time. To reverse this trend, the bank should focus on refreshing governance frameworks, strengthening accountability, and ensuring that privacy controls evolve alongside digital transformation and regulatory change.

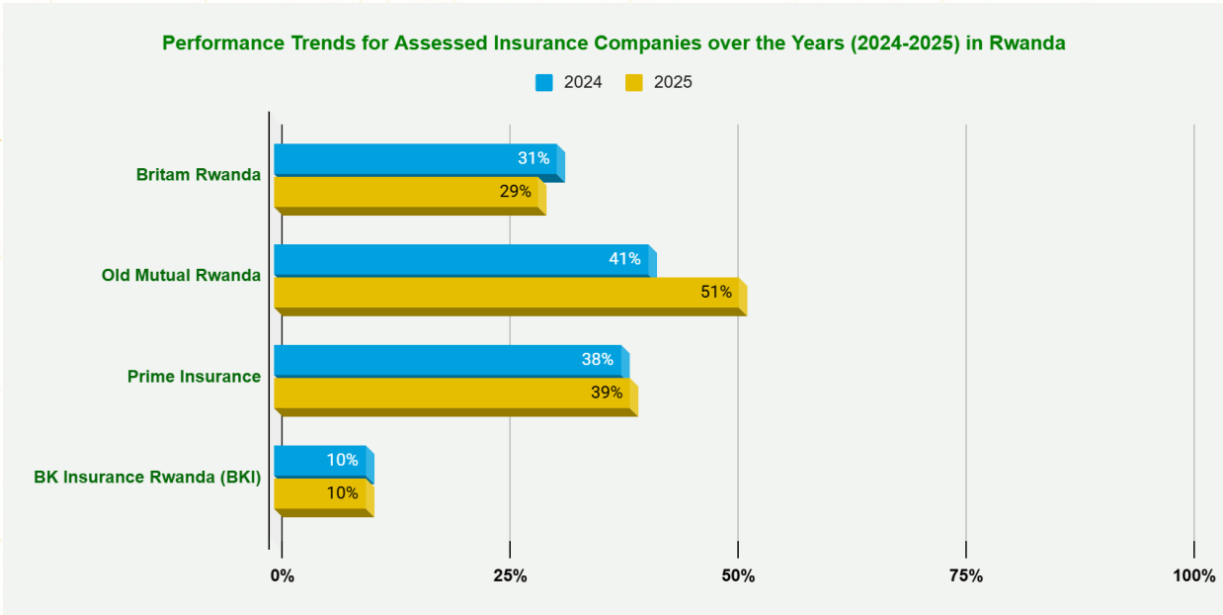
Pride Microfinance shows consistent improvement, rising from 32% in 2023 to 42% in 2024 and further to 53% in 2025. Last year's analysis correctly identified early progress, and the 2025 data confirms that this improvement has continued rather than plateaued. The steady upward trend suggests increasing institutional commitment to privacy governance and improved implementation of security and compliance measures. Pride Microfinance has materially reduced its compli-

ance risk and is transitioning toward moderate-to-strong privacy maturity. Sustaining this progress will require continued investment in governance, staff awareness, and privacy-by-design practices, particularly as digital services expand.

Centenary Bank demonstrates high performance and stability. After a dramatic improvement from 0% in 2021 to 57% in 2024, the bank maintained this level in 2025. Last year’s analysis highlighted Centenary Bank as the strongest improver, and the 2025 results confirm that these gains have been sustained. The ability to maintain performance at this level suggests that privacy and data protection controls are increasingly embedded into governance and operational processes. Centenary Bank currently demonstrates relatively strong alignment with data protection laws. Ongoing assurance, periodic reviews, and adaptation to regulatory developments will be essential to maintaining this position and avoiding regression.

Last year’s analysis highlighted Centenary Bank’s dramatic improvement, Stanbic Bank’s upward momentum, Pride Microfinance’s emerging progress, and Absa Bank’s decline from earlier highs. The 2025 data validates these conclusions, showing that Centenary Bank has sustained its gains, Stanbic Bank has continued to improve, Pride Microfinance has strengthened its position, and Absa Bank has stabilised but not yet recovered its former performance. Overall, the banking and finance sector shows meaningful but uneven progress in compliance with data protection laws and privacy practices. Centenary Bank and Stanbic Bank demonstrate relatively strong and sustained performance, while Pride Microfinance shows encouraging upward momentum. Absa Bank, although still at a moderate level, faces a risk of long-term erosion if improvements are not prioritised. To ensure sustainable compliance and maintain customer trust, all institutions must continue embedding robust governance, strong security safeguards, and privacy-by-design principles across their operations.

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



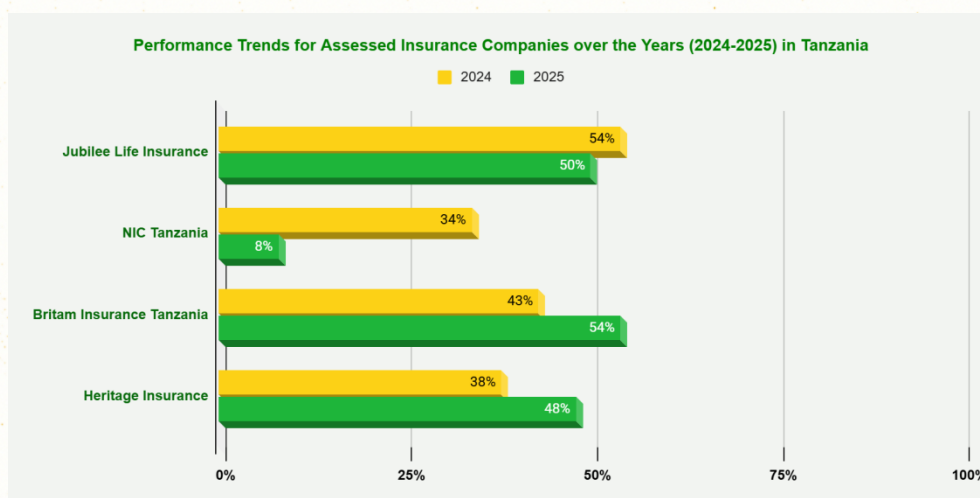
The performance of insurance companies in Rwanda in adhering to data protection and privacy standards shows marked differences across the sector between 2024 and 2025. Old Mutual Rwanda exhibited a significant improvement, rising from 41% in 2024 to 51% in 2025. This increase reflects strengthened privacy practices, likely driven by enhanced compliance frameworks, systematic data protection policies, and focused employee training. The improvement indicates a proactive approach to managing sensitive customer data and aligning with regulatory requirements.

Prime Insurance experienced a slight increase, moving from 38% to 39%. While this suggests incremental progress in privacy compliance, the modest improvement points to the need for ongoing efforts to enhance processes, monitor adherence, and close potential gaps in data protection.

In contrast, Britam Rwanda saw a decline from 31% to 29%, signaling potential weaknesses or challenges in maintaining robust privacy controls. This reduction could be due to outdated practices, insufficient monitoring, or limited resources dedicated to compliance, which raises concerns about exposure to regulatory risks and reputational impact.

BK Insurance Rwanda (BKI) maintained a low performance of 10% across both years. This stagnation highlights persistent gaps in privacy and data protection practices, indicating a high risk of non-compliance and the need for urgent intervention to establish effective data governance and safeguard customer information.

Overall, the data reveals uneven performance across the insurance sector, with some companies making substantial progress while others lag behind. These trends underscore the critical importance of continuous investment in privacy frameworks, regular audits, staff training, and regulatory alignment. Companies that fail to improve may face heightened regulatory scrutiny, increased risk of data breaches, and diminished customer trust, while those demonstrating proactive compliance are better positioned to maintain credibility and operational resilience in the evolving data protection landscape.



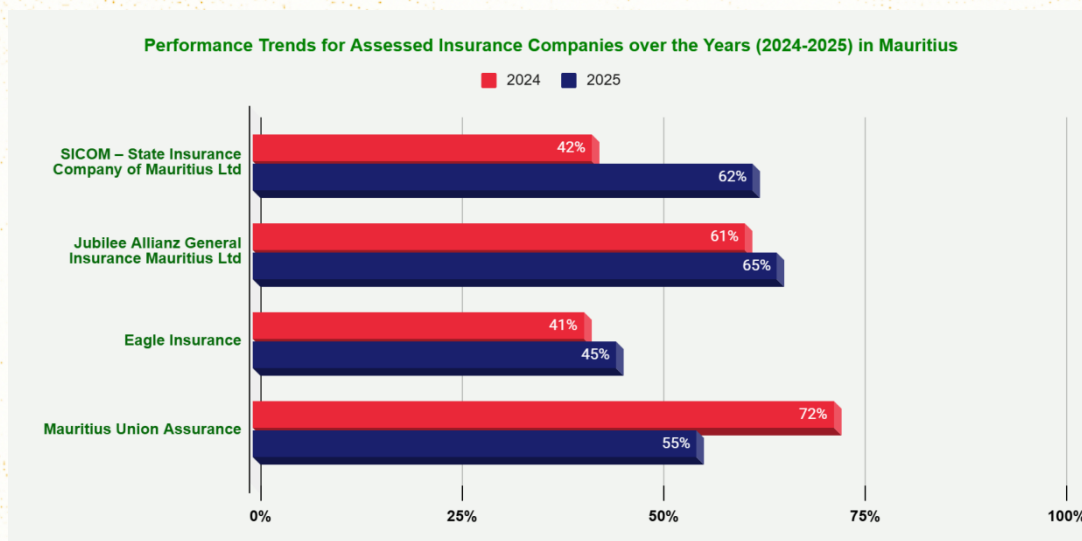
An assessment of data protection and privacy compliance performance among selected insurance companies in Tanzania reveals notable variations in progress and maturity between 2024 and 2025. Jubilee Life Insurance recorded a decline in performance, decreasing from 54% in 2024 to 50% in 2025. Although the company continues to demonstrate relatively strong compliance compared to some peers, the downward trend suggests challenges in sustaining established privacy controls. This may point to gaps in ongoing monitoring, evolving regulatory requirements, or the need to refresh internal data protection policies and staff awareness programs.

NIC Tanzania experienced a significant drop, from 34% in 2024 to 8% in 2025. This sharp decline indicates serious weaknesses in data protection and privacy practices and raises concerns regarding regulatory compliance and data governance. The results suggest potential lapses in implementing privacy controls, insufficient oversight, or failure to adapt to heightened data protection expectations, exposing the company to elevated legal, operational, and reputational risks.

In contrast, Britam Insurance Tanzania demonstrated substantial improvement, increasing from 43% in 2024 to 54% in 2025. This positive trajectory reflects strengthened compliance efforts, likely driven by improved data governance structures, enhanced security measures, and greater organizational awareness of privacy obligations. The improvement positions the company more favorably in managing sensitive customer data and aligning with data protection regulations.

Heritage Insurance also showed notable progress, rising from 38% to 48% over the same period. This improvement suggests deliberate efforts to address prior gaps in privacy compliance, potentially through policy updates, staff training, and better implementation of privacy-by-design principles. While progress is evident, further improvements are required to reach higher compliance maturity.

Overall, the data highlights uneven compliance maturity across the insurance sector. Companies showing improvement demonstrate the benefits of sustained investment in data protection frameworks and governance, while declining or low performance underscores the risks associated with inadequate compliance mechanisms. These trends emphasize the importance of continuous monitoring, regulatory alignment, and institutional commitment to data protection and privacy. Failure to maintain or improve compliance may result in increased regulatory scrutiny, exposure to data breaches, and erosion of customer trust, whereas consistent improvement enhances operational resilience and stakeholder confidence.



An assessment of data protection and privacy compliance performance among selected insurance companies in Mauritius indicates both progress and regression across the sector between 2024 and 2025.

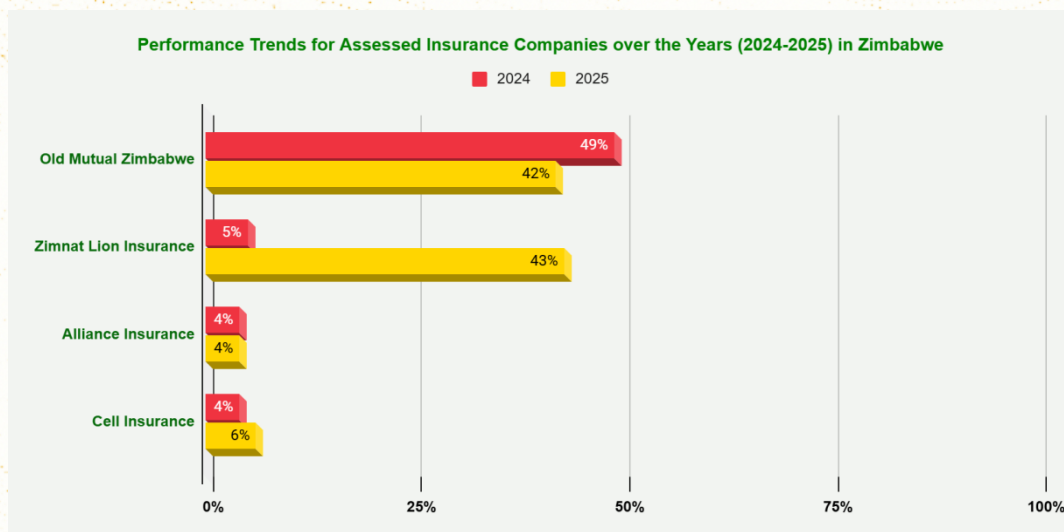
State Insurance Company of Mauritius Ltd (SICOM) demonstrated a substantial improvement in compliance performance, increasing from 42% in 2024 to 62% in 2025. This significant rise suggests strengthened data governance arrangements, improved implementation of privacy controls, and greater alignment with regulatory requirements under Mauritius' data protection framework. The improvement reflects a more proactive approach to managing personal and sensitive data and reducing compliance risks.

Jubilee Allianz General Insurance Mauritius Ltd maintained a consistently high level of performance, improving slightly from 61% in 2024 to 65% in 2025. This steady upward trend indicates a relatively mature data protection and privacy program, characterized by effective policies, ongoing compliance monitoring, and institutionalized privacy practices. The company appears well positioned to manage regulatory obligations and protect customer data effectively.

Eagle Insurance recorded a modest improvement, rising from 41% to 45%. While this progress indicates incremental strengthening of privacy practices, the overall performance remains moderate. This suggests that although foundational controls may be in place, further efforts are required to enhance compliance maturity, particularly in areas such as risk assessments, staff awareness, and incident response readiness.

In contrast, Mauritius Union Assurance (MUA) experienced a notable decline, falling from 72% in 2024 to 55% in 2025. Despite remaining above the mid-range, the decrease signals potential challenges in sustaining previously strong compliance standards. This decline may reflect gaps in ongoing monitoring, evolving regulatory expectations, or resource constraints affecting the consistency of data protection practices.

Overall, the data reveals uneven progress across the Mauritian insurance sector. Companies demonstrating improvement highlight the positive impact of sustained investment in privacy governance, compliance oversight, and organizational awareness. Conversely, declining performance underscores the importance of continuous reinforcement of data protection controls to prevent regression. These trends reinforce the need for insurers to embed privacy as a core operational priority, conduct regular compliance reviews, and adapt proactively to regulatory and technological developments to safeguard customer trust and minimize legal and reputational risks.



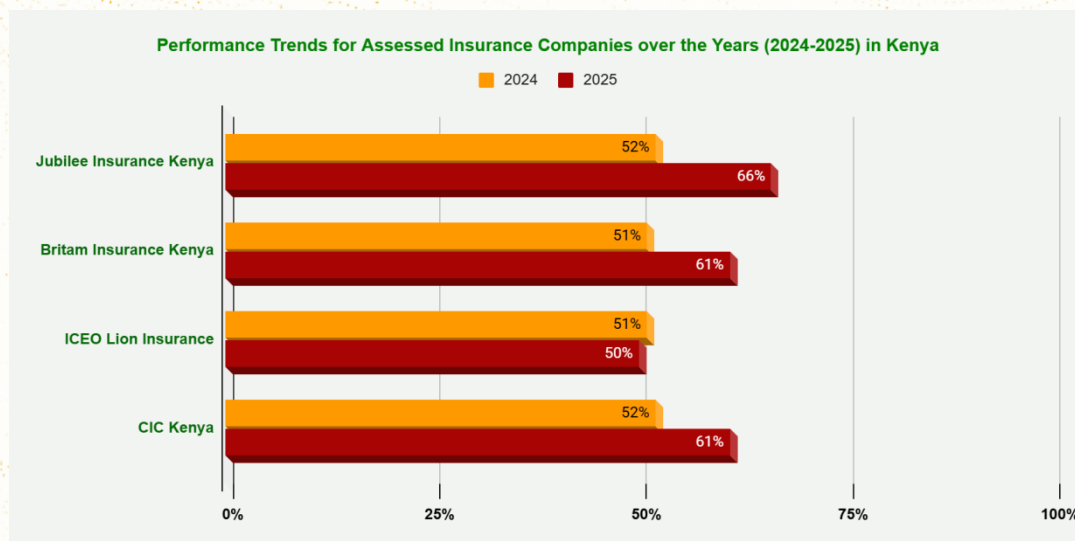
An analysis of data protection and privacy compliance performance among selected insurance companies in Zimbabwe reveals significant variation in compliance maturity and progress between 2024 and 2025. Old Mutual Zimbabwe recorded a decline in performance, decreasing from 49% in 2024 to 42% in 2025. While the company continues to demonstrate moderate compliance relative to other market participants, the downward trend suggests challenges in sustaining privacy controls. This may reflect gaps in continuous compliance monitoring, evolving regulatory expectations, or the need to update data protection policies and operational practices to maintain alignment with legal and best-practice standards.

Zimnat Lion Insurance showed a marked improvement, increasing from 5% in 2024 to 43% in 2025. This significant rise indicates substantial strengthening of data protection and privacy practices, likely driven by the introduction of governance structures, enhanced security controls, and increased organizational awareness of compliance obligations. The improvement reflects a positive shift toward more responsible handling of personal data and reduced regulatory risk.

Alliance Insurance remained unchanged at a low level of 4% in both 2024 and 2025. This stagnation highlights persistent deficiencies in data protection and privacy compliance, suggesting limited implementation of core privacy controls and governance mechanisms. The consistently low performance places the company at high risk of regulatory non-compliance, data breaches, and associated reputational damage.

Cell Insurance demonstrated slight improvement, increasing from 4% in 2024 to 6% in 2025. While this indicates some progress, overall performance remains very low. The data suggests that initial steps toward compliance may have been taken; however, substantial effort is still required to establish effective data protection frameworks and meet regulatory expectations.

Overall, the findings indicate uneven compliance across the Zimbabwean insurance sector. While some companies have made notable strides in strengthening privacy practices, others continue to lag significantly. These trends underscore the importance of sustained investment in data protection governance, regular compliance assessments, and staff training. Insurers that fail to address persistent compliance gaps remain exposed to regulatory enforcement, operational disruption, and erosion of customer trust, whereas those demonstrating improvement are better positioned to enhance resilience and credibility in an increasingly data-driven regulatory environment.



An assessment of data protection and privacy compliance performance among selected insurance companies in Kenya indicates overall improvement across the sector between 2024 and 2025, with varying degrees of progress among individual insurers.

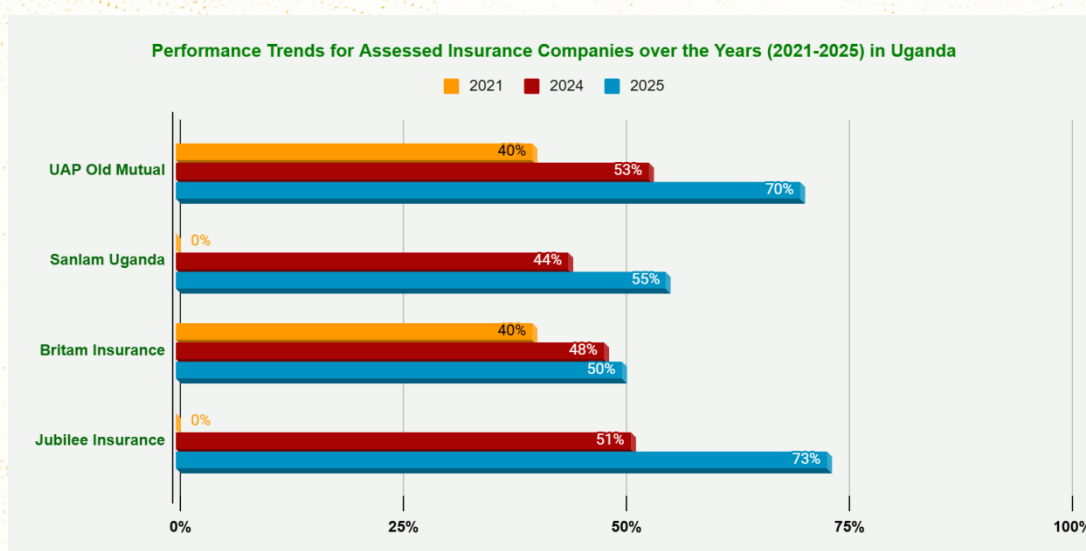
Jubilee Insurance Kenya demonstrated a strong improvement in compliance performance, increasing from 52% in 2024 to 66% in 2025. This notable rise suggests enhanced implementation of data protection frameworks, strengthened governance structures, and improved organizational awareness of privacy obligations. The upward trend reflects a proactive approach to aligning operations with data protection requirements and mitigating privacy-related risks.

Britam Insurance Kenya also showed consistent improvement, rising from 51% to 61%. This progress indicates ongoing efforts to strengthen privacy controls, such as improved data handling procedures, policy updates, and staff training. The improvement positions the company more favorably in managing personal and sensitive customer data in line with regulatory expectations.

ICEO Lion Insurance recorded a marginal decline, decreasing slightly from 51% in 2024 to 50% in 2025. While the change is minimal, it suggests stagnation in compliance efforts and highlights the need for renewed focus to prevent regression. Without continuous improvement, the company may face challenges in keeping pace with evolving data protection requirements and emerging risks.

CIC Insurance Group Kenya showed a clear improvement, increasing from 52% to 61%. This positive trend reflects strengthened privacy practices and greater institutional commitment to data protection compliance, likely supported by improved oversight and implementation of internal controls.

Overall, the data indicates a generally positive trajectory for data protection and privacy compliance within the Kenyan insurance sector, with most companies demonstrating measurable improvements. However, the mixed performance underscores the importance of sustained investment in privacy governance, regular compliance reviews, and continuous staff training. Insurers that maintain upward momentum are better positioned to ensure regulatory compliance, reduce exposure to data breaches, and strengthen customer trust, while those showing stagnation or decline risk falling behind regulatory expectations and best practice standards.



The data protection and privacy compliance performance of UAP Old Mutual, Sanlam Uganda, Britam Insurance, and Jubilee Insurance demonstrates sustained and, in most cases, accelerated improvement over the period 2021 to 2025. Compared with last year's assessment, the 2025 results indicate that earlier gains have not only been maintained but further strengthened, reflecting growing institutional maturity in data protection governance across the sector.

UAP Old Mutual continues to show a strong upward trajectory. Following its improvement from 40% in 2021 to 53% in 2024, the company recorded a further increase to 70% in 2025. This progression indicates a consolidation of earlier compliance efforts and the embedding of data protection practices into core operations. The 2025 score suggests enhanced implementation of privacy controls, stronger oversight mechanisms, and improved accountability for personal data handling. Compared to last year's analysis, UAP Old Mutual has moved closer to best-practice compliance, although continuous refinement remains necessary to address emerging risks and regulatory developments.

Sanlam Uganda has demonstrated one of the most significant transformations in the sector. After improving from 0% in 2021 to 44% in 2024, the company achieved 55% in 2025, confirming that the improvements noted in last year's analysis have translated into sustained compliance gains. This continued upward trend suggests that foundational data protection frameworks introduced in earlier years are now being operationalized more effectively. While progress is evident, the current performance level indicates the need to further strengthen monitoring, incident response readiness, and staff awareness to achieve higher compliance maturity.

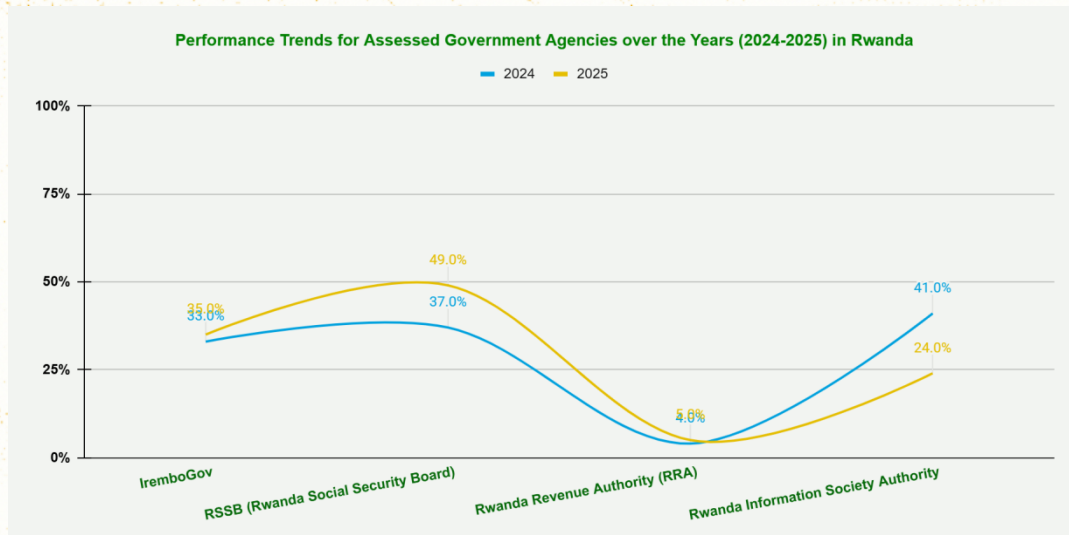
Britam Insurance has shown steady but incremental improvement. The company moved from 40% in 2021 to 48% in 2024, and further to 50% in 2025. This suggests that Britam Insurance has maintained its commitment to enhancing privacy practices, but the pace of improvement has slowed relative to peers. Compared with last year's analysis, the marginal increase highlights the importance of renewed focus on strengthening governance structures, risk assessments, and data lifecycle management to avoid stagnation.

Jubilee Insurance continues to demonstrate strong momentum. Building on its significant rise from 0% in 2021 to 51% in 2024, the company recorded 73% in 2025, representing the highest score among the four insurers. This improvement confirms that the substantial progress identified in last year's analysis has been reinforced through more advanced privacy controls and compliance mechanisms. The 2025 result indicates a higher level of alignment with regulatory expectations and positions Jubilee Insurance as a sector leader in data protection and privacy practices.

Overall, the 2025 results reflect a positive and maturing compliance landscape within the Ugandan insurance sector. Compared to last year's analysis, all four companies have either sustained or improved their performance, suggesting that investments in data protection frameworks, governance, and compliance oversight are yielding tangible results. However, the differing rates of progress underscore the need for continuous improvement. Companies with rapid gains must focus on sustainability and resilience, while those with slower growth should reassess their compliance strategies to avoid plateauing.

As regulatory expectations and cyber risks continue to evolve, maintaining and strengthening data protection practices will be critical to mitigating legal and reputational risks, enhancing customer trust, and ensuring long-term operational resilience.

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



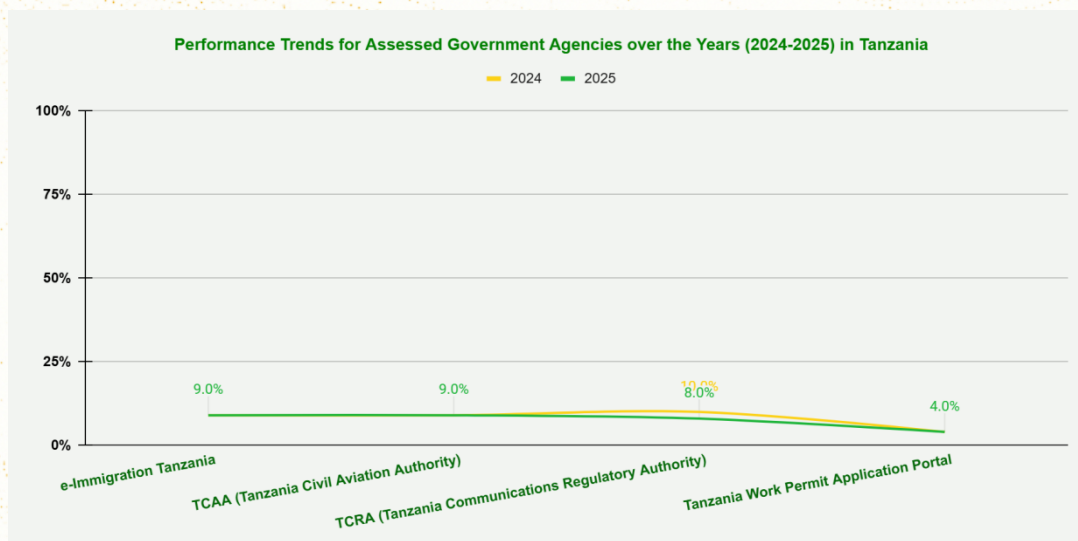
An assessment of data protection and privacy compliance performance across selected public service institutions in Rwanda indicates mixed progress between 2024 and 2025, with varying levels of compliance maturity and consistency. IremboGov recorded a modest improvement, increasing from 33.0% in 2024 to 35.0% in 2025. This incremental progress suggests gradual strengthening of privacy practices, likely reflecting improvements in governance processes and awareness of data protection obligations. However, the relatively moderate score indicates that while foundational measures may be in place, further enhancement is required to ensure robust protection of personal data, particularly given the platform's role in handling large volumes of citizen information.

Rwanda Social Security Board (RSSB) demonstrated a notable improvement, rising from 37% in 2024 to 49% in 2025. This significant increase indicates strengthened data protection and privacy controls, possibly driven by improved policy implementation, better oversight, and enhanced handling of sensitive personal and financial data. The upward trend reflects growing alignment with data protection requirements, although additional efforts are needed to reach higher levels of compliance maturity.

Rwanda Revenue Authority (RRA) showed only a marginal increase, from 4.0% in 2024 to 5.0% in 2025. Despite the slight improvement, the overall performance remains very low, highlighting persistent gaps in data protection and privacy compliance. Given the highly sensitive nature of taxpayer data managed by the institution, this level of performance presents significant compliance, security, and reputational risks, underscoring the need for urgent and comprehensive remedial action.

Rwanda Information Society Authority (RISA) maintained a static performance of 24.0% in both 2024 and 2025. This lack of progress suggests stagnation in strengthening privacy practices and may indicate limited prioritization of data protection improvements during the period under review. While baseline controls may exist, the absence of measurable advancement highlights the need for renewed focus on compliance monitoring, policy updates, and capacity building.

Overall, the data reveals uneven progress in data protection and privacy compliance across the assessed institutions. Improvements by RSSB and, to a lesser extent, IremboGov demonstrate the positive impact of targeted investments in data governance and compliance oversight. Conversely, the persistently low or stagnant performance of RRA and RISA raises concerns regarding exposure to regulatory non-compliance, data breaches, and erosion of public trust. These findings underscore the importance of sustained institutional commitment to data protection, particularly for entities managing large volumes of sensitive personal data. Continuous improvement through regular compliance assessments, staff training, strengthened governance frameworks, and effective enforcement of privacy policies will be critical to ensuring regulatory alignment, safeguarding citizen data, and enhancing public confidence in digital public services.



An assessment of data protection and privacy compliance performance among selected public digital platforms and regulatory authorities in Tanzania indicates persistently low levels of compliance maturity between 2024 and 2025, with limited evidence of improvement across most institutions.

e-Immigration Tanzania recorded a static performance of 9.0% in both 2024 and 2025. The absence of improvement suggests stagnation in the implementation of data protection and privacy controls. Given the platform's role in processing highly sensitive personal and biometric data, this consistently low score raises concerns about exposure to data protection risks and highlights the need for enhanced governance, security controls, and compliance oversight.

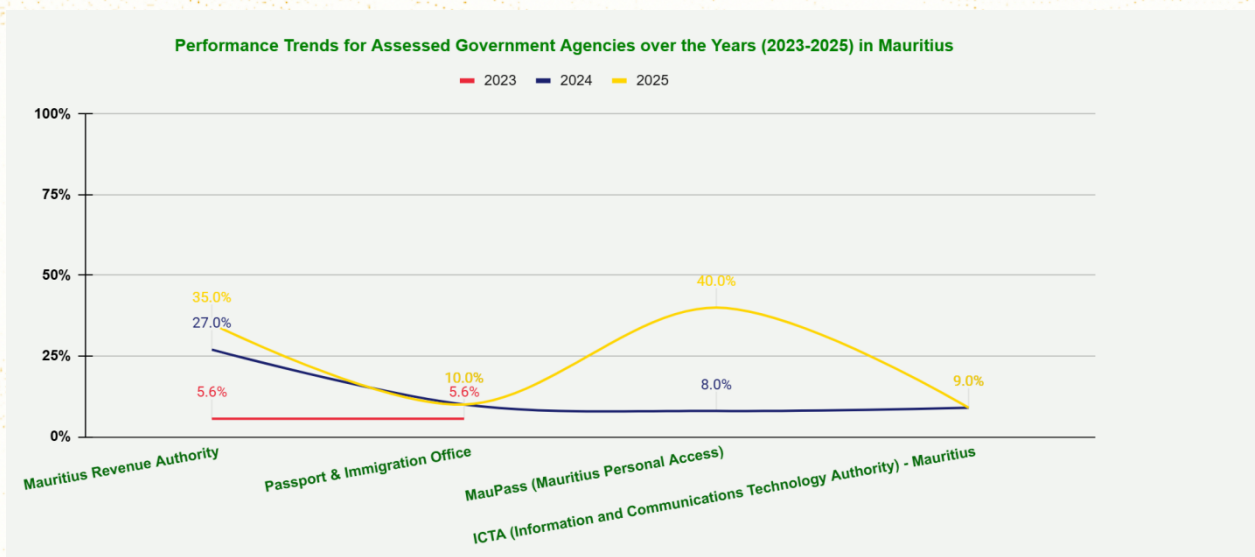
Tanzania Civil Aviation Authority (TCAA) similarly maintained a score of 9.0% across both years. This unchanged performance indicates limited progress in strengthening privacy practices despite the authority's handling of personal and operational data related to aviation safety and regulation. The findings point to potential gaps in policy implementation, staff awareness, and data security mechanisms.

Tanzania Communications Regulatory Authority (TCRA) experienced a slight decline, decreasing from 10.0% in 2024 to 8.0% in 2025. This reduction suggests challenges in sustaining even basic compliance measures and may reflect insufficient prioritization of data protection initiatives. As a regulator in the communications sector, the decline is particularly concerning and underscores the need for renewed focus on internal data governance and compliance leadership.

Tanzania Work Permit Application Portal recorded a consistently low performance of 4.0% in both years. This stagnation indicates significant deficiencies in data protection and privacy practices. Given the sensitive nature of personal, employment, and immigration-related data processed through the portal, the low score presents elevated risks of non-compliance, data breaches, and loss of public trust.

Overall, the data reflects a concerning lack of progress in data protection and privacy compliance among the assessed Tanzanian public digital platforms and authorities. Persistently low and stagnant scores suggest systemic weaknesses in governance structures, limited enforcement of privacy policies, and insufficient institutional capacity to address data protection obligations.

These trends highlight the urgent need for comprehensive reforms, including the establishment of clear accountability mechanisms, regular compliance assessments, capacity building, and investment in secure data management systems. Without targeted interventions, these institutions remain highly exposed to regulatory, operational, and reputational risks. Strengthening data protection and privacy practices is essential not only for legal compliance but also for safeguarding sensitive personal data and maintaining public confidence in digital public services.



The data protection and privacy compliance performance of the Mauritius Revenue Authority (MRA), Passport & Immigration Office, MauPass (Mauritius Personal Access), and the Information and Communications Technology Authority (ICTA) reflects a mixed trajectory between 2023 and 2025, with some institutions consolidating progress while others remain stagnant at low compliance levels. Compared with last year's analysis, the 2025 results provide clearer evidence of where improvements have been sustained and where gaps persist.

Mauritius Revenue Authority (MRA) has continued the positive trajectory identified in last year's assessment. Following its improvement from 5.6% in 2023 to 27.0% in 2024, the MRA further increased its score to 35.0% in 2025. This sustained upward trend confirms that the progress noted in the previous analysis was not transitional but indicative of a longer-term strengthening of data protection practices. The improvement suggests enhanced governance structures, better policy implementation, and increased attention to safeguarding taxpayer data. However, despite this progress, the overall score remains moderate, indicating that further investment is needed to achieve higher compliance maturity and alignment with international best practices.

The Passport & Immigration Office has shown no improvement since last year's analysis. The score remained at 10.0% in 2024 and 2025, following 5.6% in 2023. While the initial increase between 2023 and 2024 suggested some foundational steps toward compliance, the lack of further progress in 2025 indicates stagnation. Given the highly sensitive nature of identity, travel, and biometric data handled by this office, the persistently low score highlights ongoing weaknesses in privacy controls and underscores the urgent need for targeted interventions to strengthen data protection frameworks and operational safeguards.

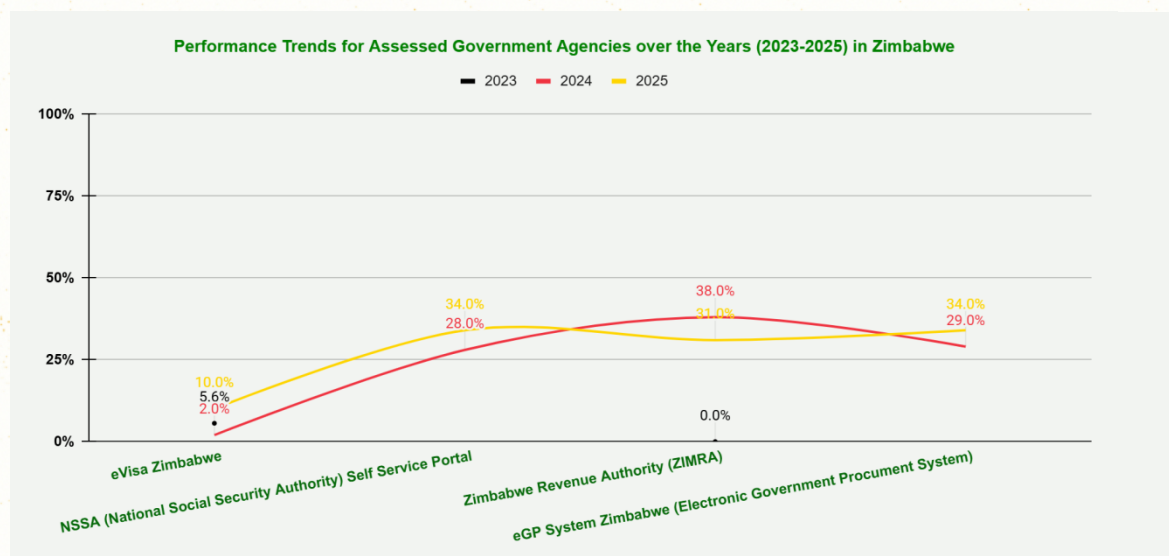
MauPass (Mauritius Personal Access) demonstrates the most dramatic improvement among the assessed institutions. After scoring 8.0% in 2024, the platform recorded a substantial increase to 40.0% in 2025. This sharp rise suggests a significant strengthening of privacy and data protection practices, likely reflecting focused efforts to address earlier gaps, enhance system security, and improve governance over citizen digital identity data. The 2025 performance marks a clear shift toward greater compliance maturity, although continued efforts will be required to sustain and deepen these improvements.

In contrast, the Information and Communications Technology Authority (ICTA) recorded a low and static performance of 9.0% in 2025 (with no measurable improvement reported). This lack of progress suggests limited advancement in strengthening internal data protection practices. As a key authority with oversight responsibilities in the ICT sector, this stagnation raises concerns about leadership in privacy compliance and the ability to model best practices for regulated entities.

Overall, the 2025 results show a divergence in compliance maturity across Mauritian public institutions. Compared with last year's analysis, the Mauritius Revenue Authority and MauPass have demonstrated sustained and, in the case of MauPass, accelerated improvement, indicating that focused investment and institutional commitment can yield measurable compliance gains. Conversely, the continued stagnation of the Passport & Immigration Office and ICTA highlights persistent structural and governance challenges.

These findings underscore the importance of moving beyond initial compliance measures toward continuous improvement, particularly for institutions managing large volumes of sensitive personal data.

Sustained progress will require stronger accountability mechanisms, regular compliance assessments, staff capacity building, and consistent enforcement of data protection policies. Institutions that fail to advance risk increased regulatory exposure, potential data breaches, and erosion of public trust, while those demonstrating improvement are better positioned to meet evolving data protection obligations and enhance confidence in digital public services.



The assessment of data protection and privacy compliance performance across selected e-government platforms in Zimbabwe, namely the eVisa Zimbabwe system, NSSA Self-Service Portal, Zimbabwe Revenue Authority (ZIMRA), and the Electronic Government Procurement (eGP) System reveals uneven progress between 2023 and 2025. Compared with last year's analysis, the 2025 results provide clearer insight into the sustainability of earlier gains and emerging compliance challenges.

The eVisa Zimbabwe system shows a gradual but modest improvement over the review period. Following a score of 5.6% in 2023 and a decline to 2.0% in 2024, the system improved to 10.0% in 2025. This increase indicates that some remedial actions have been undertaken since last year's assessment, partially addressing previously identified gaps. However, despite the improvement, the overall performance remains very low, suggesting that fundamental weaknesses persist in data protection governance, security controls, and compliance oversight. Given the sensitive personal and travel-related data processed by the platform, the system remains exposed to significant privacy and regulatory risks.

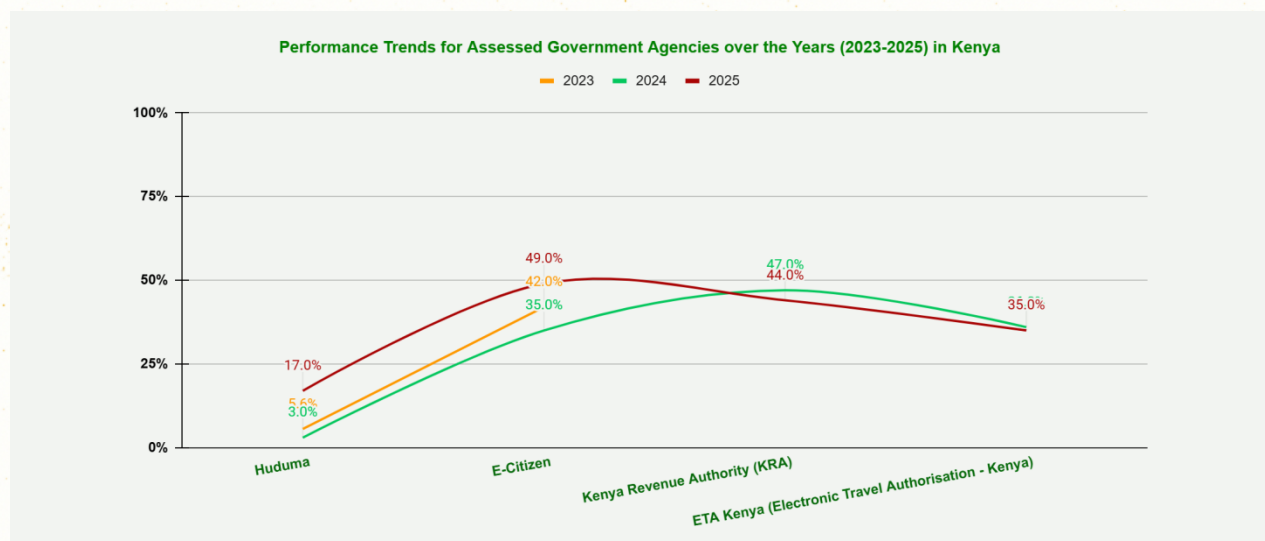
The NSSA Self-Service Portal demonstrates a strong and sustained upward trajectory. From 0.0% in 2023, the portal improved to 28.0% in 2024 and further to 34.0% in 2025. This continued progress suggests that the improvements noted in earlier assessments have been consolidated and expanded. The upward trend reflects strengthened data protection frameworks, improved internal controls, and increased institutional attention to safeguarding contributor and beneficiary data. While the performance has improved considerably, additional enhancements are still required to reach higher levels of compliance maturity.

In contrast, the Zimbabwe Revenue Authority (ZIMRA) experienced a regression in 2025. After a significant improvement from 0.0% in 2023 to 38.0% in 2024, ZIMRA's score declined to 31.0% in 2025. This decrease suggests challenges in sustaining the momentum highlighted in last year's analysis. While the authority still demonstrates moderate compliance relative to other entities, the decline indicates potential gaps in ongoing monitoring, policy enforcement, or adaptation to evolving data protection requirements. Sustained effort will be necessary to prevent further regression and to consolidate earlier gains.

The Electronic Government Procurement (eGP) System continued to show positive progress, improving from 29.0% in 2024 to 34.0% in 2025. This upward trend indicates strengthening data protection practices, particularly in the governance of procurement-related data and user access controls. The improvement suggests growing institutional awareness of privacy obligations and increased alignment with compliance expectations.

Overall, the 2025 results indicate mixed compliance maturity across Zimbabwe's e-government systems. Compared with last year's analysis, some platforms such as the NSSA Self-Service Portal and the eGP System, have demonstrated sustained improvement, highlighting the effectiveness of targeted interventions and institutional commitment. Conversely, the regression observed at ZIMRA and the persistently low performance of the eVisa system underscore the risks associated with inconsistent implementation and insufficient governance oversight.

These findings emphasize the need for continuous compliance monitoring, regular risk assessments, and sustained investment in data protection capabilities across all e-government platforms. Entities handling highly sensitive citizen data must prioritize the institutionalization of privacy-by-design principles to ensure regulatory compliance, reduce exposure to data breaches, and maintain public trust in digital government services.



The data protection and privacy compliance performance of key e-government platforms in Kenya (Huduma, e-Citizen, Kenya Revenue Authority (KRA), and the Electronic Travel Authorisation (ETA) system) shows mixed trends between 2023 and 2025. Compared with last year's analysis, the 2025 results provide insight into whether the declines observed in 2024 were temporary or indicative of deeper compliance challenges.

Huduma demonstrates a notable recovery in 2025. After a decline from 5.6% in 2023 to 3.0% in 2024, as highlighted in last year's analysis, Huduma's score increased significantly to 17.0% in 2025. This improvement suggests renewed efforts to address earlier shortcomings in data protection practices, potentially through improved governance structures or strengthened controls. Despite this positive movement, the overall score remains low, indicating that Huduma is still at an early stage of compliance maturity and requires sustained intervention to adequately protect citizen data.

e-Citizen shows a partial rebound following the decline noted in the previous assessment. After decreasing from 42.0% in 2023 to 35.0% in 2024, the platform improved to 49.0% in 2025, surpassing its 2023 performance. This upward trend indicates that corrective measures may have been implemented to strengthen privacy practices and address earlier gaps.

The 2025 score suggests a more established and maturing approach to data protection, although continuous improvement remains necessary given the scale and sensitivity of data processed by the platform.

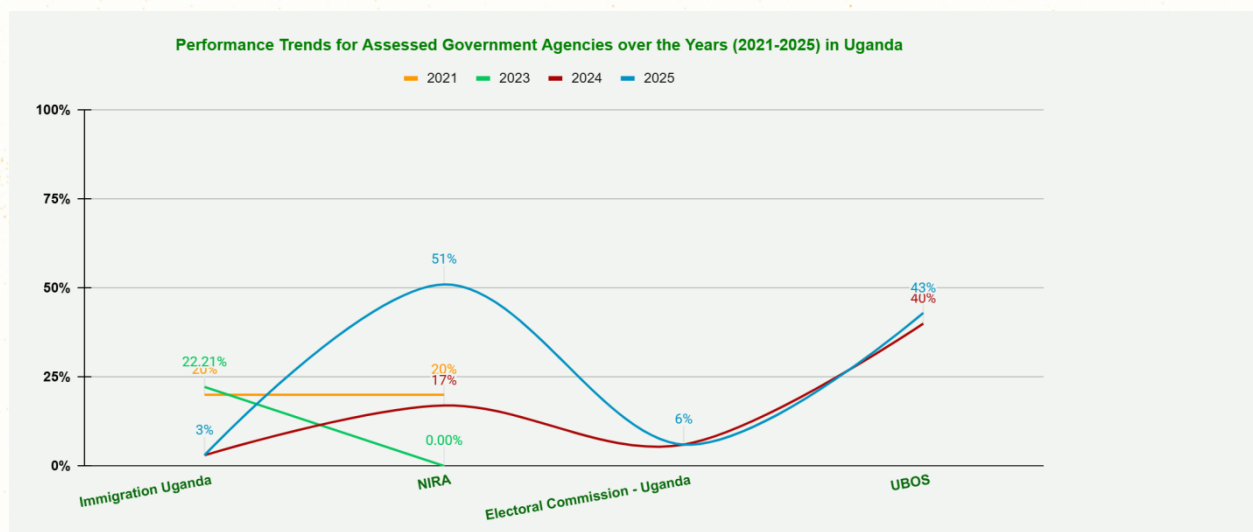
The Kenya Revenue Authority (KRA) experienced a slight decline in 2025, decreasing from 47.0% in 2024 to 44.0%. While still maintaining a relatively strong compliance position, the downward trend suggests challenges in sustaining previous gains. This regression highlights the importance of continuous monitoring and reinforcement of data protection controls, particularly given the highly sensitive financial and taxpayer data handled by the authority.

The Electronic Travel Authorisation (ETA) system shows relative stability with a marginal decline from 36.0% in 2024 to 35.0% in 2025. This consistency indicates that while baseline privacy controls may be in place, progress has plateaued. Given the personal and travel-related data processed by the system, further enhancements are needed to strengthen compliance maturity and resilience against privacy risks.

Overall, the 2025 results suggest that some of the declines observed in 2024 particularly, for Huduma and e-Citizen have been partially or fully reversed, indicating responsiveness to identified compliance gaps. However, the mixed performance across platforms underscores the uneven maturity of data protection practices within Kenya's e-government ecosystem.

These trends reinforce the need for sustained investment in privacy governance, regular compliance assessments, and the institutionalization of privacy-by-design principles. Platforms that demonstrate recovery and improvement must focus on sustaining momentum, while those showing stagnation or regression risk increased exposure to regulatory scrutiny, data breaches, and erosion of public trust. Strengthening data protection and privacy practices remains critical to ensuring compliance with Kenya's data protection framework and maintaining confidence in digital government services.

The data protection and privacy compliance performance of Immigration Uganda, the National Identification and Registration Authority (NIRA), the Electoral Commission of Uganda, and the Uganda Bureau of Statistics (UBOS) reflects divergent trajectories between 2021 and 2025. Compared with last year's analysis, the 2025 results clarify whether earlier trends represented temporary fluctuations or more structural compliance challenges. Immigration Uganda continues to exhibit a significant decline in compliance performance. After scoring 20% in 2021 and 22.21% in 2023, the institution dropped sharply to 3% in 2024, a trend highlighted in last year's analysis.



The score remained unchanged at 3% in 2025, indicating that the regression identified previously has not been addressed. This persistent low performance suggests entrenched weaknesses in privacy governance, oversight, and implementation of data protection controls. Given the sensitive personal and biometric data handled by Immigration Uganda, the sustained decline presents serious compliance, security, and reputational risks, underscoring the need for urgent remedial action.

In contrast, NIRA has demonstrated substantial and sustained improvement. Following a decline from 20% in 2021 to 0% in 2023, NIRA improved to 17% in 2024, as noted in last year's analysis, and further increased to 51% in 2025. This marked improvement indicates that earlier corrective measures have been successfully consolidated and scaled. The 2025 performance suggests strengthened data protection frameworks, improved governance structures, and greater institutional focus on safeguarding national identity data. While continued refinement is necessary, NIRA's trajectory reflects a significant shift toward compliance maturity.

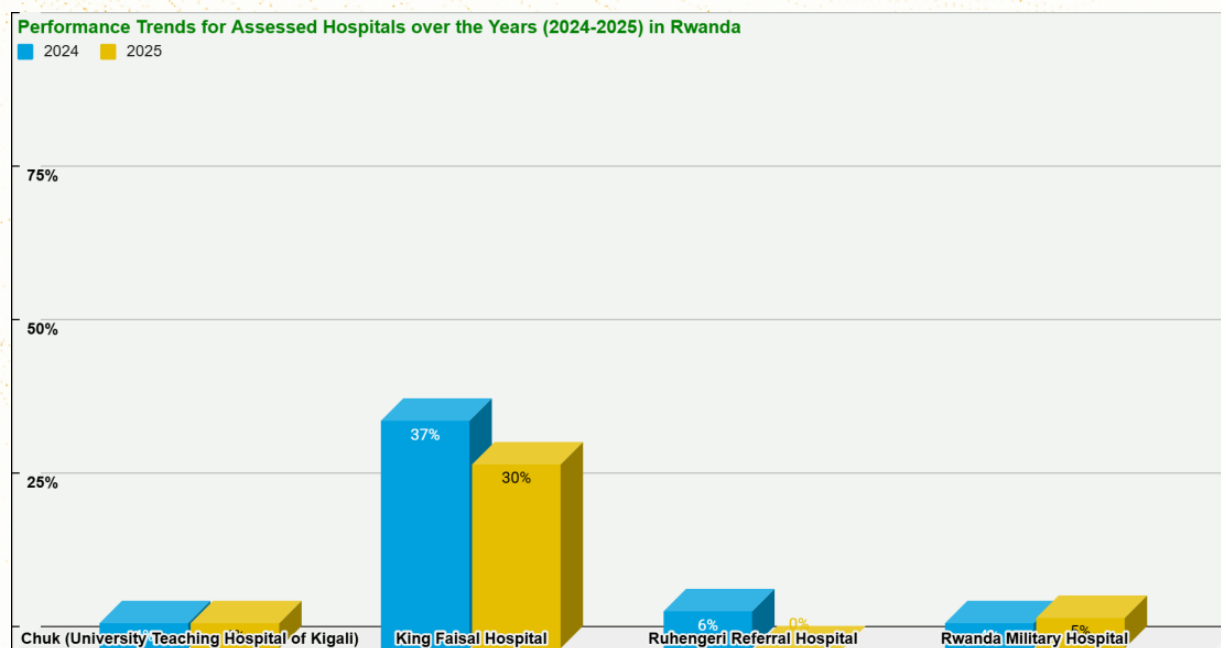
The Electoral Commission of Uganda shows consistently low and stagnant performance, recording 6% in both 2024 and 2025. Although no earlier data is available for comparison, the lack of improvement across the two most recent years suggests limited progress in strengthening data protection and privacy practices. Given the sensitive voter registration and electoral data managed by the Commission, the persistently low score raises concerns about exposure to data protection risks and the need for targeted capacity building and governance reforms.

UBOS demonstrates steady, incremental improvement. From 40% in 2024, the institution increased its score to 43% in 2025, indicating gradual strengthening of privacy practices. While the progress is modest, it suggests a level of institutional awareness and ongoing effort to improve data protection controls. However, given the volume and sensitivity of personal and statistical data handled by UBOS, further enhancements are required to reach higher compliance maturity and resilience.

Overall, the 2025 results show a divergence in compliance maturity across Uganda's e-government landscape. Compared with last year's analysis, NIRA has made exceptional progress, demonstrating that sustained institutional commitment can rapidly improve compliance outcomes. Conversely, Immigration Uganda's continued low performance confirms the severity of the regression identified previously, highlighting an urgent need for structural reform and enforcement of privacy obligations.

The stagnation observed at the Electoral Commission and the incremental progress at UBOS further emphasize the uneven pace of compliance across institutions. These findings underscore the importance of continuous compliance monitoring, leadership accountability, and investment in data protection capabilities. Institutions managing sensitive citizen data must embed privacy-by-design principles and strengthen governance frameworks to ensure regulatory compliance, mitigate data breach risks, and maintain public trust in digital government services.

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



An assessment of data protection and privacy compliance performance among selected public health institutions in Rwanda namely, CHUK (University Teaching Hospital of Kigali), King Faisal Hospital, Ruhengeri Referral Hospital, and Rwanda Military Hospital reveals generally low and uneven levels of compliance maturity between 2024 and 2025. Given the highly sensitive nature of health and patient data processed by these institutions, the findings underscore significant risks related to data protection and privacy.

CHUK (University Teaching Hospital of Kigali) recorded a static score of 4% in both 2024 and 2025, indicating no measurable improvement in data protection and privacy practices. This stagnation suggests persistent gaps in governance, limited implementation of privacy controls, and inadequate staff awareness. Considering CHUK's central role in providing tertiary healthcare services and handling large volumes of sensitive patient data, the lack of progress presents elevated compliance and reputational risks.

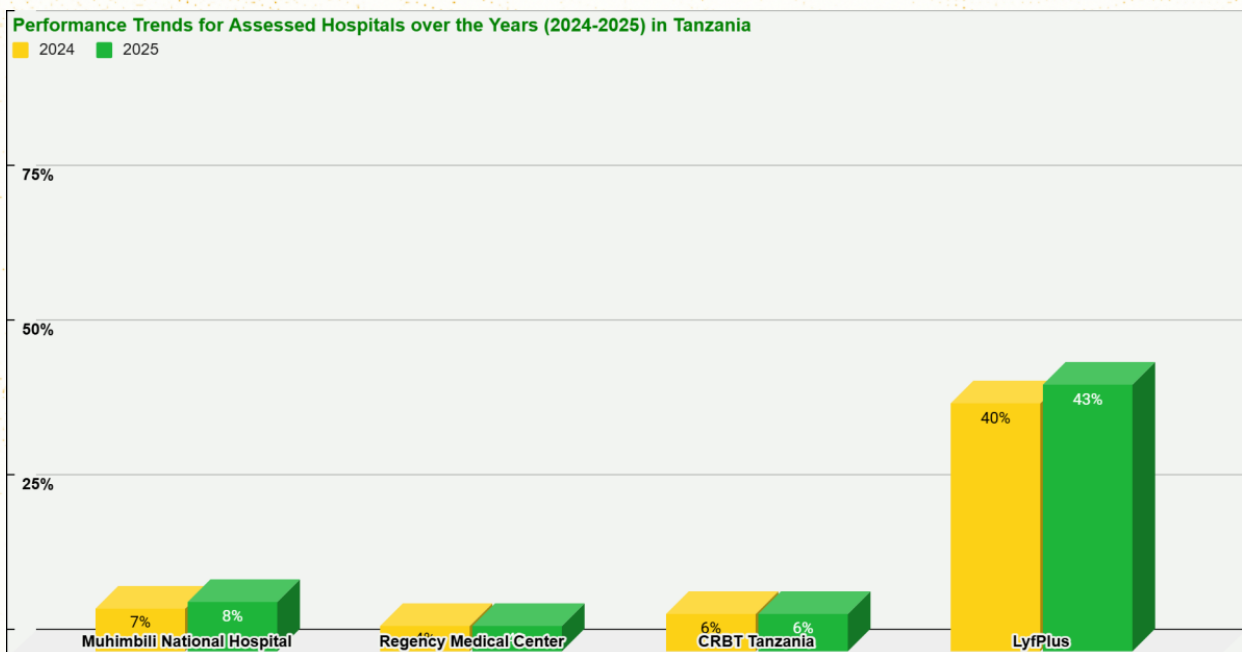
King Faisal Hospital experienced a decline in performance, dropping from 37% in 2024 to 30% in 2025. While the hospital continues to demonstrate relatively stronger compliance compared to other assessed facilities, the downward trend indicates challenges in sustaining previously established privacy practices. This regression may reflect gaps in continuous monitoring, policy enforcement, or adaptation to evolving data protection requirements within the health sector.

Ruhengeri Referral Hospital showed a significant deterioration, falling from 6% in 2024 to 0% in 2025. This result indicates the absence of effective data protection and privacy controls during the reporting period. Given the sensitivity of medical records and personal health information, this decline highlights critical vulnerabilities and the urgent need for foundational interventions to establish basic data protection frameworks.

Rwanda Military Hospital recorded a marginal improvement, increasing from 4% in 2024 to 5% in 2025. Although the increase is minimal, it suggests some effort to improve compliance. Nevertheless, the overall performance remains very low, indicating that existing measures are insufficient to adequately safeguard patient and staff data.

Overall, the data points to systemic weaknesses in data protection and privacy compliance across public health institutions in Rwanda. With the exception of King Faisal Hospital which, despite a decline, remains comparatively more advanced, the institutions exhibit either stagnation or regression in compliance maturity.

These findings highlight the urgent need for sector-wide strengthening of data protection practices, including the establishment of clear governance structures, routine compliance assessments, staff training on handling health data, and investment in secure health information systems. Failure to address these gaps exposes institutions to heightened risks of data breaches, regulatory non-compliance, and erosion of patient trust. Strengthening data protection and privacy practices is essential to protecting sensitive health information and supporting safe and ethical healthcare delivery.



An assessment of data protection and privacy compliance performance among selected health sector institutions in Tanzania, Muhimbili National Hospital, Regency Medical Center, CRBT Tanzania, and LyfPlus reveals uneven levels of compliance maturity between 2024 and 2025. Given the highly sensitive nature of health and personal data processed by these institutions, the results highlight varying degrees of institutional commitment and capacity to meet data protection and privacy obligations.

Muhimbili National Hospital recorded a marginal improvement, increasing from 7% in 2024 to 8% in 2025. While the increase suggests some progress in strengthening data protection practices, the overall score remains very low. This indicates that privacy controls, governance structures, and staff awareness mechanisms are still underdeveloped. Considering the hospital's role as a national referral facility handling large volumes of sensitive patient data, the low compliance level presents significant privacy and regulatory risks.

Regency Medical Center maintained a static score of 4% across both years. The absence of improvement suggests stagnation in data protection and privacy efforts, potentially reflecting limited prioritization of compliance initiatives. The consistently low score indicates substantial gaps in safeguarding patient data and highlights the need for foundational improvements in data governance and security practices.

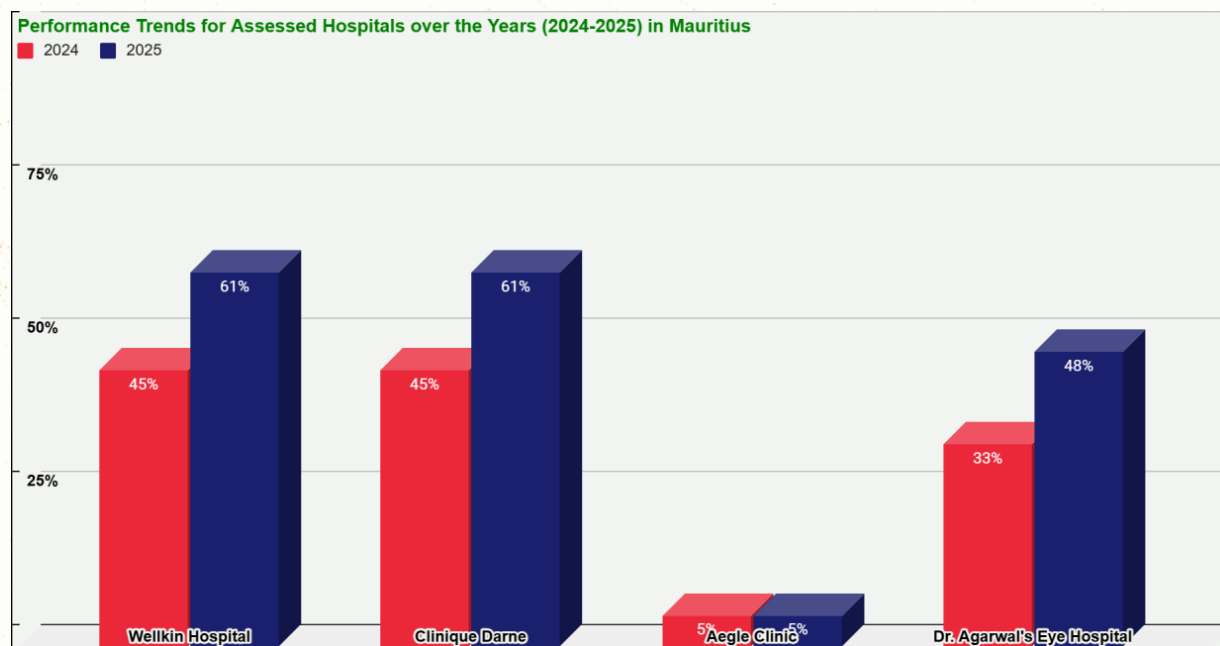
CRBT Tanzania recorded no change, maintaining a score of 6% in both 2024 and 2025. While the institution demonstrates slightly stronger performance than some peers, the lack of progress indicates that existing privacy measures have not been strengthened. Given CRBT's handling of sensitive health and personal data, the static performance suggests exposure to compliance and data security risks.

In contrast, LyfPlus demonstrated relatively strong and improving performance, increasing from 40% in 2024 to 43% in 2025. This improvement indicates a more mature approach to data protection and privacy compliance, likely supported by clearer governance structures, stronger data handling practices, and greater organizational awareness. LyfPlus stands out among the assessed institutions as having made meaningful progress toward aligning with data protection requirements.

Overall, the data highlights significant disparities in data protection and privacy compliance maturity within Tanzania's health sector. Public and traditional healthcare institutions show persistently low or stagnant performance, suggesting systemic challenges in implementing effective privacy frameworks. In contrast, LyfPlus demonstrates that targeted investment and institutional commitment can lead to measurable compliance improvements.

These findings underscore the urgent need for strengthened data protection governance across the health sector, including regular compliance assessments, staff training on handling sensitive health data, and investment in secure health information systems. Institutions with persistently low compliance levels remain vulnerable to regulatory non-compliance, data breaches, and loss of patient trust. Enhancing data protection and privacy practices is essential to safeguarding personal health information and supporting safe, ethical, and compliant healthcare delivery.

An assessment of data protection and privacy compliance performance among selected health sector institutions namely, Wellkin Hospital, Clinique Darne, Aegle Clinic, and Dr. Agarwal's Eye Hospital shows varied levels of compliance maturity and progress between 2024 and 2025. Given the sensitive nature of health and personal data processed by these institutions, the results provide important insights into their ability to meet data protection and privacy obligations.



Wellkin Hospital demonstrated a significant improvement in compliance performance, increasing from 45% in 2024 to 61% in 2025. This notable rise suggests strengthened data protection governance, improved handling of patient information, and greater institutional awareness of privacy requirements. The 2025 performance indicates a maturing compliance framework and positions the hospital as one of the stronger performers among the assessed institutions.

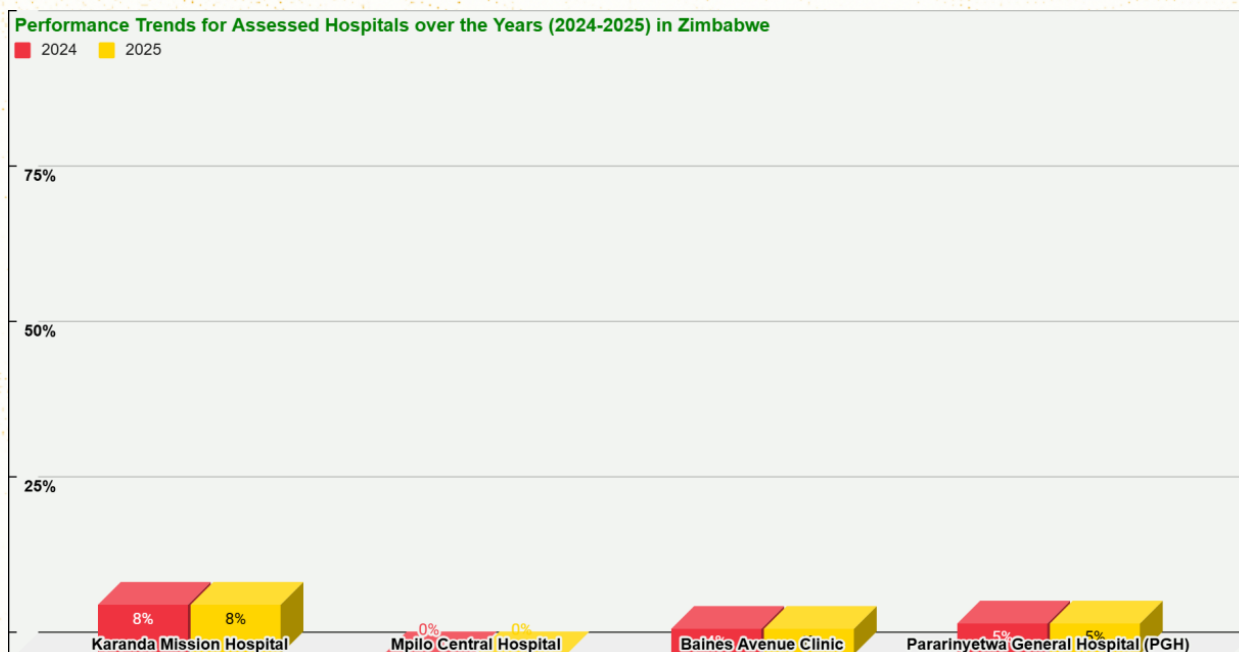
Clinique Darne similarly recorded substantial progress, improving from 45% in 2024 to 61% in 2025. This parallel increase suggests targeted efforts to enhance privacy controls, possibly through updated policies, improved staff training, and strengthened security measures. The improvement reflects a growing commitment to safeguarding patient data and aligning with data protection standards.

In contrast, Aegle Clinic maintained a consistently low score of 5% in both years. The lack of improvement indicates persistent deficiencies in data protection and privacy practices. This stagnation highlights significant vulnerabilities in the handling of patient data and underscores the urgent need for foundational interventions to establish basic privacy governance and compliance mechanisms.

Dr. Agarwal's Eye Hospital showed clear progress, increasing from 33% in 2024 to 48% in 2025. This improvement reflects strengthened privacy practices and growing compliance maturity, although the 2025 score suggests there remains room for further enhancement to reach higher compliance levels comparable to leading institutions.

Overall, the data reveals a divergent compliance landscape within the health sector. Wellkin Hospital and Clinique Darne demonstrate that sustained investment in data protection frameworks and organizational capacity can yield significant compliance gains. Dr. Agarwal's Eye Hospital also shows positive momentum, though continued efforts are required to consolidate progress.

Conversely, the persistently low performance of Aegle Clinic presents serious compliance and reputational risks, particularly given the sensitivity of health data. These findings underscore the need for sector-wide prioritization of data protection, including clear governance structures, regular compliance reviews, staff training, and investment in secure health information systems. Strengthening data protection and privacy practices is essential to ensuring regulatory compliance, protecting patient confidentiality, and maintaining trust in healthcare service delivery.



An assessment of data protection and privacy compliance performance among Zimbabwe's Karanda Mission Hospital, Mpilo Central Hospital, Baines Avenue Clinic, and Parirenyatwa General Hospital (PGH), indicates persistently low levels of compliance maturity between 2024 and 2025. Given the highly sensitive nature of health and patient data handled by these institutions, the findings raise serious concerns regarding the adequacy of data protection and privacy safeguards.

Karanda Mission Hospital maintained a score of 8% in both 2024 and 2025, indicating no measurable improvement in data protection and privacy practices. While the hospital demonstrates some minimal level of compliance, the stagnation suggests limited progress in strengthening governance structures, implementing privacy controls, or enhancing staff awareness. The consistently low score highlights ongoing vulnerabilities in the handling of patient data.

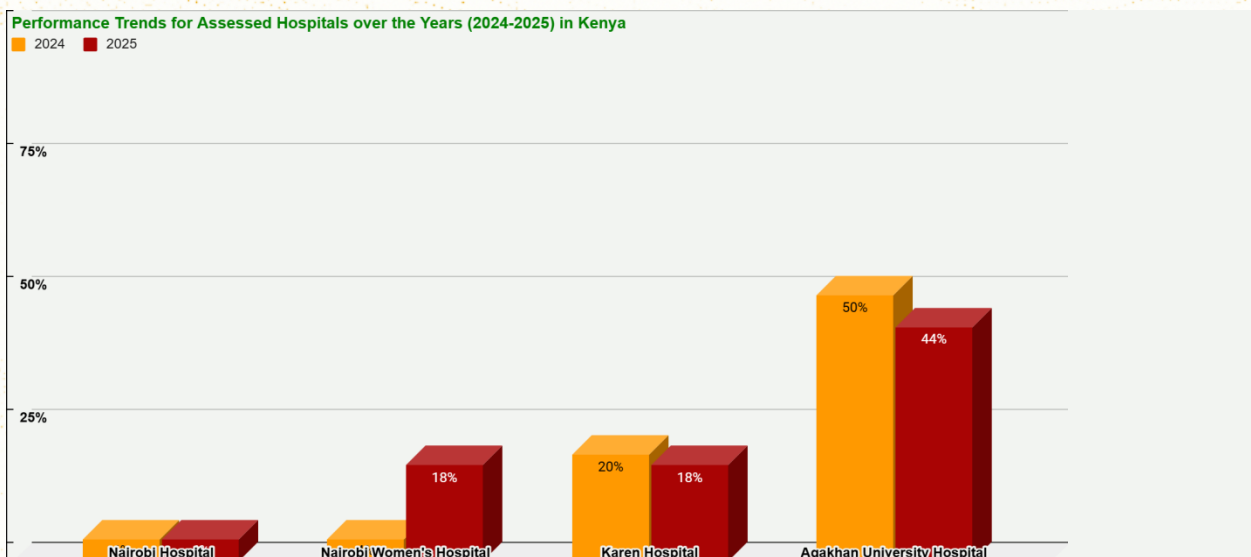
Mpilo Central Hospital recorded a score of 0% in both 2024 and 2025, indicating a complete absence of measurable data protection and privacy controls during the period under review. This persistent lack of compliance presents significant risks, particularly given the hospital's role as a major public referral facility managing large volumes of sensitive patient information. The findings suggest an urgent need for foundational interventions to establish basic data protection frameworks and safeguards.

Baines Avenue Clinic maintained a static score of 4% across both years. The absence of improvement points to persistent gaps in data protection practices and a lack of prioritization of privacy compliance. The low score indicates that existing measures, if any, are insufficient to ensure the confidentiality and security of patient data.

Parirenyatwa General Hospital (PGH) recorded a consistent score of 5% in both 2024 and 2025. While marginally higher than some peers, the unchanged performance suggests stagnation and limited advancement in privacy compliance maturity. Given the scale and complexity of operations at PGH, the low score highlights significant exposure to data protection and regulatory risks.

Overall, the data reveals systemic weaknesses in data protection and privacy compliance across the assessed health sector institutions. The absence of improvement over the two-year period suggests that data protection has not been adequately prioritized within institutional governance and operational frameworks.

These findings underscore the urgent need for sector-wide reforms, including the establishment of clear data protection governance structures, regular compliance assessments, targeted staff training, and investment in secure health information systems. Institutions with persistently low or non-existent compliance levels remain highly vulnerable to data breaches, regulatory non-compliance, and erosion of patient trust. Strengthening data protection and privacy practices is critical to safeguarding sensitive health information and supporting ethical, secure, and compliant healthcare delivery.



An assessment of data protection and privacy compliance performance among selected Kenyan hospitals namely; Nairobi Hospital, Nairobi Women's Hospital, Karen Hospital, and Aga Khan University Hospital reveals varied levels of compliance maturity and mixed trends between 2024 and 2025. Given the highly sensitive nature of patient and health data handled by these institutions, the findings provide important insight into their alignment with data protection and privacy obligations.

Nairobi Hospital recorded a consistently low score of 4% in both 2024 and 2025, indicating no measurable improvement in data protection and privacy practices. This stagnation suggests persistent gaps in governance structures, limited implementation of privacy controls, and insufficient staff awareness. The unchanged low performance highlights significant vulnerabilities in safeguarding patient data and exposes the institution to elevated compliance and reputational risks.

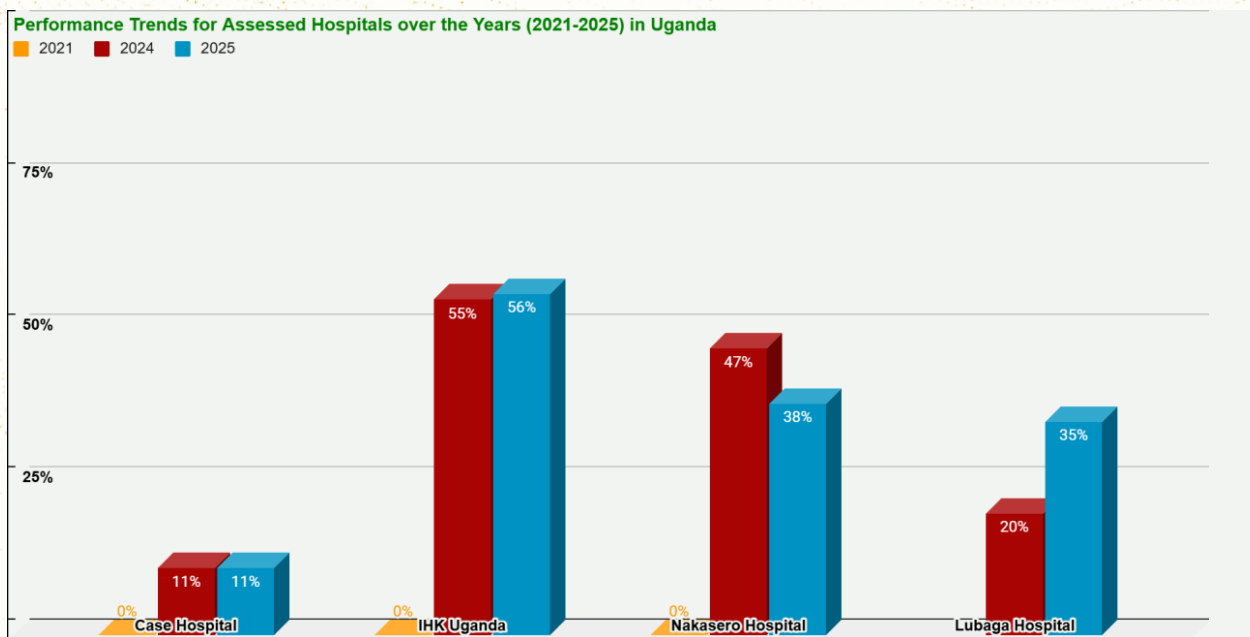
Nairobi Women's Hospital demonstrated notable improvement, increasing from 4% in 2024 to 18% in 2025. This upward trend indicates deliberate efforts to strengthen data protection practices, potentially through policy development, improved data handling procedures, and increased institutional awareness of privacy requirements. While the improvement is encouraging, the 2025 score remains moderate, suggesting the need for continued investment to achieve higher compliance maturity.

Karen Hospital experienced a slight decline, decreasing from 20% in 2024 to 18% in 2025. Although the reduction is marginal, it suggests challenges in sustaining previously established privacy practices. The hospital maintains a moderate level of compliance; however, the downward trend underscores the importance of continuous monitoring and reinforcement of data protection controls to prevent further regression.

Aga Khan University Hospital recorded a decline in performance, falling from 50% in 2024 to 44% in 2025. Despite the decrease, the hospital remains the strongest performer among the assessed institutions. The regression may reflect evolving compliance expectations or gaps in maintaining consistency across privacy controls. Sustained effort will be required to preserve its relatively advanced compliance posture and align with best practices.

Overall, the data indicates uneven data protection and privacy compliance maturity among Kenyan hospitals. While Nairobi Women's Hospital demonstrates meaningful progress, Nairobi Hospital continues to lag significantly, and both Karen Hospital and Aga Khan University Hospital show signs of regression.

These trends underscore the need for sustained and systematic investment in data protection governance across the health sector. Hospitals handling sensitive patient data must prioritize continuous compliance assessments, staff training, and strengthening of technical and organizational safeguards. Institutions that fail to address persistent gaps remain exposed to regulatory sanctions, data breaches, and erosion of patient trust, while those that maintain or improve compliance are better positioned to support ethical, secure, and compliant healthcare delivery.



An assessment of data protection and privacy compliance among Case Hospital, IHK Uganda, Nakasero Hospital, and Lubaga Hospital reveals a generally positive trajectory since 2021, though varying levels of maturity are evident across institutions.

Case Hospital maintained a score of 11% in 2025, unchanged from 2024. This stability suggests that while initial steps to establish privacy measures have been sustained since its rise from 0% in 2021, progress remains modest. The institution continues to have significant gaps in governance, technical safeguards, and staff awareness, highlighting the need for continued investment in privacy and data protection frameworks.

IHK Uganda showed a slight improvement, increasing from 55% in 2024 to 56% in 2025. This steady high score demonstrates that the hospital has developed a relatively mature approach to data protection, with robust privacy policies and practices likely in place. IHK Uganda remains the leader in the group, reflecting a strong commitment to safeguarding patient information, reducing legal and compliance risks, and enhancing patient trust.

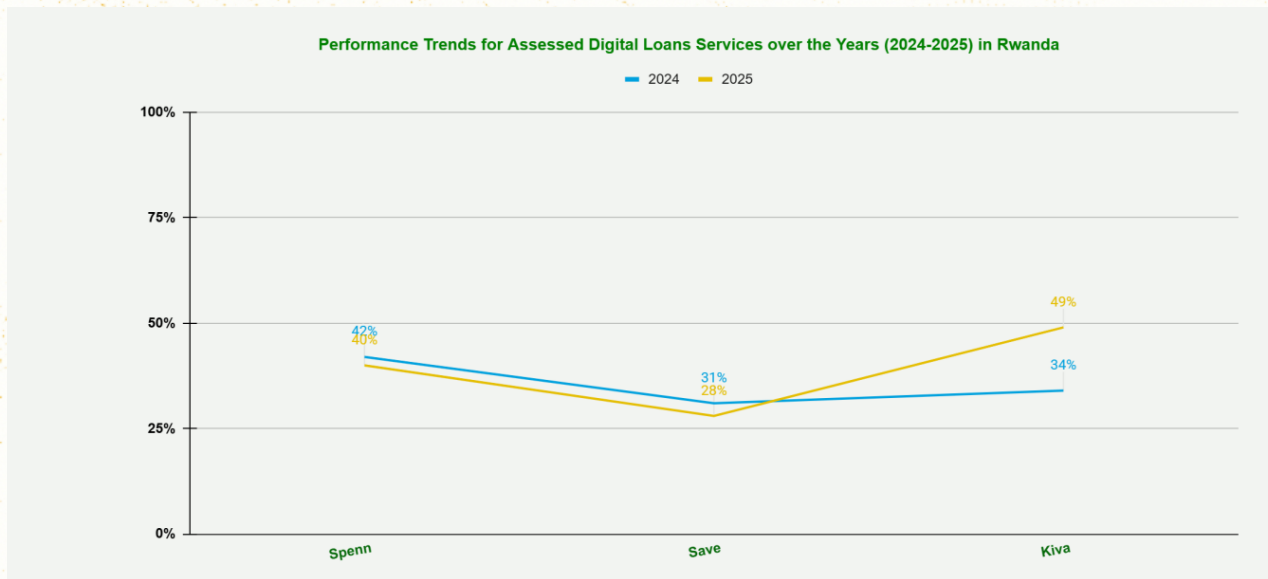
Nakasero Hospital experienced a decline from 47% in 2024 to 38% in 2025, indicating potential challenges in sustaining previously implemented privacy measures. While still performing above Case and Lubaga Hospitals, the drop suggests a need for renewed focus on maintaining and strengthening data protection governance, staff training, and monitoring mechanisms.

Lubaga Hospital showed a notable improvement, rising from 20% in 2024 to 35% in 2025. This increase reflects significant progress in implementing privacy and data protection practices, signaling the hospital's commitment to strengthening compliance and safeguarding patient data. However, despite the improvement, there is still room to enhance maturity to meet industry best practices.

Overall, the data illustrates a sector in gradual improvement, with some institutions like IHK Uganda achieving relatively mature compliance, while others remain at early stages of data protection implementation. The variation highlights the importance of continuous investment in privacy governance, staff training, and technical safeguards to maintain and improve compliance levels.

Hospitals that demonstrate consistent improvement, such as Lubaga Hospital, signal growing readiness to protect patient data and align with regulatory standards. Conversely, institutions with stagnant or declining scores, like Case Hospital and Nakasero Hospital, remain vulnerable to data breaches, regulatory penalties, and reputational damage. Strengthening data protection practices across all hospitals is critical to ensure patient confidentiality, regulatory compliance, and trust in the healthcare system.

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



An assessment of data protection and privacy compliance performance among Spenn, Save, and Kiva shows varying trends over the two-year period. Given the highly sensitive financial and personal data processed by these digital loan platforms, the findings offer important insight into their privacy maturity and regulatory alignment.

Spenn recorded a slight decrease from 42% in 2024 to 40% in 2025, indicating a minor regression in data protection and privacy practices. While the score remains relatively moderate, the decline may suggest challenges in maintaining or enhancing internal privacy controls, policies, and staff awareness. Continued focus is required to ensure sustained compliance with evolving data protection regulations and to mitigate risks related to sensitive financial data.

Save experienced a decline from 31% in 2024 to 28% in 2025, signaling a slight deterioration in its privacy framework. This suggests that the company may face challenges in strengthening governance, technical safeguards, or operational practices for data protection. The low to moderate score highlights the need for accelerated efforts to enhance data protection measures to maintain customer trust and comply with regulatory standards.

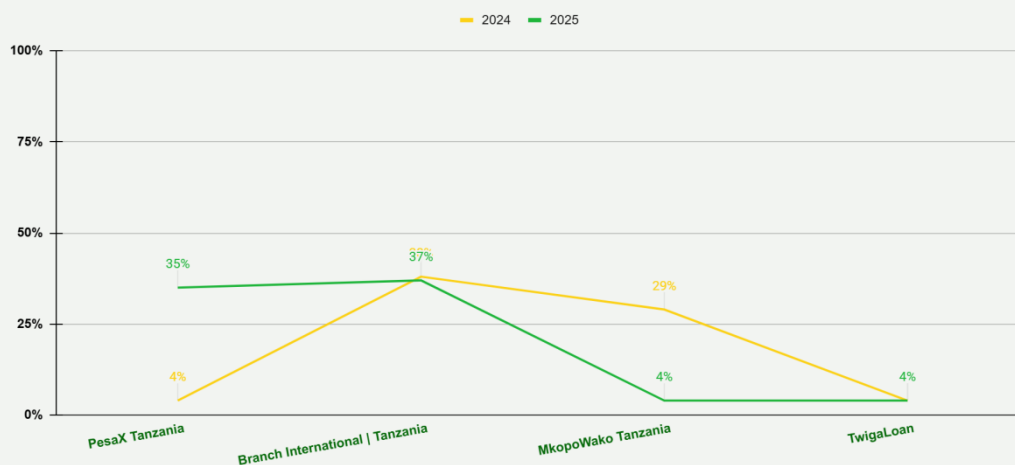
Kiva, in contrast, demonstrated a significant improvement, rising from 34% in 2024 to 49% in 2025. This notable increase indicates that Kiva has made substantial progress in strengthening its data protection and privacy practices, likely through improved policy implementation, enhanced technical safeguards, and greater organizational awareness.

The improvement positions Kiva as a leading performer in this group, reflecting a commitment to safeguarding customer data and reducing compliance risks.

Overall, the data highlights uneven privacy and data protection maturity among digital loan service providers. Kiva stands out for its significant progress, demonstrating that deliberate investment in privacy practices can yield measurable results. In contrast, Spenn and Save show slight declines, signaling a need for renewed focus on maintaining and enhancing data protection frameworks.

These findings underscore the importance of continuous assessment, staff training, and investment in secure digital infrastructure. Providers with stagnant or declining performance remain vulnerable to regulatory non-compliance, data breaches, and loss of customer trust. Strengthening privacy and data protection practices is critical not only for compliance but also for ensuring the secure handling of highly sensitive financial and personal information in the digital loan sector.

Performance Trends for Assessed Digital Loans Services over the Years (2024-2025) in Tanzania



An assessment of data protection and privacy compliance among PesaX Tanzania, Branch International Tanzania, MkopoWako Tanzania, and TwigaLoan reveals significant fluctuations over the two-year period, highlighting varying levels of maturity in safeguarding sensitive financial and personal data.

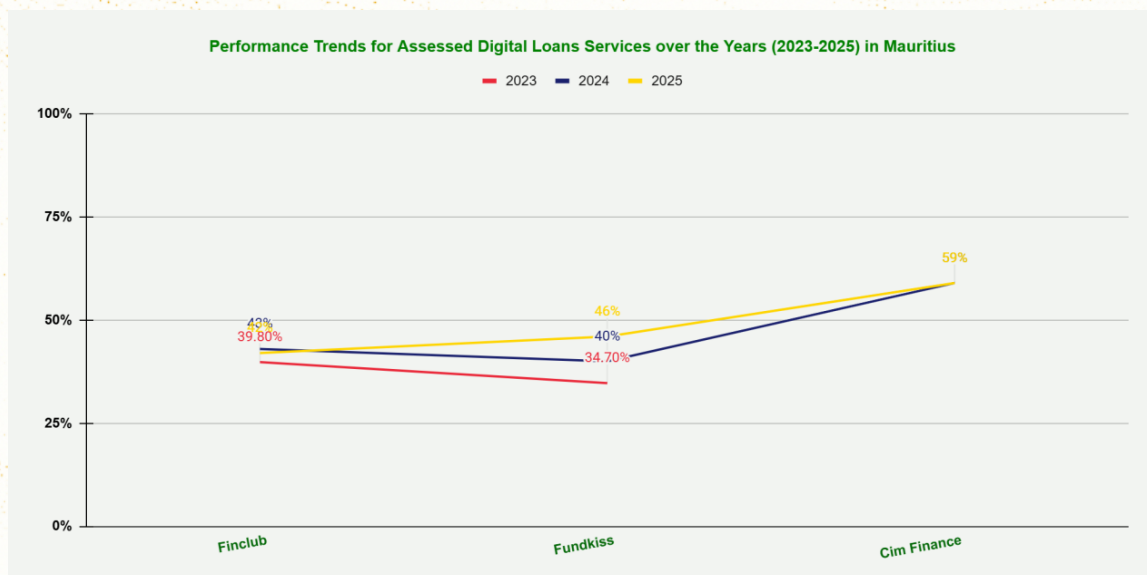
PesaX Tanzania exhibited a remarkable increase in compliance performance, rising from 4% in 2024 to 35% in 2025. This substantial improvement suggests that the company has taken significant steps to strengthen its privacy framework, implement robust data protection policies, and enhance operational controls. The progress indicates a growing commitment to safeguarding customer data and aligning with relevant data protection regulations.

Branch International Tanzania maintained a relatively stable score, slightly decreasing from 38% in 2024 to 37% in 2025. While the marginal decline is not significant, it suggests the need for continuous monitoring and reinforcement of existing privacy controls to sustain compliance. Branch Tanzania demonstrates moderate maturity in data protection practices, reflecting ongoing efforts to protect sensitive financial information.

MkopoWako Tanzania experienced a sharp decline from 29% in 2024 to 4% in 2025, signaling a major regression in data protection and privacy practices. This drop indicates serious gaps in governance, technical safeguards, or operational compliance, and exposes the company to heightened regulatory and reputational risks. Immediate corrective actions are required to rebuild its privacy framework and ensure protection of customer data.

TwigaLoan maintained a consistently low score of 4% in both years, indicating persistent deficiencies in privacy and data protection practices. The stagnant low performance highlights significant vulnerabilities in handling sensitive financial information, underscoring the urgent need for foundational privacy controls and regulatory compliance measures.

Overall, the data highlights a highly uneven compliance landscape among digital loan providers in Tanzania. PesaX Tanzania stands out for its remarkable improvement, demonstrating that focused investment in privacy and data protection can yield tangible results. Branch Tanzania shows moderate maturity with stable performance, while MkopoWako Tanzania and TwigaLoan lag significantly, presenting critical risks. These trends underscore the importance of continuous improvement in privacy governance, staff training, and technical safeguards. Providers with low or declining performance remain highly vulnerable to data breaches, regulatory penalties, and erosion of customer trust. Strengthening privacy and data protection frameworks is essential not only for regulatory compliance but also for ensuring the secure handling of sensitive financial and personal information in the growing digital loan sector.



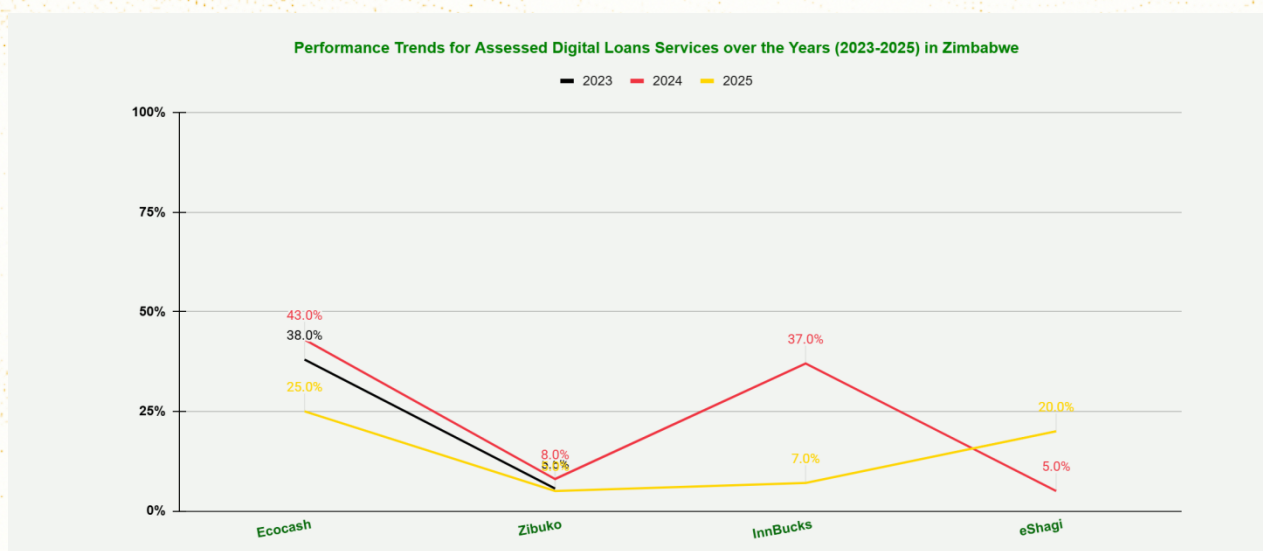
An assessment of data protection and privacy compliance among Finclub, Fundkiss, and Cim Finance shows differing trajectories between 2023 and 2025, reflecting varying levels of maturity in privacy governance and compliance within the digital loan services sector.

Finclub demonstrated steady improvement from 39.8% in 2023 to 43% in 2024, confirming the positive trend noted in last year's analysis. However, in 2025, its score declined slightly to 42%, indicating a minor regression. While this decrease is marginal, it suggests challenges in sustaining momentum or fully embedding privacy controls across operations. Overall, Finclub maintains a moderate level of compliance, but continued focus is needed to strengthen governance, monitoring, and implementation to prevent stagnation.

Fundkiss continued its upward trajectory beyond 2024. After improving from 34.7% in 2023 to 40% in 2024, the company further increased its score to 46% in 2025. This sustained improvement reflects consistent efforts to enhance data protection policies, operational controls, and staff awareness. Fundkiss's progress indicates growing compliance maturity and a stronger alignment with data protection and privacy requirements compared to previous years.

Cim Finance demonstrated stable and relatively strong performance, maintaining a score of 59% in both 2024 and 2025. Although 2023 data is not available for comparison, the consistent high score suggests that Cim Finance has established a mature data protection and privacy framework. The stability indicates effective governance structures and the ability to sustain compliance over time, positioning the institution as a sector leader.

Overall, the data reflects a gradual strengthening of data protection and privacy practices within the digital loan services sector, though progress remains uneven. Fundkiss shows clear and sustained improvement, while Finclub appears to be plateauing after earlier gains. Cim Finance continues to demonstrate comparatively strong and stable compliance. These findings underscore the importance of continuous investment in privacy governance, staff training, and monitoring mechanisms. Providers that sustain or improve compliance are better positioned to manage regulatory risk and maintain customer trust, while those experiencing stagnation risk falling behind evolving data protection expectations. Strengthening data protection and privacy practices remains critical to ensuring secure handling of sensitive financial and personal data in the digital loan services sector.



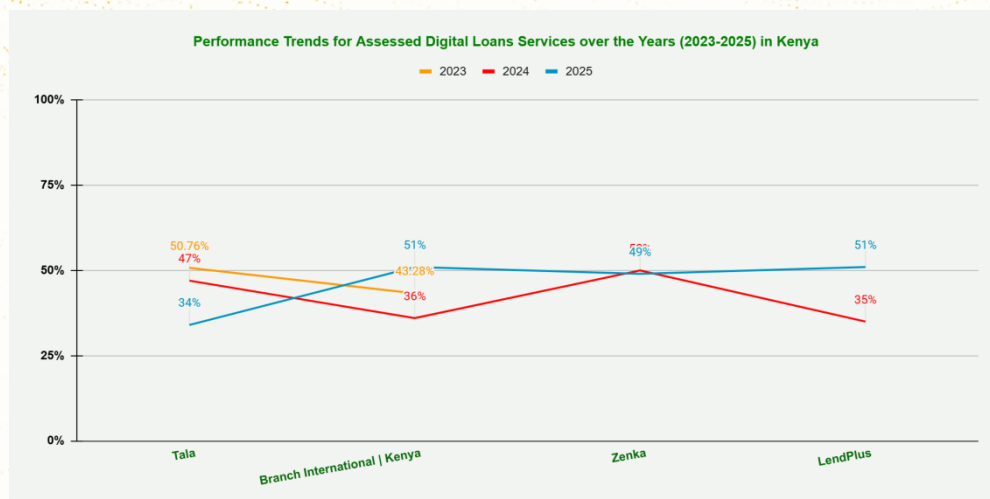
An assessment of data protection and privacy compliance among Ecocash, Zibuko, InnBucks, and eShagi shows mixed performance trends between 2023 and 2025, indicating uneven compliance maturity across the digital loan services sector.

Ecocash demonstrated positive progress from 38.0% in 2023 to 43.0% in 2024, as noted in last year's analysis, reflecting strengthened data protection practices. However, in 2025, its score declined significantly to 25.0%, indicating a marked regression. This drop suggests challenges in sustaining previously implemented privacy controls or adapting to evolving compliance requirements. Despite earlier progress, the 2025 decline exposes increased regulatory and reputational risks and underscores the need for renewed focus on maintaining robust data protection governance.

Zibuko showed a modest improvement from 5.6% in 2023 to 8.0% in 2024, consistent with the positive but limited progress highlighted in last year's analysis. In 2025, however, its score declined to 5.0%, effectively erasing the gains made in 2024. This regression highlights persistent weaknesses in privacy and data protection practices and suggests that compliance efforts have not been institutionalized.

InnBucks experienced a sharp decline, dropping from 37.0% in 2024 to 7.0% in 2025. Although 2023 data is unavailable, the steep reduction between 2024 and 2025 indicates a significant deterioration in data protection and privacy practices. This suggests serious gaps in governance, internal controls, or ongoing compliance monitoring, exposing the company to heightened data protection risks. eShagi demonstrated a notable improvement, increasing from 5.0% in 2024 to 20.0% in 2025. This upward trend indicates initial efforts to strengthen data protection measures and improve compliance maturity. While encouraging, the 2025 score remains relatively low, signaling that further work is required to establish a comprehensive and sustainable privacy framework.

Overall, the data reveals significant volatility in data protection and privacy compliance across digital loan service providers. While some platforms, such as eShagi, show encouraging improvement, others including Ecocash, Zibuko, and InnBucks have experienced notable regressions after earlier progress. These findings underscore the importance of sustained and institutionalized privacy governance, rather than one-off compliance initiatives. Providers with declining or unstable performance face increased risks of regulatory non-compliance, data breaches, and erosion of customer trust. Strengthening data protection and privacy practices through continuous monitoring, staff training, and investment in secure systems remains critical for ensuring the safe handling of sensitive financial and personal data in the digital loan services sector.



An assessment of data protection and privacy compliance among Tala, Branch International (Kenya), Zenka, and Lend-Plus reveals shifting performance trends between 2023 and 2025, highlighting varying levels of compliance maturity within the digital loan services sector.

Tala experienced a continued decline in performance over the review period. After dropping from 50.76% in 2023 to 47% in 2024, as noted in last year's analysis, Tala's score further decreased to 34% in 2025. This sustained downward trend indicates challenges in maintaining previously established data protection and privacy controls. While Tala had historically demonstrated relatively strong compliance, the decline suggests a need to reassess governance structures, monitoring mechanisms, and operational practices to prevent further regression and mitigate regulatory and reputational risks.

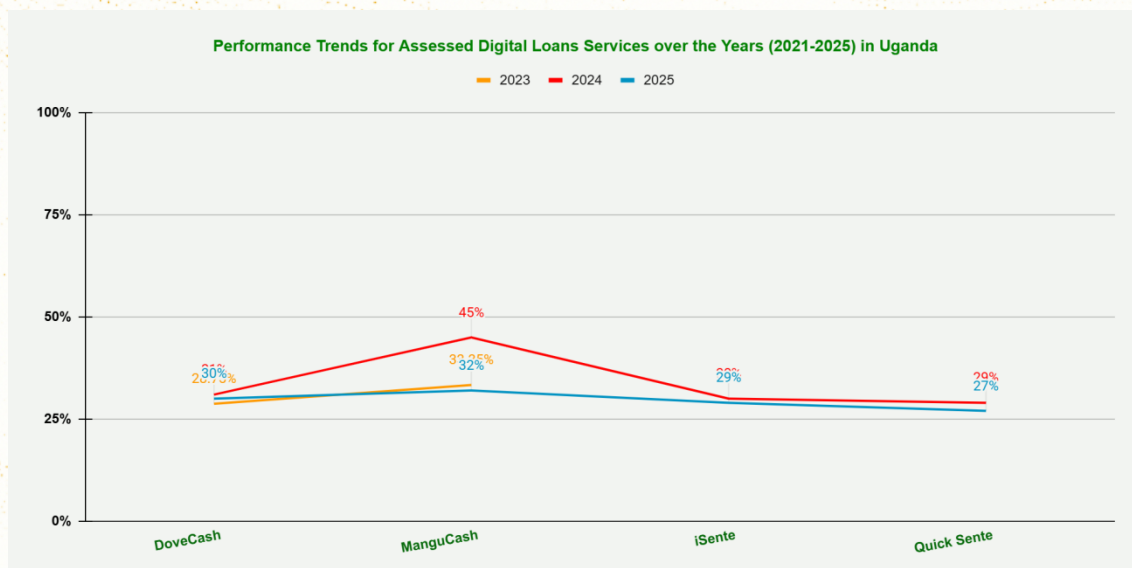
Branch International (Kenya) shows a recovery following the decline observed in 2024. After decreasing from 43.28% in 2023 to 36% in 2024, Branch improved significantly to 51% in 2025. This rebound suggests renewed focus on strengthening data protection policies, technical safeguards, and organizational accountability. The improvement positions Branch among the stronger performers in 2025, reflecting a more mature and proactive approach to privacy compliance.

Zenka maintained relatively stable performance, with a slight decrease from 50% in 2024 to 49% in 2025. Although 2023 data is unavailable, the marginal change suggests that Zenka has largely sustained its data protection and privacy practices. The consistently high score indicates a solid compliance foundation, though continued improvement is necessary to reach higher maturity levels and adapt to evolving regulatory requirements.

LendPlus demonstrated notable improvement, increasing from 35% in 2024 to 51% in 2025. This significant rise indicates substantial progress in strengthening data protection and privacy practices, potentially through improved governance, policy implementation, and staff training. The improvement reflects growing compliance maturity and a stronger commitment to safeguarding customer data.

Overall, the data reflects a dynamic and uneven compliance landscape within the digital loan services sector. While Tala shows a concerning downward trend, Branch International (Kenya) and LendPlus demonstrate that targeted corrective actions can reverse declines and significantly improve compliance outcomes. Zenka's stable performance suggests a relatively mature framework that requires ongoing reinforcement.

These findings underscore the importance of continuous monitoring, institutionalized privacy governance, and sustained investment in data protection measures. Digital loan providers experiencing declining performance face increased exposure to regulatory enforcement, data breaches, and erosion of consumer trust. Conversely, those demonstrating recovery or improvement are better positioned to manage compliance risks and maintain confidence in their handling of sensitive financial and personal data.



An assessment of data protection and privacy compliance among DoveCash, ManguCash, iSente, and Quick Sente shows mixed performance trends between 2023 and 2025, indicating varying levels of maturity in data protection practices across the digital loan services sector.

DoveCash demonstrated gradual improvement from 28.75% in 2023 to 31% in 2024, as highlighted in last year's analysis. However, in 2025, its score declined slightly to 30%, suggesting a minor regression. While the platform maintains a moderate level of compliance, the stagnation indicates challenges in sustaining momentum and fully embedding privacy controls. Continued investment in governance, monitoring, and staff awareness will be necessary to prevent further decline.

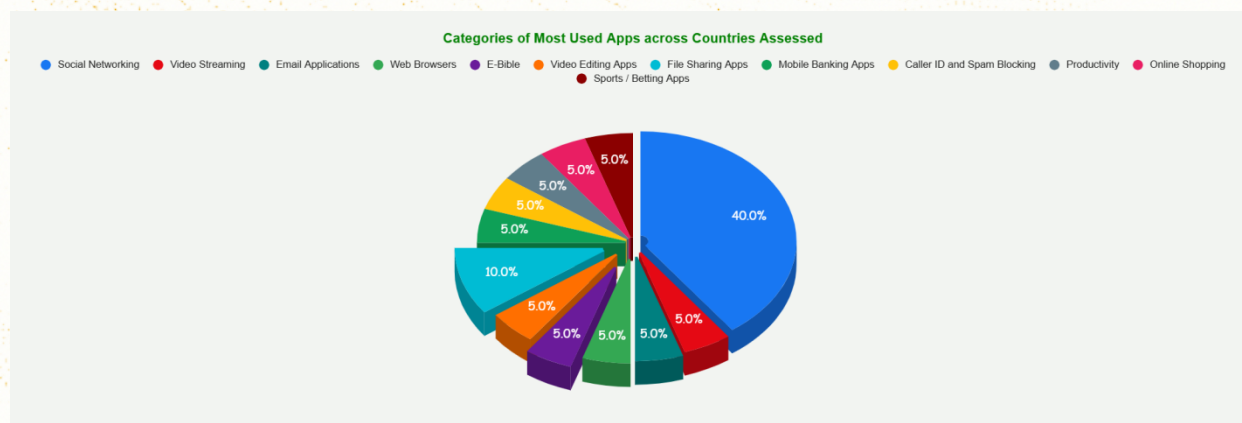
ManguCash showed strong progress from 33.35% in 2023 to 45% in 2024, confirming the positive trend noted previously. In 2025, however, its score fell significantly to 32%, representing a notable regression. This decline suggests difficulties in maintaining the enhanced privacy measures introduced in 2024, potentially due to gaps in ongoing compliance monitoring or institutionalization of controls. Despite earlier gains, the 2025 performance exposes renewed compliance risks.

iSente experienced a slight decline from 30% in 2024 to 29% in 2025. Although 2023 data is unavailable, the marginal decrease suggests relatively stable but modest compliance maturity. The scores indicate that while some privacy measures are in place, further strengthening is required to align with higher data protection standards.

Quick Sente also recorded a small decrease, dropping from 29% in 2024 to 27% in 2025. This downward trend, though limited, points to challenges in sustaining data protection practices. The consistently low-to-moderate scores highlight the need for stronger governance structures and more robust privacy controls.

Overall, the data indicates volatility and limited sustainability of data protection improvements among digital loan service providers. While some platforms, such as ManguCash and DoveCash, showed progress between 2023 and 2024, these gains were not consistently maintained into 2025. These findings underscore the importance of institutionalizing data protection and privacy measures, rather than relying on short-term compliance efforts. Providers with declining or stagnant performance remain vulnerable to regulatory non-compliance, data breaches, and erosion of customer trust. Strengthening governance frameworks, continuous compliance monitoring, and staff training will be critical to ensuring secure handling of sensitive financial and personal data within the digital loan services sector.

3.3 Overall Assessment of the most used Apps in the countries

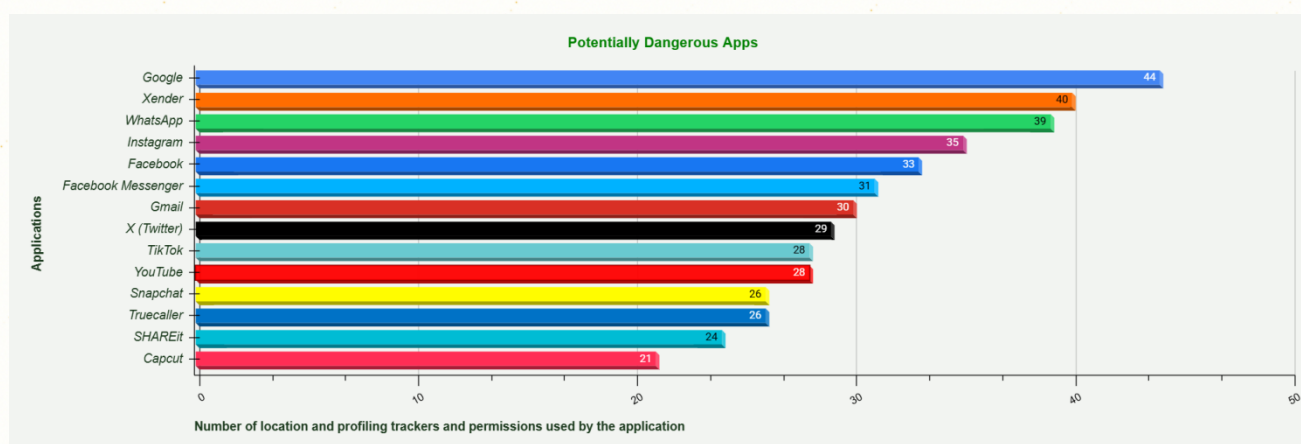


The assessment also reviewed the 20 most widely used mobile applications across the evaluated countries. Consistent with last year's findings, social networking apps remained the largest category, though their share declined to 40% of the top apps from 60% in the previous analysis. File-sharing apps were next at 10%, while the other categories including video streaming, email, web browsing, e-Bible apps, video editing tools, mobile banking, caller ID and spam blocking, productivity tools, online shopping, and sports/betting apps each accounted for 5%, down from about 6.7% each last year.

This relative decline in the prevalence of social networking apps signals weakening or inconsistent privacy protections, even as these platforms continue to process extensive sensitive personal data such as user profiles, interactions, location information, contacts, and behavior patterns. The regression may reflect expanded data uses (for example, for AI training or advanced advertising), increased third-party integrations, or slower adaptation to evolving regulatory requirements. Other app categories similarly lag, often lacking basic safeguards. The even lower performance among non-social categories underscores systemic shortcomings throughout the ecosystem.

These deficiencies have direct adverse effects on data subjects' rights under established national and international data protection frameworks. Fundamental rights related to information and transparency, access and portability, rectification and erasure, restrictions on processing and objection, and protection from automated decision-making are increasingly at risk, particularly in categories scoring below social networking apps such as mobile banking, email, web browsers, and file-sharing services. For instance, financial applications managing transaction data or browsers tracking user activity may expose individuals to extended data retention, unauthorized sharing, or breaches without sufficient mechanisms to exercise their rights. This erosion of protections undermines user autonomy and heightens the risk of identity theft, discriminatory profiling, and financial harm.

Across categories, common deficiencies include excessive collection of personal data beyond what is strictly necessary, inadequate encryption of data both in transit and at rest, opaque data-sharing practices with advertisers and partners, deficient consent mechanisms (such as pre-ticked boxes or bundled consents), and a lack of transparent reporting or comprehensive data protection impact assessments.



The figure above highlights **14 Apps** classified as potentially dangerous based on the number of embedded trackers and permissions, an increase from 10 last year indicating a growing risk in mobile privacy. *Trackers* are pieces of software embedded in apps to collect and store information about users' online behaviours, such as websites visited, links clicked,

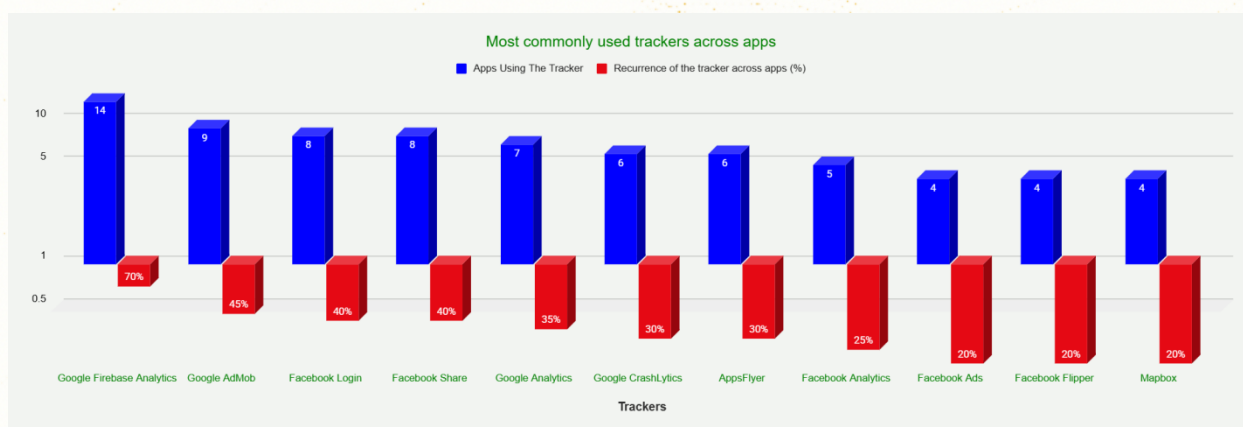
time spent in different features, device identifiers, and location data. While tracking can support useful functions like crash reporting and app performance analytics, it also enables detailed profiling and personalised advertising, often without clear user understanding or meaningful consent, posing significant privacy risks.

Several widely used apps demonstrate particularly high tracker counts. Googlebranded apps remain prominent, reflecting extensive data collection across services such as Search, Maps, Gmail, and YouTube, which can include location, browsing behaviour, and personal identifiers; this practice raises concerns about transparency and user control, and may trigger compliance issues under regulations like GDPR. Filesharing apps such as Xender similarly show high tracking activity despite their primary function not requiring such extensive data collection, suggesting potential use of collected data for profiling and advertising rather than core functionality.

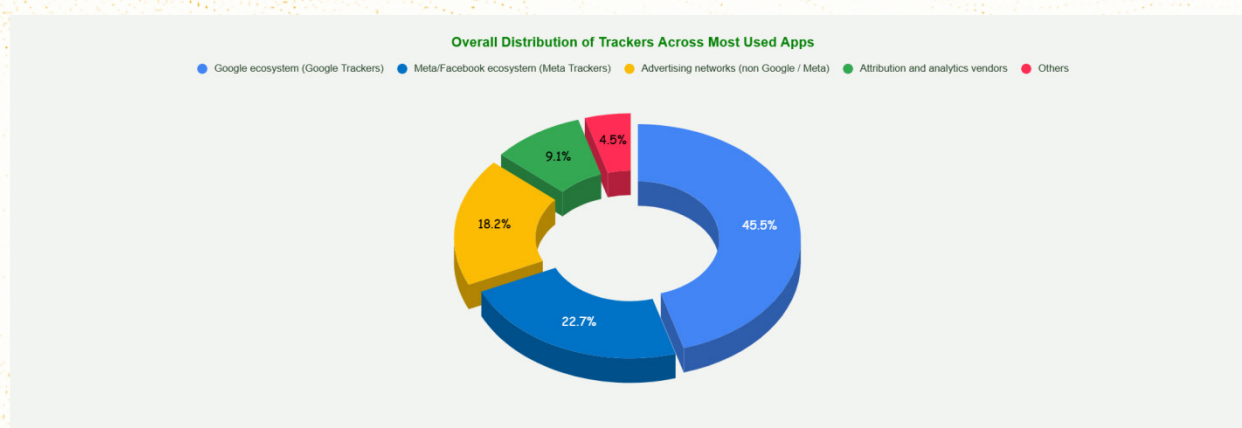
Messaging and social platforms like WhatsApp, Instagram, Facebook, X (formerly Twitter), and Facebook Messenger also exhibit substantial tracking. Although some apps offer encryption for communication content, trackers still collect metadata (e.g., device information and interaction patterns), which can be used to build detailed user profiles with limited transparency or control. Email and video platforms like Gmail and YouTube show similar patterns, where invisible trackers or behavioural data capture can reveal engagement behaviour and expose users to profiling or thirdparty data flows without explicit consent.

Other popular apps such as TikTok, Snapchat, Truecaller, SHAREit, and CapCut each contain significant tracker footprints despite disparate functions, amplifying broader privacy and data protection concerns across categories. In particular, tracking mechanisms that collect identifiers and behavioural signals can erode user autonomy and increase the risk of data sharing beyond necessary operational purposes.

Across this set of hightracker apps, key issues include a lack of clear disclosures and consent mechanisms, pervasive data collection that exceeds functional necessity, and limited user control over how personal information is used and shared with potential implications for profiling, targeted advertising, and security vulnerabilities such as data breaches. These findings underscore the urgent need for stronger transparency, improved consent practices, data minimization, and enhanced compliance with data protection principles to protect users' rights and personal data in a landscape where pervasive tracking has become the norm rather than the exception.



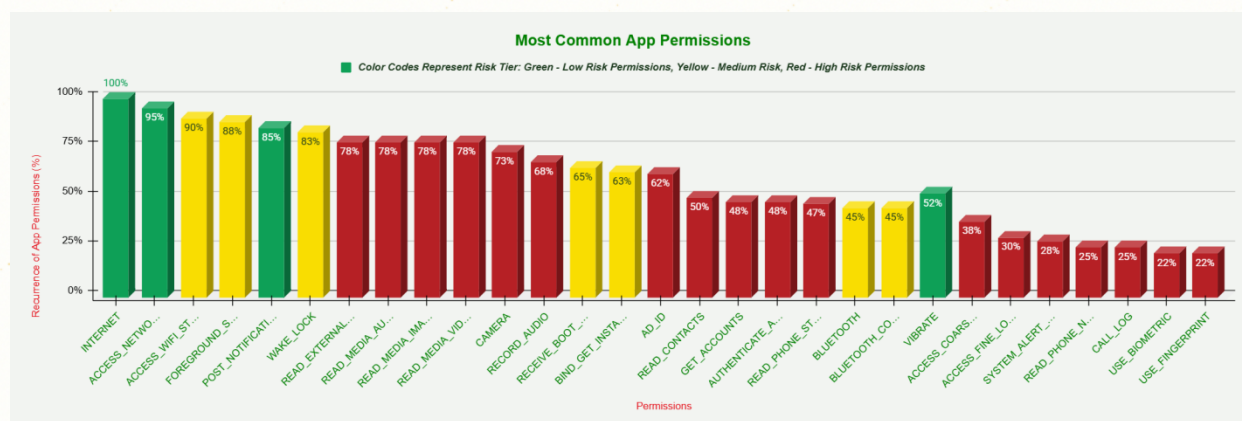
The analysis of trackers embedded in the most-used apps reveals a high concentration of a small number of recurring tracking technologies, rather than a diverse ecosystem. Google Firebase Analytics emerges as the most dominant tracker, appearing in roughly 70% of the sampled apps, followed by Google AdMob at approximately 45%, and Facebook (Meta) technologies such as Facebook Login and Facebook Share at around 40%. Google Analytics, Google Crashlytics, and AppsFlyer also show notable recurrence, each appearing in approximately 30–35% of apps. This pattern indicates that a limited set of trackers form the core surveillance infrastructure of popular applications. Importantly, most apps do not rely on a single tracker; instead, they deploy multiple trackers simultaneously, creating layered and overlapping data collection practices that significantly increase cumulative privacy risk.



In sum, the analysis shows that tracking in popular apps is highly concentrated and dominated by a small number of corporate ecosystems, rather than being evenly distributed across many providers. Google trackers account for almost half of all observed tracking activity (45.5%), while Meta (Facebook) trackers contribute nearly a quarter (22.7%), meaning that over two-thirds of user data flows are directed to just two companies. This dominance is driven by the widespread, often default, use of analytics, advertising, and identity SDKs that are deeply embedded in app development workflows and frequently deployed together within the same app.

While trackers are commonly justified as necessary for analytics, monetization, performance monitoring, and growth measurement, the findings indicate that their scale, persistence, and overlap significantly amplify privacy risks. Users are routinely exposed to layered tracking that enables cross-app aggregation, long-term profiling, and data sharing with third parties they have no direct relationship with or practical ability to avoid. As a result, the primary privacy concern is not the presence of any single tracker, but the cumulative impact of dominant tracking ecosystems, which systematically reduce user control, weaken meaningful consent, and pose material challenges to data protection and privacy rights.

A striking feature of the findings is the concentration of tracker ownership among a few large technology companies, primarily Google and Meta (Facebook). Google-owned trackers including Firebase Analytics, AdMob, Google Analytics, Crashlytics, and Tag Manager collectively appear in over 80% of the sampled apps, positioning Google as the dominant backend data processor across the mobile app ecosystem. Meta follows closely through Facebook Login, Facebook Share, Facebook Ads, and Facebook Analytics, which together appear in more than half of the apps analyzed. Attribution and advertising trackers such as AppsFlyer, Adjust, Unity Ads, Vungle, Mintegral, and Pangle further extend data flows to a broader advertising technology ecosystem. This concentration means that user data generated across ostensibly unrelated apps is frequently funneled to the same corporate entities, increasing the likelihood of cross-app aggregation, profiling, and long-term retention beyond the control or awareness of users.



App permissions are requests made by applications to access specific features or data on your mobile phone, such as your camera, contacts, location, or storage. These permissions are necessary for certain app functions. For example, a navigation app needs location access to provide directions, or a messaging app requires access to contacts to help you communicate. When used appropriately, permissions enable apps to deliver their intended services efficiently and securely. However, granting permissions without understanding their necessity can expose your personal data to misuse or compromise your privacy.

Excessive permissions could lead to potential risks like data breaches, targeted advertising, or unauthorized access to sensitive information. Examples of these are apps that request access to multiple sensitive areas like your camera, storage, location, and call logs without a clear justification for why all of these are needed.

Across the apps analysed, a relatively small set of permissions recur consistently, indicating common design patterns rather than app-specific necessity. The most prevalent permissions as highlighted in the above figure fall into three broad clusters: network and background operation permissions (such as `INTERNET`, `ACCESS_NETWORK_STATE`, `ACCESS_WIFI_STATE`, `WAKE_LOCK`, `FOREGROUND_SERVICE`, `RECEIVE_BOOT_COMPLETED`), media and sensor access permissions (including `CAMERA`, `RECORD_AUDIO`, `READ_EXTERNAL_STORAGE` and the newer `READ_MEDIA` variants), and identity, advertising, and account-related permissions (notably `GET_ACCOUNTS`, `AUTHENTICATE_ACCOUNTS`, `AD_ID`, and AdServices attribution permissions). Their high recurrence reflects the fact that most modern apps rely on persistent connectivity, background syncing, analytics, notifications, media sharing, and monetisation through advertising or in-app purchases.

From a functional perspective, many of these permissions are defensible in isolation. Network and foreground service permissions enable real-time messaging, media uploads, notifications, and smooth app performance; media and camera access supports core features such as photo sharing, video recording, and content creation; advertising and attribution permissions are used to measure installs, personalise ads, and sustain free-to-use business models. However, the privacy reality emerges when these permissions are combined and persist over time. Continuous network access paired with background execution and device wake locks allows apps to operate almost continuously, while media, microphone, and camera permissions create pathways to highly sensitive personal data. Advertising and account-related permissions further enable linkage between app activity, device identifiers, and user profiles, often across multiple services and apps.

The cumulative impact on user privacy is therefore significant. Rather than isolated data points, these permissions facilitate broad behavioural visibility, revealing where users are, who they communicate with, what media they create or consume, and how they interact with their devices. Even permissions considered “low risk” on their own such as network state or Wi-Fi access can meaningfully contribute to profiling when combined with identifiers and background operation. For a privacy scorecard, the key concern is not merely whether permissions are technically justified, but whether their scope, frequency, and persistence are proportionate, transparently disclosed, and meaningfully controllable by users. In practice, the high recurrence of sensitive and quasi-sensitive permissions suggests a structural imbalance where user data protection is often secondary to optimisation, monetisation, and convenience.

3.4 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.

3.4.1 Telecommunications Sector Analysis

3.4.1.1 Overview of the sector and data collectors evaluated

The telecommunications sector across Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda continues to anchor national digital transformation efforts, providing essential infrastructure for mobile connectivity, internet access, and digital financial services. The assessment covered major operators across these countries, including Nigeria’s MTN Nigeria, Airtel Nigeria, Globacom Limited, and 9Mobile; Ghana’s MTN Ghana, AT Ghana, Telecel Ghana, and Glomobile Ghana; and Botswana’s Mascom Wireless, BTC, Orange Botswana, and BoFiNet.

Across the region, telecom operators serve as primary custodians of large volumes of personal data due to their role in mobile communications, mobile money ecosystems, and increasingly digital service portfolios. Markets such as Kenya and Ghana demonstrate strong innovation and rapid uptake of mobile services with Safaricom, MTN Ghana, and Telecel driving expansion of 4G/5G networks and integrated digital platforms. Nigeria, the continent’s largest telecom market, continues to formalize its privacy and regulatory landscape, with its major operators handling complex, high-volume data environments.

Countries like Rwanda and Mauritius show steady advancement driven by national digital strategies and strong regulatory oversight, while Tanzania and Uganda maintain highly competitive markets characterised by widespread mobile money use and expanding broadband coverage.

Meanwhile, Botswana and Zimbabwe though operating in more constrained economic contexts, continue to rely on telecom operators such as Mascom, Orange Botswana, Econet, and NetOne to sustain digital connectivity and essential communication services.

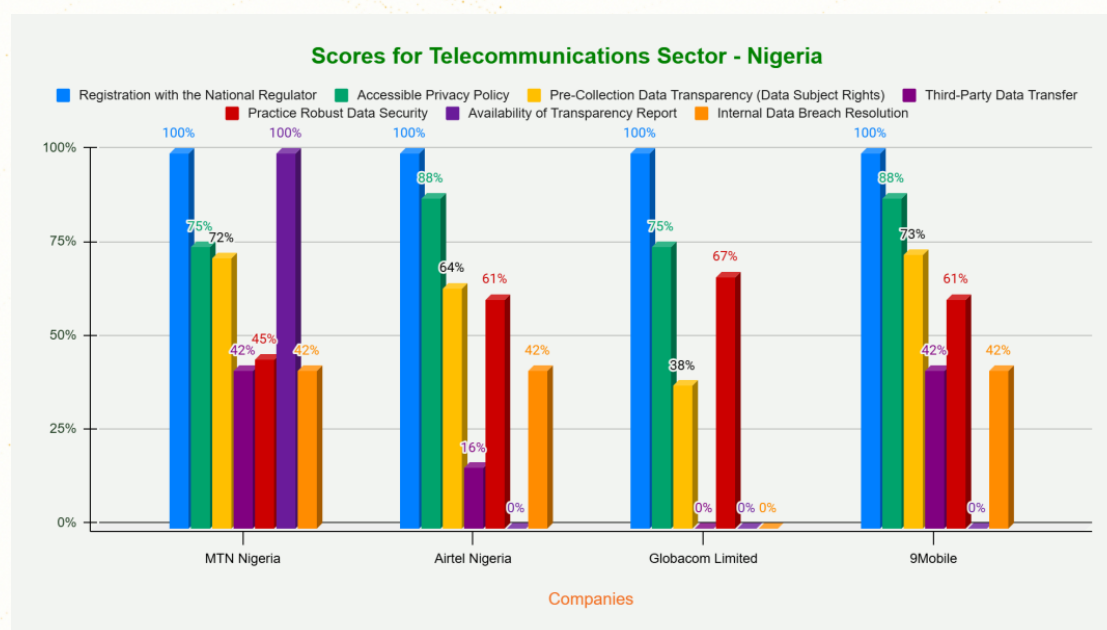
Overall, the sector is marked by growth, increasing data intensity, and expanding service diversification. Yet, this rapid evolution places significant responsibility on telecom companies to strengthen privacy governance, enhance transparency, and align more closely with emerging data protection frameworks. As digital infrastructure deepens and user reliance on telecommunications increases, the privacy practices of these operators remain central to consumer trust and regulatory compliance across the region.

3.4.1.2 Analysis of compliance with each criterion

In the telecommunications sector, the assessment covered 35 data collectors across the nine participating countries. These included: four operators each from Nigeria (MTN Nigeria, Airtel Nigeria, Globacom Limited, 9Mobile), Ghana (MTN Ghana, AT Ghana, Telecel Ghana, Glomobile Ghana), Tanzania (Vodacom, Tigo, TTCL, Airtel Tanzania), Mauritius (Emtel, Liquid Telecom, my.t, Atcomm), Zimbabwe (Econet, TelOne, NetOne, Liquid Telecom Zimbabwe), Kenya (Zuku, Safaricom, Jamii Telecommunications Limited, Airtel Kenya), and Uganda (MTN Uganda, Lycamobile, Airtel Uganda, Roke Telkom); and Botswana (Mascom Wireless, BTC, Orange Botswana and BonFiNet). In Rwanda (MTN Rwanda, Airtel Rwanda, Liquid Telecom Rwanda), three companies were assessed in the country due to market size and operator availability.

a. MTN Nigeria, Airtel Nigeria, Globacom Limited, 9Mobile in Nigeria

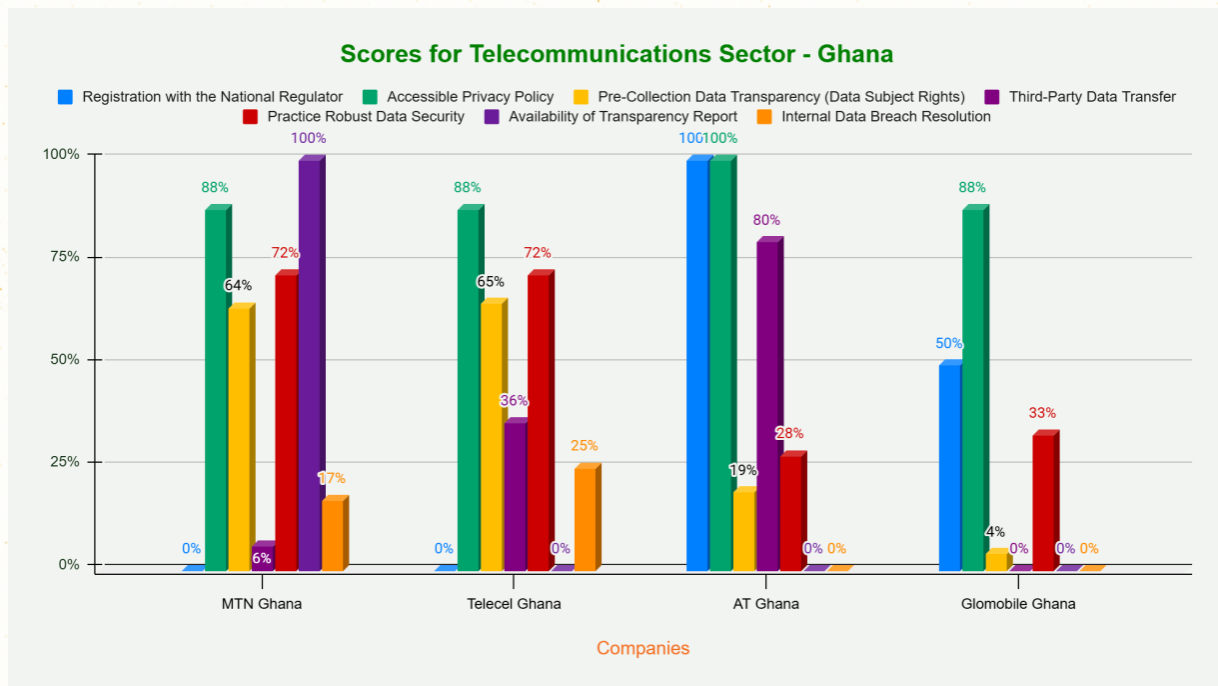
The data shows that while all four Nigerian telecom operators scored 100% on registration with the national regulator, their broader privacy practices differ sharply, revealing uneven compliance and consumer protection.



MTN Nigeria is the only operator with a 100% score for a transparency report and also leads alongside 9Mobile with 42% on third-party data transfer disclosures, though MTN performs poorly on security with 45%. Airtel Nigeria, Globacom Limited, and 9Mobile each scored 0% on transparency reports, and Airtel's third-party transfer score is low at 16% while Globacom scores 0%. On accessible privacy policies, Airtel Nigeria and 9Mobile lead with 88%, followed by MTN Nigeria and Globacom at 75% each. For pre-collection transparency and data-subject rights, 9Mobile scored 73%, MTN 72%, Airtel 64%, and Globacom the lowest. In security practices, Globacom leads with 67%, followed by Airtel and 9Mobile at 61%, while MTN trails with 45%. For internal resolution mechanisms, MTN, Airtel, and 9Mobile share the highest score of 42%, with Globacom again scoring the least. Overall, the scores indicate that while basic regulatory registration is universal, critical areas like transparency reporting, data-sharing clarity, security robustness, and user-rights protections remain inconsistent and expose customers to varying levels of privacy risk.

b. MTN Ghana, AT Ghana, Telecel Ghana, Glomobile Ghana in Ghana

The assessment of Ghana's telecommunications sector reveals a landscape of uneven privacy maturity, with operators showing wide variations in regulatory compliance, transparency, and data protection performance.



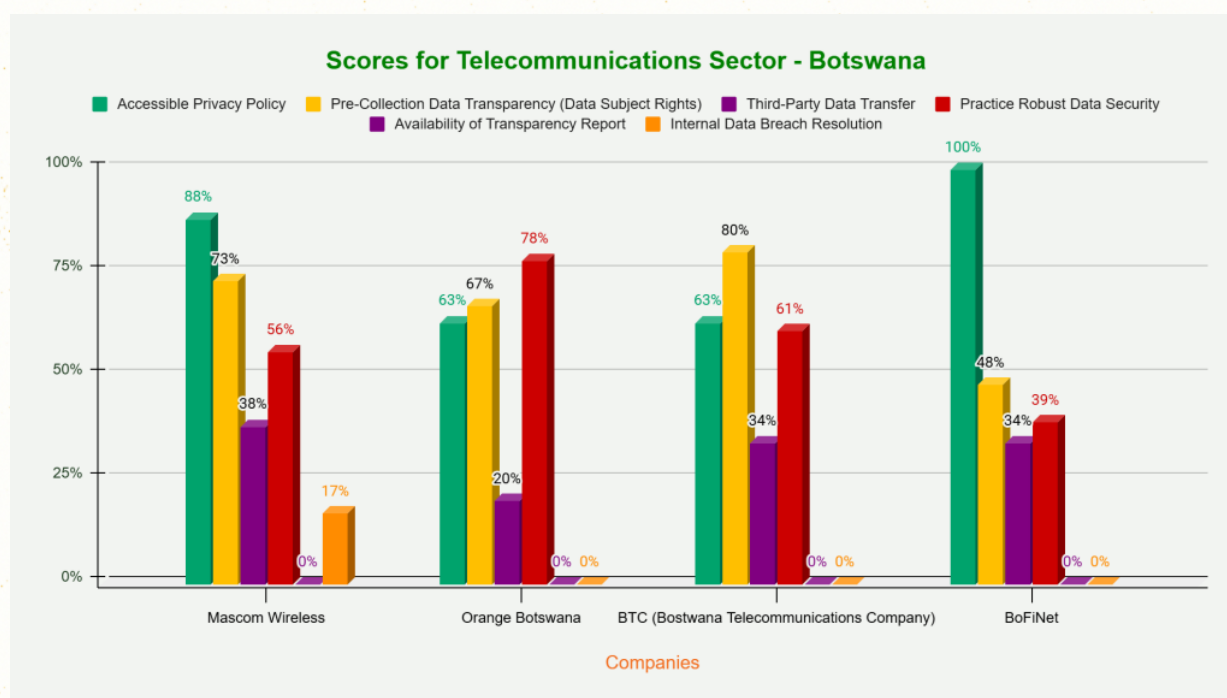
Registration with the national regulator sharply differentiates the companies: AT Ghana scores 100% and maintains an active registration, Glomobile Ghana scores 50% with an expired certification, while MTN Ghana and Telecel Ghana score 0%, signaling significant compliance gaps.

Transparency reporting is similarly inconsistent. MTN Ghana leads with 100%, Telecel follows with 36%, while AT Ghana and Glomobile score 0%, limiting visibility into government and law-enforcement data requests. Third-party data-transfer practices also vary: Glomobile Ghana scores 80%, MTN Ghana 6%, and AT Ghana and Telecel 0%, raising concerns about unclear or undisclosed data-sharing arrangements. Although AT Ghana provides the only fully accessible privacy policy (100%), the rest of the operators score 0%, and their policies rely heavily on technical language that reduces user comprehension.

Pre-collection transparency is strongest for Telecel Ghana (65%) and MTN Ghana (64%), while AT Ghana and Glomobile provide minimal detail on data categories, purposes, retention, or user rights. In terms of security, MTN and Telecel lead with 72%, but offer limited policy descriptions of safeguards; AT Ghana performs poorly despite acceptable SSL scores, and Glomobile trails with weak security practices. Internal resolution mechanisms remain underdeveloped across all operators, with Telecel scoring 25%, MTN 17%, and AT Ghana and Glomobile 0%, indicating weak channels for addressing user concerns. Overall, the sector exhibits fragmented and inconsistent privacy governance—despite isolated areas of strength, the combination of regulatory lapses, weak transparency, insufficient security detail, and inadequate user-protection mechanisms highlights a pressing need for stronger regulatory enforcement, clearer communication, and more robust privacy frameworks.

c. *Mascom Wireless, Wireless BTC (Botswana Telecommunications Company), Orange Botswana, BonFiNet in Botswana*

The performance of Botswana's telecommunications operators i.e., Mascom Wireless, BTC, Orange Botswana, and BoFiNet, reveals a sector with moderate but uneven privacy maturity, characterised by partial strengths alongside substantive gaps in transparency, user rights, security, and accountability.



All four operators did not have publicly available information to mount an evaluation on performance in respect of registration with the national data protection regulator, but maintained publicly accessible privacy policies. Indicator-level results highlight deeper weaknesses: no operator has published a transparency report (0%), third-party data-sharing disclosures remain limited (Mascom 38%, BTC and BoFiNet 34%, Orange 20%), and internal resolution mechanisms are severely underdeveloped, with Mascom scoring only 17% and all others 0%. Pre-collection transparency varies widely, BTC leads with 80%, followed by Mascom (73%), Orange (67%), and BoFiNet (48%), while security practices range from Orange's strong 78% to BoFiNet's modest 39%, exposing inconsistent implementation of technical and organisational safeguards. Privacy policy accessibility is strongest at BoFiNet (100%) and Mascom (88%), though accessibility often masks gaps in clarity, depth, and operational detail.

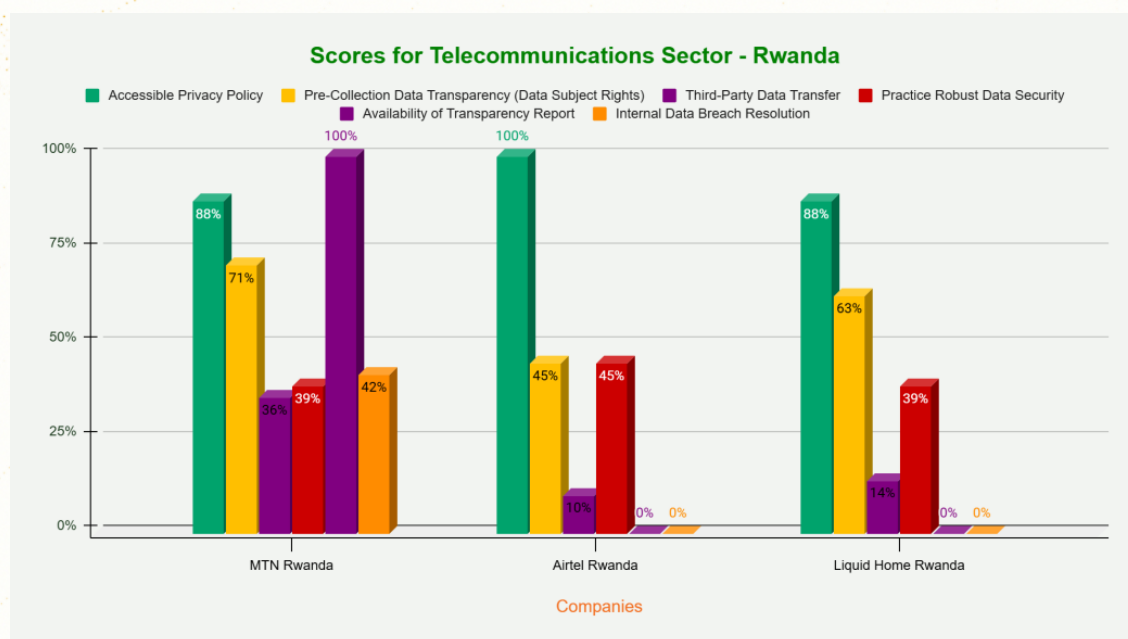
These quantitative findings align with the qualitative assessment of each operator's privacy posture. Mascom Wireless is among the stronger performers, offering a structured policy and restrictions on law-enforcement access, but its breach-handling procedures are vague and it lacks transparency reporting, weakening overall accountability. Orange Botswana provides one of the most comprehensive and user-friendly notices in the market, clearly articulating data categories, lawful bases, and user rights; however, insufficient detail on third-party recipients and silence on user breach notification create critical transparency gaps. BTC performs well on user-rights disclosures and offers strong DPO accessibility, yet its third-party sharing descriptions are incomplete and breach resolution mechanisms remain unclear. BoFiNet lags behind its peers: despite having a highly accessible policy, it offers minimal detail on user rights, security measures, or breach processes, resulting in the weakest overall privacy governance framework.

Overall, Botswana's telecom sector demonstrates basic regulatory compliance but lacks the depth, operationalisation, and consistency expected of a mature data-protection environment. The absence of clear breach-response procedures, user-notification obligations, comprehensive third-party disclosures, and updated transparency reporting (none published since 2023) leaves both consumers and operators exposed to significant risk. As Botswana strengthens its data-protection ecosystem, all four providers will face increasing pressure to elevate their privacy practices, moving beyond procedural compliance toward robust, user-centred, and accountable data-protection frameworks aligned with global standards and essential for sustaining public trust in a rapidly digitising economy.

d. MTN Rwanda, Airtel Rwanda and Liquid Telecom Rwanda in Rwanda

All three operators maintained publicly accessible privacy policies, with Airtel Rwanda leading at 100% availability, up from 75% in the previous assessment. Both MTN Rwanda and Liquid Telecom Rwanda also provided accessible policies, each at 88%, consistent with last year's results. In terms of pre-collection data transparency and data subject rights, MTN Rwanda scored highest at 71%, followed by Liquid Telecom Rwanda at 63%, indicating some progress in informing users about data practices before collection.

However, across all three operators there were notable gaps in compliance relating to third-party data transfers, data security measures, and internal breach resolution mechanisms each of which registered low levels of adherence to expected standards. Additionally, apart from MTN Rwanda, none of the operators published transparency reports, a deficiency that persisted from last year and highlights ongoing limitations in organizational accountability and public reporting. The figure presents further details on the performance, with an in-depth discussion of the three companies provided below.



All three operators; MTN Rwanda, Airtel Rwanda, and Liquid Home Rwanda continue to publish publicly accessible privacy policies that exceed minimum length requirements, ensuring baseline transparency for users. This year, Airtel Rwanda's privacy policy stood out for clarity and readability, achieving a Hemingway grade of 6 and a word count of 1,251, which contributed to its highest overall score of 100% among the three. MTN Rwanda's policy was the longest at 2,913 words but was less accessible in language, reflected in a Hemingway grade of 13 and an 88% score, while Liquid Home Rwanda's policy, at 1,591 words with a grade of 12, also scored 88%. Despite all meeting publication and accessibility benchmarks, differences in readability significantly affected their overall performance, with Airtel leading in clarity and user-friendliness.

Compared with last year, where all three companies similarly had privacy policies exceeding 200 words: MTN's at 2,878 words, Airtel's at 1,235 words, and Liquid Telecom's at 1,666 words, the readability landscape has shifted. Last year, MTN and Liquid Telecom's policies were deemed relatively readable, while Airtel's was more challenging for users to understand. This year's assessment shows improvements in Airtel's accessibility alongside continued readability challenges for MTN and Liquid Home, underscoring the importance of clear language in enhancing user comprehension.

A comparative review of last year's detailed analysis also highlighted specific strengths and weaknesses in the content of these policies. Liquid Telecom last year provided comprehensive coverage of data collection, retention, and user rights (including access, correction, objection, restriction, and deletion), and prohibited sharing data with advertisers, though it lacked specifics on data types collected, company contact information, and third-party recipients. MTN outlined data types collected and user rights, allowed permanent deletion, and required opt-in for advertising, but offered limited contact information and permitted broad third-party sharing without clear recipient lists. Airtel specified company contact details and data types collected but lacked defined retention periods and clear provisions on key user rights. Across all three, there was inconsistent handling of breach resolution and law enforcement access, revealing persistent gaps in data protection practice.

In security assessments conducted last year, SSL server scores varied (MTN: B; Airtel: A; Liquid Telecom: B), while security header scores were weaker overall (MTN: F; Airtel: D; Liquid Telecom: D). Only MTN's policy mentioned data security measures, albeit without specific detail, while Airtel and Liquid Telecom did not address data security explicitly in their policies.

Overall, while policy availability and publication have improved, significant differences remain in readability, transparency, and substantive content. Airtel Rwanda's gains in readability contrast with ongoing challenges for MTN and Liquid Home in making their policies fully accessible to users. Persistent gaps in clarity around data security, breach resolution, and third-party sharing highlight the need for continued enhancement of privacy communications to better inform and protect users.

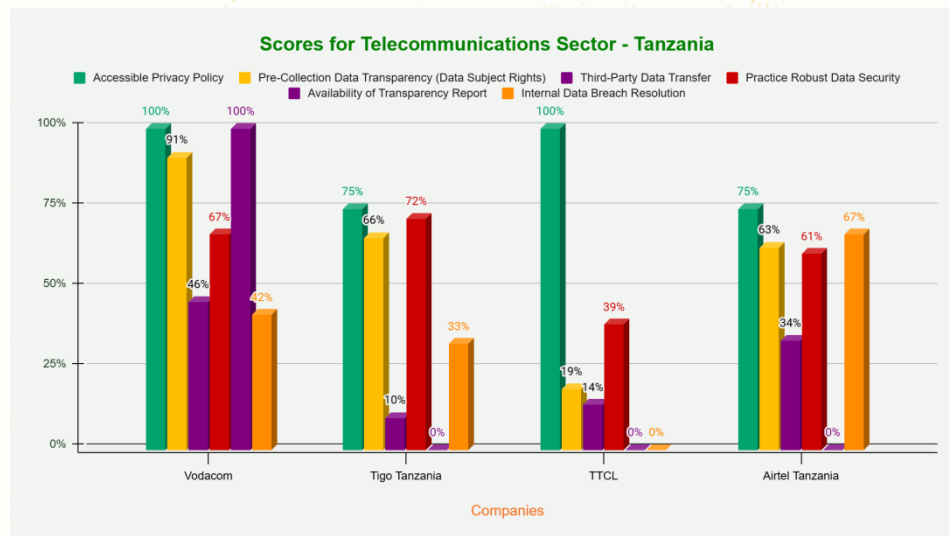
e. *Vodacom, Tigo Tanzania, TTCL and Airtel Tanzania from Tanzania*

As in the previous year, Vodacom and TTCL achieved perfect scores (100%) for the indicator measuring the accessibility of privacy policies, with Airtel Tanzania and Tigo Tanzania close behind at 75% each. Vodacom also remained the only operator to comply with the indicator for an available transparency report, consistent with last year's finding.

Performance on indicators relating to data subject rights and data security was relatively strong across the operators. Vodacom led in data subject rights compliance at 91%, followed by Tigo Tanzania at 66% and Airtel Tanzania at 63%. For data security, Tigo Tanzania was in the lead with 72%, with Vodacom at 67% and Airtel Tanzania at 61%.

In contrast, all operators performed poorly on the third-party data transfer indicator, with scores below 50%, indicating widespread gaps in transparency and controls over data shared with external entities. Similarly, compliance with internal data breach resolution mechanisms was generally low; Airtel Tanzania led this area at 67%, while the remaining companies scored below 50%.

Overall, Vodacom stood out for its consistent performance across multiple indicators, including privacy policy accessibility, transparency reporting, and data subject rights, while other operators demonstrated mixed performance with clear opportunities for improvement. The figure provides additional insights into these results, with a more detailed discussion presented below.



Vodacom and TTCL have the most accessible privacy policies, each scoring a full 100%. Vodacom's high score is supported by strong compliance in pre-data collection practices, particularly around transparency before data is gathered, with Tigo Tanzania trailing closely behind in this area. Despite this relative strength, all companies performed poorly on third-party data transfer indicators. Scores were low across multiple metrics, including whether personal data is shared with third parties and advertisers, whether those third parties are listed, whether the specific types of data shared are specified, whether data is shared only under lawful requirements (such as court orders), and whether multiple reporting channels (such as dedicated hotlines, online forms, or email addresses) are outlined for breach notifications. This suggests that effective checks and compliance mechanisms for data transfers to third parties are largely absent.

In terms of data security practices, Vodacom, Tigo Tanzania, and Airtel Tanzania show reasonable compliance, with policies that include relevant commitments and controls. In contrast, TTCL scores poorly; its policy mentions data privacy in general terms but lacks specific details on actionable security measures.

Vodacom also achieves a perfect score (100%) for transparency report availability, being the only operator that publishes a transparency report on its corporate website. All other companies score zero on this indicator due to the absence of any publicly accessible transparency reporting.

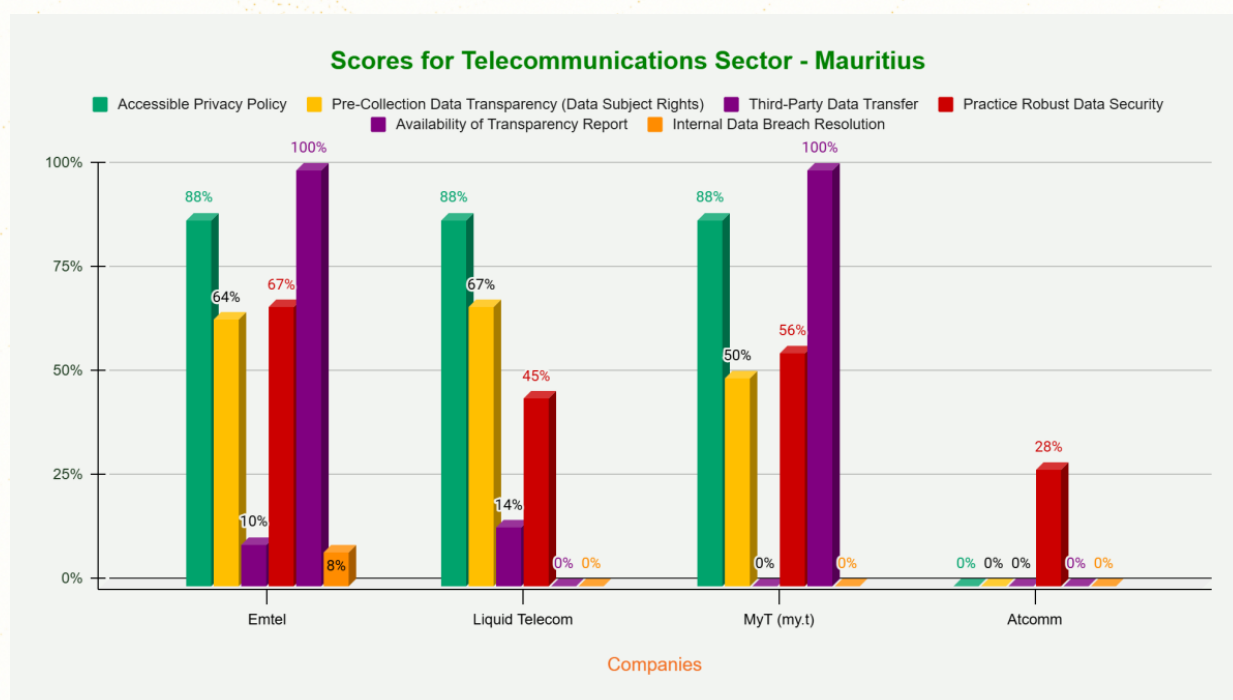
For internal data breach resolution, Airtel Tanzania performs best among the group. It scores fairly across most of the metrics but falls short in explaining how users can report a data breach. The other operators register lower performance in this area, indicating a broader need for clearer breach reporting and resolution mechanisms.

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

Of the four operators assessed, Emtel, Liquid Telecom, and MyT (my.t) each maintained accessible privacy policies, with all three scoring 88% on this indicator. Compared to last year, MyT declined from its previous perfect score of 100%, while Emtel and Liquid Telecom maintained their 88% standing from the prior assessment.

In the area of data subject rights, Liquid Telecom led with 67% compliance, followed by Emtel at 64% and MyT at 50%. This reflects varying levels of commitment to informing users about their rights to access, correct, restrict, or delete personal data rights confirmed in part by MyT's articulated data subject rights framework in its published privacy policy.

Consistent with last year, all operators demonstrated low compliance on third-party data transfer, with scores below 50%, indicating that none sufficiently disclose whether personal data is shared with third parties or detail the recipients and terms of such transfers.



For data security, Emtel led with 67%, followed by MyT at 56%, while Liquid Telecom and Atcomm scored below 50%. This suggests varied maturity in articulating and implementing security measures in policy provisions, with some operators lacking clear commitments to protect data against unauthorized access and breaches.

On transparency reporting, Emtel and MyT both achieved full compliance, being the only operators to publish transparency reports, whereas Liquid Telecom and Atcomm scored 0% for lacking any such reports. This mirrors last year's broader trend of limited transparency reporting across the sector.

Finally, all operators registered poor performance on internal data breach resolution, with Liquid Telecom, MyT, and Atcomm showing the weakest compliance. This indicates ongoing gaps in how companies describe breach detection, reporting channels, resolution procedures, and timelines an area that also featured prominently as a weakness in the previous year's assessment.

Overall, while basic privacy policy publication remains consistent, notable declines (e.g., MyT's drop in privacy policy accessibility) and persistent weaknesses in third-party transfer, breach resolution, and transparency reporting highlight the need for enhanced privacy governance and accountability across the telecom operators. The figure below provides additional information, with a more detailed discussion on the performance following.

g. Econet, TelOne, NetOne and Liquid Telecom Zimbabwe in Zimbabwe

TelOne and NetOne continued to lead in accessible privacy policy compliance, each scoring 88%, with Liquid Home Zimbabwe trailing at 63%.

Compared to last year, this represents a shift in leadership: Econet and Liquid Telecom Zimbabwe previously led with 63% on this indicator, while Liquid Home maintained a similar position. This change suggests that TelOne and NetOne have strengthened the visibility and accessibility of their privacy disclosures, an important baseline for user awareness and accountability.

On data subject rights, NetOne (81%) and Liquid Home (67%) recorded the highest compliance among the operators, indicating relatively stronger acknowledgement of users' rights to access, correct, object to, or delete their personal data. By contrast, other operators scored below 50%, showing persistent gaps in how clearly user rights are articulated and operationalised in published policies. This variation reflects uneven alignment with core data protection principles that emphasise transparency and user control.

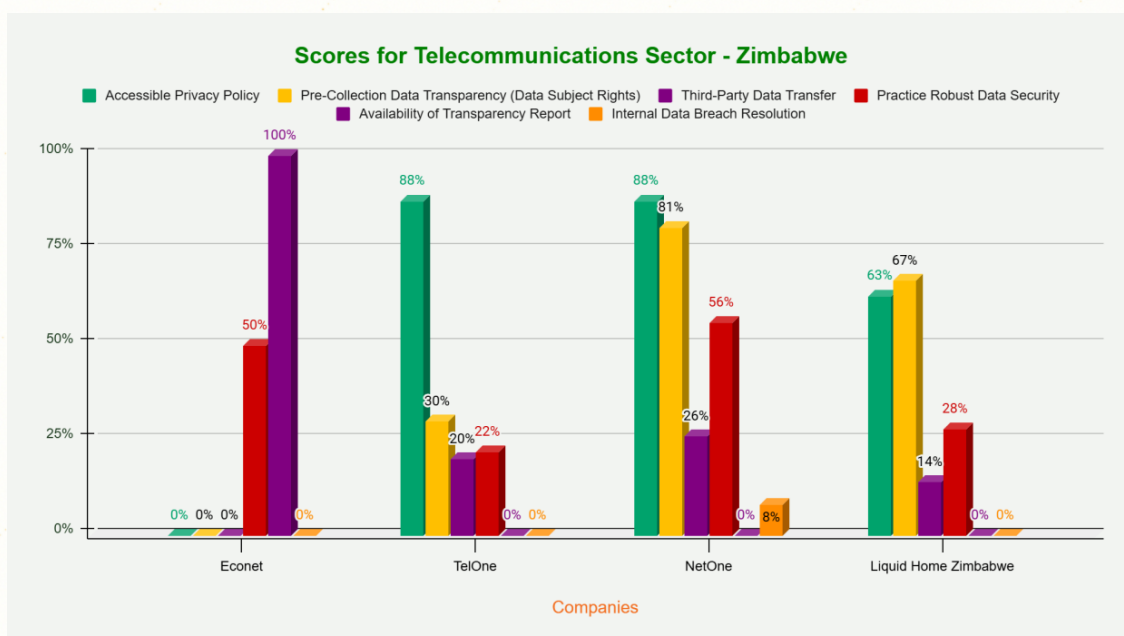
Across all operators, third-party data transfer compliance remained very low (below 50%), highlighting a systemic weakness in disclosing whether and how personal data is shared with external entities. This includes inadequate visibility on the categories of third parties, purposes of sharing, and safeguards to ensure lawful and secure transfers. Weaknesses in this area expose users to potential risks of unauthorized disclosure and reduce accountability for downstream data use.

In data security practices, NetOne and Econet led with moderate scores (56% and 50% respectively), but overall compliance among operators was low. This outcome suggests that while some policies mention data protection measures, few provide sufficiently detailed commitments or mechanisms to safeguard personal data against unauthorized access or breaches. Effective security practices are fundamental to building trust and demonstrating compliance with data protection requirements; low scores in this area may signal weak institutional controls or communication gaps in policy disclosures.

Only Econet published a transparency report, achieving a perfect score (100%) on this indicator, while TelOne, NetOne, and Liquid Home scored 0% due to the absence of such reports. Last year, Econet similarly stood alone in publishing a transparency report, reinforcing a persistent gap in corporate reporting and accountability across most operators. Transparency reports are critical for informing the public about data practices, governance, and accountability measures, and their absence undermines trust and inhibits external oversight.

All operators registered very low compliance on internal data breach resolution, indicating that few policies clearly outline how breaches are detected, reported, remediated, or how users are informed.

This weak performance is consistent with last year's findings, where internal redress mechanisms were similarly absent or poorly articulated. Lack of robust breach resolution mechanisms not only impedes operational readiness but also increases regulatory risk and diminishes user confidence in the operator's ability to protect personal data.



TelOne and NetOne as noted above, perform above average on accessible privacy policies, each presenting reasonably detailed and fairly readable policies that help users understand how their data is handled. In contrast, Econet performs poorly in this category, largely because it lacks a published privacy policy, while Liquid Home Zimbabwe records an average score, indicating room for improvement in clarity and accessibility.

Under the pre-data collection transparency indicator, NetOne stands out, providing a comprehensive list of the types of data it collects, the purposes for collection, and clear provisions on targeted marketing with an opt-out option. NetOne's approach aligns more closely with accepted data protection principles. Liquid Home Zimbabwe and TelOne follow, demonstrating some commitment to pre-collection transparency, while Econet again scores zero, reflecting an absence of clear disclosure practices.

All telecommunication companies perform poorly on third-party data transfer transparency, with Econet scoring zero. This suggests that most operators do not adequately disclose whether personal data is shared with external parties, the categories of third parties involved, or the safeguards in place an important gap in compliance with global data protection expectations.

In the area of data security practices, TelOne leads with the best performance, achieving a moderately fair score of 56% by detailing specific security measures in its policy. Liquid Home Zimbabwe scores the lowest (28%), indicating that its policy lacks substantive information on how data is protected against unauthorized access or compromise.

Econet redeems itself under the transparency report indicator, earning a perfect score for making its transparency report publicly available. None of the other companies publish a transparency report, highlighting a broader shortfall in meeting international best practices for data protection accountability and openness.

While some operators show improvements in privacy policy accessibility and recognition of data subject rights, the overall picture reveals significant structural weaknesses in their privacy practices. Across the board, there is low disclosure of third-party data sharing, minimal transparency reporting, inconsistent commitments to data security, and poor breach management practices, suggesting that many companies are not fully meeting expectations under contemporary data protection frameworks.

Such deficiencies not only undermine user trust but also expose companies to increased regulatory scrutiny and potential non-compliance with national and international data protection standards that require clear articulation of user rights, documented security controls, and transparent data governance practices.

In particular, performance on internal data breach resolution is very weak among all operators. The highest score recorded is 8% by NetOne, but this reflects only an indirect reference to breach-related details rather than a clearly articulated data breach process. Most companies do not meaningfully address how breaches are detected, reported, managed, or communicated to affected users, highlighting a widespread gap in institutional readiness and policy clarity.

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

All operators demonstrated full compliance with registration with the national regulator, with each scoring 100%, indicating that they are all formally recognised and subject to regulatory oversight. In terms of accessible privacy policies, JTL led with a perfect score (100%), followed by Zuku, Safaricom, and Airtel Kenya each scoring 88%, showing broad progress in making privacy statements publicly available and visible to users.

For the data subject rights indicator, Airtel Kenya took the lead at 68%, followed by Safaricom at 63% and Zuku at 56%, reflecting varying degrees of commitment to informing users about their rights and how to exercise them. These outcomes suggest a general trend toward enhancing user empowerment compared to last year, when detailed articulation of pre-collection transparency and rights was uneven across operators. In last year's analysis, Safaricom, JTL, and Airtel Kenya each scored 100% for accessible privacy policies, while third-party data transfer and internal breach resolution were areas of very low compliance across the sector.

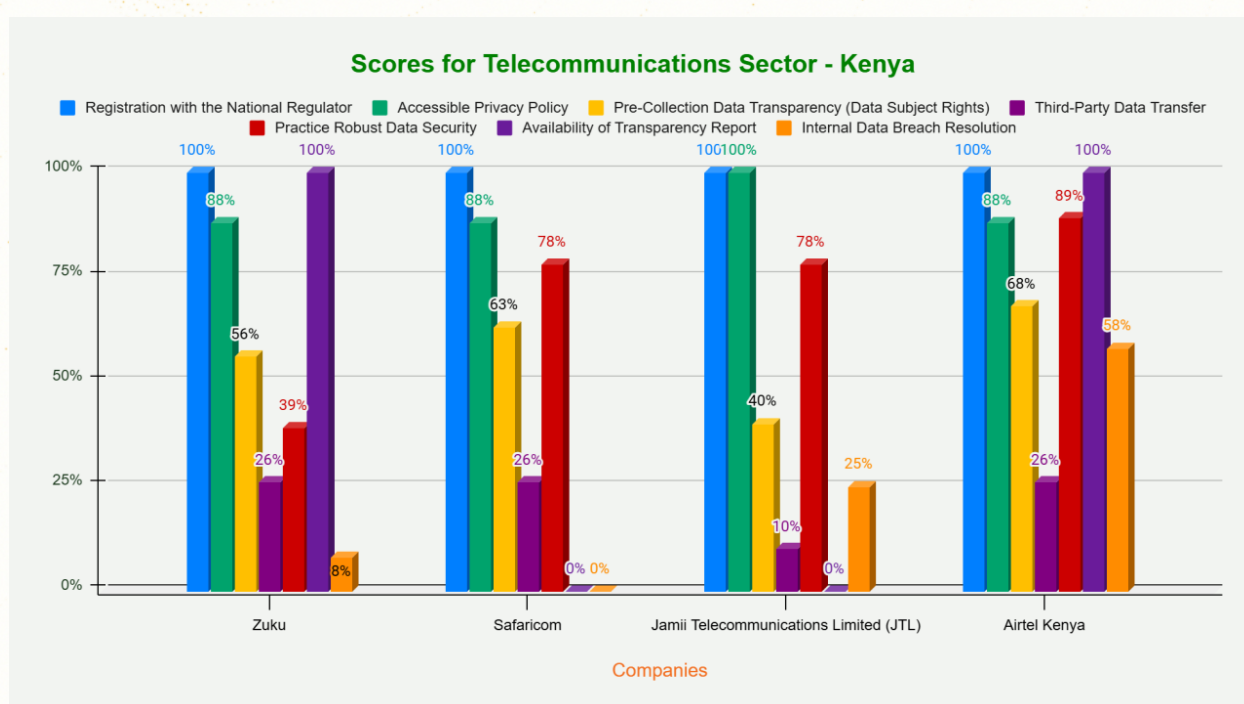
Despite this progress, all operators continue to score poorly on compliance with third-party data transfer indicators, with results below 50%. This persistent gap indicates that, while privacy policies are being published, there is still limited transparency around how and with whom personal data is shared outside the operator, undermining full compliance with data protection expectations and reducing users' ability to understand the flow of their information.

Under data security, Airtel Kenya leads with a strong score of 89%, followed by Safaricom and JTL each at 78%, indicating that these operators are comparatively better at articulating security commitments and measures to protect personal data. However, lower scores among others show that many operators still need to strengthen their security disclosures and practices in policy documentation.

On the transparency reporting indicator, Zuku and Airtel Kenya both achieved perfect scores (100%) by publishing transparency reports, while the remaining operators did not, reflecting uneven implementation of this accountability mechanism. The availability of transparency reports represents an important step toward openness and accountability, but the continued absence of such reports for some operators suggests that compliance with internationally recognised data protection practices remains inconsistent.

Finally, all operators scored low on internal data breach resolution, with Airtel Kenya leading at only 58%, while others scored below 50%. This indicates that few operators clearly outline in their policies how data breaches are detected, reported, and resolved, representing a continued weakness compared to last year, when internal breach resolution was one of the lowest-scoring indicators across the sector.

In sum, while there have been improvements in privacy policy accessibility and articulation of data subject rights, significant structural gaps remain, especially in third-party data transfer transparency, uniform security disclosures, and breach management practices. These weaknesses highlight that many operators are not yet fully aligned with contemporary data protection standards, potentially undermining user trust and exposing them to regulatory scrutiny as data protection laws increasingly emphasise transparency, accountability, and robust user safeguards. The figure below provides additional details on the performance, followed by a further discussion.



The telecommunications sector exhibits a wide range of privacy compliance, from Safaricom Kenya's industry-leading performance to Jamii Telecommunications' concerning low score. This variation reflects notable differences in how operators prioritise data protection, invest in governance frameworks, and respond to regulatory expectations.

Safaricom Kenya achieved a perfect compliance score (100%), demonstrating comprehensive implementation of privacy practices. The company's robust framework includes internationally recognised certifications such as ISO 27701 for Privacy Information Management Systems, which validates its commitment to structured privacy governance across services including customer support, billing, and mobile money operations. Safaricom also publishes detailed retention schedules and maintains dedicated privacy resources, contributing to its exemplary score.

Airtel Kenya performed with strong compliance, showing that international operators often benefit from global privacy governance models applied across multiple jurisdictions. Airtel's privacy policy includes extensive categorisation of personal data covering identity, contact, financial, location, device, and usage information, along with clear consent mechanisms and disclosures about third-party sharing. However, gaps remain, such as the lack of explicit reference to Kenya's Data Protection Act 2019 and absence of complaint procedures through the Office of the Data Protection Commissioner.

In contrast, Zuku Kenya scored poorly, underscoring ongoing compliance challenges. The company's weak score reflects deficiencies in its privacy policy, including the absence of specific data retention periods, incomplete data subject rights information, and limited transparency around third-party data sharing. Zuku has also faced regulatory enforcement actions, including a KES 500,000 fine by the Office of the Data Protection Commissioner (ODPC) for violations of data retention and unauthorized marketing practices, demonstrating the risks of inadequate compliance.

Jamii Telecommunications' extremely low score is the most concerning finding across the sector, indicating a near-absence of formal privacy protection measures despite serving a substantial customer base. The company lacks any publicly accessible privacy policy, violating basic transparency requirements under Kenya's Data Protection Act and warranting urgent regulatory investigation and enforcement.

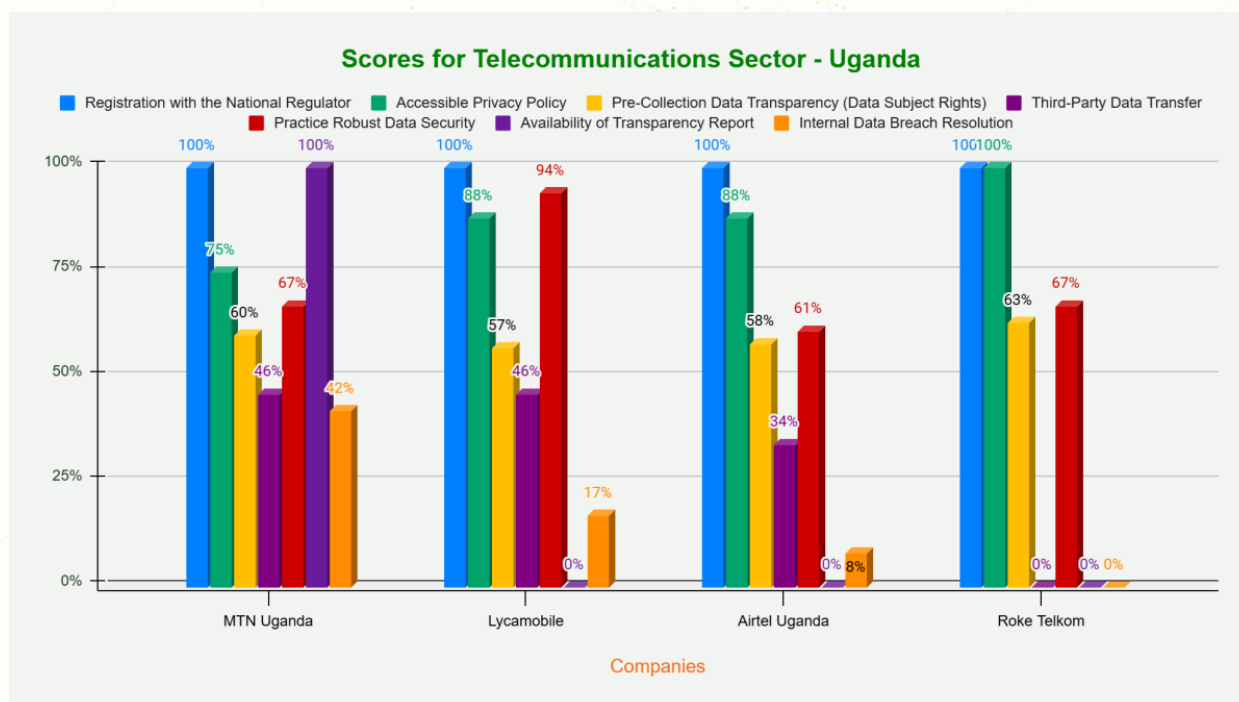
Comparison with last year shows a significant shift in the compliance landscape. Previously, both Safaricom and JTL maintained comprehensive and accessible privacy policies, with Safaricom's policy closely aligned to the Data Protection Act and including detailed user rights, lawful bases for processing, and engagement mechanisms, while JTL's policy similarly framed robust processing principles and safeguards. Last year, transparency reporting and enforcement readiness were largely absent across the sector.

The current assessment suggests that Safaricom has further strengthened its privacy practices, while other operators show mixed progress. Airtel's improved score reflects stronger policy articulation, but areas such as regulatory references and complaint channels still need enhancement. Meanwhile, Zuku's regulatory penalty highlights the concrete consequences of privacy non-compliance, and Jamii's lack of policy underscores persistent accountability gaps.

Overall, these findings highlight the critical importance of robust privacy governance, transparent data handling, and regulatory alignment within the telecommunications sector. Operators demonstrating strong frameworks such as Safaricom and Airtel Kenya are better positioned to build user trust and mitigate regulatory risks, whereas those with limited compliance face increased scrutiny, potential penalties, and reputational harm.

i. MTN Uganda, Lycamobile, Airtel Uganda and Roke Telkom in Uganda

MTN Uganda, Airtel Uganda, Lycamobile, and Roke Telkom remain the leading telecommunications operators in Uganda. MTN Uganda continues to dominate the market with approximately 22–22.8 million subscribers, representing nearly half of the national market, followed by Airtel Uganda with about 17.9 million subscribers. Consistent with last year's findings, MTN Uganda demonstrates relatively higher compliance across the seven assessed indicators, while systemic weaknesses persist across the sector. The figure offers additional insights into the performance, with a further discussion provided below.



All operators achieved full compliance (100%) with registration requirements under the national regulator, reflecting continued adherence to baseline licensing obligations. This marks an improvement from the previous year, when Lycamobile's status as a Mobile Virtual Network Operator (MVNO) limited regulatory oversight and contributed to compliance gaps. While all operators have publicly accessible privacy policies, their quality and effectiveness vary significantly. Roke Telkom continues to lead on accessibility and clarity of privacy policies, scoring 100%. Its policy is prominently published, concise (449 words), and written in clear language that is easy for the average user to understand.

Lycamobile and Airtel Uganda followed with scores of 88%, while MTN Uganda scored 75%, reflecting ongoing concerns also noted last year regarding the complexity and length of MTN's policy, despite its substantive strengths.

MTN Uganda remains the strongest performer on data collection transparency and user rights. As observed last year, MTN's policy clearly outlines the types of personal data collected and explicitly grants users rights to access, correct, delete their data, and lodge complaints. This continues to align well with DPPA requirements on lawful processing and data subject rights.

Roke Telkom and MTN Uganda recorded the highest scores on data subject rights this year (63% and 60%, respectively), with Lycamobile and Airtel Uganda also scoring above 50%. However, persistent gaps remain. Airtel and Lycamobile, as noted in last year's analysis, still fail to clearly articulate the purposes for data collection or comprehensively list third parties with access to user data. Roke Telkom continues to allow behavioral marketing without providing users with clear opt-in or opt-out mechanisms, a practice that raises consent and fairness concerns under data protection law.

All operators engage in third-party data sharing, yet compliance in this area remains weak, with all scores below 50%. While MTN Uganda, Lycamobile, and Airtel Uganda demonstrated incremental improvements compared to last year, Roke Telkom experienced a sharp regression, falling from 60% to 0%.

Last year, Roke Telkom's policy was noted for prohibiting third-party access to personal data; however, this position remains inadequately supported by clear breach reporting or accountability mechanisms. MTN, Airtel, and Lycamobile permit third-party access, but only MTN explicitly lists the categories of third parties involved, including enforcement and regulatory bodies, insurers, auditors, and advertisers. As in the previous year, none of the operators clearly specify the types of personal data shared, creating ongoing risks for users and undermining the principles of transparency and purpose limitation.

Lycamobile continues to exhibit serious deficiencies in this area, including lack of clarity on data retention periods, third-party data sharing, and law enforcement access. The previously identified unlawful practice of charging users UGX 43,000 to access their personal data contrary to the DPPA remains a stark example of non-compliance and weak enforcement. Lycamobile again recorded the highest score on data security (94%), consistent with last year's findings, followed by MTN Uganda and Roke Telkom (67% each), while Airtel Uganda continues to lag behind (61%).

Despite these scores, all operators performed poorly on internal data breach resolution mechanisms. As in the previous year, none of the companies provide robust processes for reporting, investigating, and remedying data breaches.

The highest score in this category was only 42%, indicating systemic weaknesses in accountability and risk management. MTN Uganda remains the only telecommunications operator to have published a transparency report, a practice it has maintained since 2023. This positions MTN as the sector leader in accountability and disclosure of government and third-party data requests. Airtel Uganda, Lycamobile, and Roke Telkom continue to offer no comparable insight, perpetuating opacity around state and commercial access to user data. While MTN also stands out for appointing a Data Protection Officer and establishing multiple channels for data subject complaints and whistleblowing, its overall performance is still constrained by policy complexity and limited specificity regarding the types of data shared with third parties.

Taken together, the findings reveal a pattern of incremental improvement without structural reform. MTN Uganda continues to set the benchmark for transparency, user rights, and governance, though it must improve policy clarity and data-sharing specificity. Roke Telkom excels in policy accessibility but lacks substantive safeguards around consent, third-party sharing, and breach accountability. Airtel Uganda's comparatively weaker security protections and limited transparency expose users to elevated risks, while Lycamobile's repeated non-compliance underscores significant enforcement gaps within Uganda's data protection regime. Without stronger regulatory enforcement and meaningful accountability measures, current practices risk entrenching a culture of formal compliance without effective protection of users' privacy rights.

3.4.1.3 Comparing companies' Performance within the sector

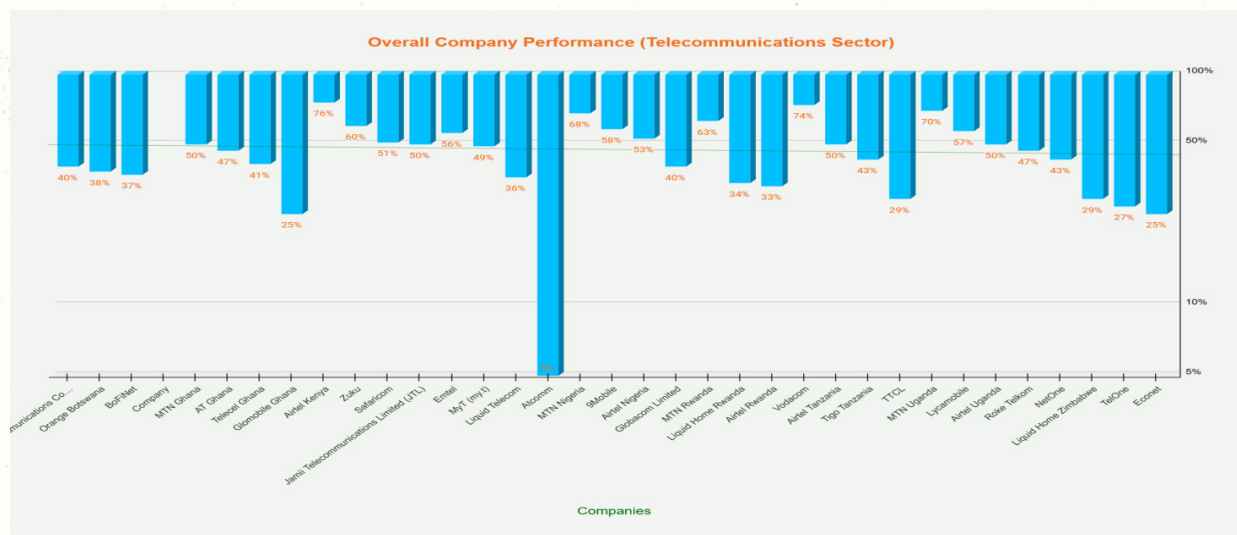
The overall scores across the telecommunications sector reveal wide disparities in privacy governance and compliance with national data protection frameworks, ranging from 76% (Airtel Kenya) to 5% (Atcomm, Mauritius). This reflects uneven maturity of data protection practices across jurisdictions. Compared with last year, the picture remains uneven but increasingly dynamic: while some operators and countries have made meaningful progress, others have stagnated or regressed.

The inclusion of Nigeria, Ghana, and Botswana deepens the comparative analysis, showing that these disparities are part of broader regional patterns. Countries such as Kenya, Uganda, Tanzania, and Nigeria demonstrate stronger or

improving compliance among leading operators, while Ghana and Botswana show clustered low-to-mid scores, pointing to systemic enforcement and accountability challenges. Overall, the findings reaffirm that privacy compliance in the telecommunications sector is neither linear nor guaranteed, and remains highly dependent on sustained regulatory oversight and corporate commitment.

High-Performing Jurisdictions: Emerging Compliance Leaders (and Trajectories)

Broadly, Kenya, Uganda, Tanzania, Nigeria, and Rwanda continue to show stronger average performance, with multiple operators improving year on year. In contrast, Botswana, Ghana, Zimbabwe, and parts of Mauritius remain clustered at the lower end, reflecting persistent systemic challenges in enforcement, accountability, and institutional capacity.



Kenya remains the strongest-performing jurisdiction overall. Airtel Kenya's score of **76%** represents both sectoral leadership and a significant improvement over last year, signalling deepening institutionalisation of privacy governance under Kenya's Data Protection Act. Zuku (**60%**) maintains a solid mid-upper position, while Safaricom's slight decline from last year (to **51%**) suggests relative stagnation rather than outright non-compliance. Safaricom's trajectory indicates that even dominant incumbents risk being overtaken if privacy reforms are not continuously strengthened.

Uganda continues to demonstrate notable progress. MTN Uganda's score of **70%** reflects consolidation of its leadership position following last year's already strong performance (69%). This stability indicates sustained investment in governance, transparency, and user rights, though further gains appear incremental rather than transformative. Lycamobile's rise to **57%** marks one of the most dramatic improvements in the region, contrasting sharply with its low score last year and suggesting corrective action following earlier compliance failures. Airtel Uganda's improvement to **50%** also reflects gradual progress, while Roke Telkom's decline to **47%** highlights how strengths in policy accessibility have not translated into sustained accountability, particularly around third-party data sharing and breach management.

Tanzania shows one of the clearest examples of upward momentum. Vodacom's increase to **74%** positions it among the top regional performers, reflecting substantial improvements since last year in data security, transparency, and governance structures. Airtel Tanzania's movement to **50%** and Tigo's rise to **43%** suggest partial progress, though compliance remains uneven and concentrated among leading operators.

Mid-Range Performers: Partial Compliance and Structural Gaps (with Change Over Time)

Nigeria presents a mixed but improving picture. MTN Nigeria (**68%**) and 9Mobile (**58%**) continue to strengthen their compliance posture, maintaining or improving upon last year's relatively strong scores. Airtel Nigeria (**53%**) shows modest progress, while Globacom (**40%**) remains a laggard. These divergences suggest uneven internalisation of Nigeria's Data Protection Act, where improvements are driven more by company-level governance capacity than by uniform enforcement.

Rwanda reflects a similar pattern. MTN Rwanda's increase to **63%** confirms steady year-on-year progress and positions it as a national leader. In contrast, Liquid Home Rwanda (**34%**) and Airtel Rwanda (**33%**) remain largely stagnant, underscoring gaps between multinational operators and smaller providers in compliance capacity.

Mauritius continues to display sharp internal contrasts. Emtel (56%) and MyT (49%) show moderate but largely static performance, while Liquid Telecom's slight decline to 36% and Atcomm's unchanged 5% point to persistent non-compliance. The lack of improvement by Atcomm, despite Mauritius' mature data protection framework, suggests weak enforcement rather than legal inadequacy.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

Botswana, Ghana, and Zimbabwe remain clustered at the lower end, with little year-on-year differentiation. In **Botswana**, Mascom Wireless (45%), BTC (40%), and Orange Botswana (38%) all remain within a narrow band, showing no clear leaders and little movement over time. This stability at low-to-mid levels suggests delayed operationalisation of data protection obligations.

Ghana shows modest top-end stability, with MTN Ghana at 50%, but a steep drop-off among smaller operators, particularly Glomobile Ghana (25%). Compared to last year, this indicates persistent unevenness rather than broad sectoral improvement.

Zimbabwe remains the weakest jurisdiction overall. Although NetOne's rise to 43% represents a significant improvement from an extremely low base last year, the sector as a whole continues to underperform. Econet's sharp decline to 25%, alongside persistently low scores for TelOne (27%) and Liquid Home Zimbabwe (29%), signals regression among incumbents and weak regulatory accountability across the market.

Key Cross-Cutting Implications

- **Improvement is possible but fragile:** Companies such as Vodacom Tanzania, Lycamobile Uganda, and MTN Rwanda demonstrate that targeted reforms can rapidly improve compliance, but regressions by Roke Telkom and Econet show gains are easily reversed.
- **Market leaders increasingly set the privacy baseline:** Multinational operators particularly MTN, Airtel, and Vodacom continue to outperform peers, benefiting from cross-border compliance frameworks and regulatory exposure. However, leadership is not guaranteed without continuous investment.
- **Enforcement, not law, is the differentiator:** Persistently low performers in Mauritius, Zimbabwe, and Botswana illustrate that strong legal frameworks alone do not ensure compliance without audits, sanctions, and follow-through.
- **Transparency, breach accountability, and third-party data sharing remain sector-wide weaknesses:** Even among top performers, scores plateau below 80%, indicating that advanced practices such as detailed transparency reporting and robust breach response mechanisms are still not fully institutionalised.

Taken together, the analysis shows a telecommunications sector marked by uneven progress and widening divergence. While countries such as Kenya, Uganda, Tanzania, Nigeria, and Rwanda demonstrate emerging leadership and improvement among key operators, others remain trapped in low-compliance equilibria. Without sustained regulatory oversight and internal accountability, these disparities risk entrenching a two-tier system of privacy protection, where users' rights depend more on the operator they choose than on the guarantees of national data protection laws. Continuous monitoring, enforcement, and corporate investment in privacy governance remain essential to closing this gap and aligning sector practices with both national and international data protection standards.

3.4.2 e-Commerce Sector Analysis

3.4.2.1 Overview of the sector and data collectors evaluated

E-commerce across East, West, and Southern Africa continues to grow rapidly, driven by increased internet access, widespread smartphone use, expanding digital payment systems, and changing consumer behaviour. This growth has made e-commerce a key economic driver while significantly increasing the volume and sensitivity of personal data collected by online platforms.

The assessment covers a diverse set of markets, including Kenya, Uganda, Rwanda, Tanzania, Mauritius, Zimbabwe, and newly assessed countries-Nigeria, Ghana, and Botswana. Kenya remains a regional leader in digital innovation and online marketplaces, while Uganda and Tanzania show steady growth in mobile commerce. Rwanda continues to advance through strong government-led digital transformation, and Mauritius benefits from mature digital infrastructure and cross-border e-commerce activity. Despite economic constraints, Zimbabwe's e-commerce sector continues to expand, particularly through social-commerce models. Nigeria, as Africa's largest digital market, plays a critical role in shaping regional e-commerce practices, while Ghana and Botswana reflect emerging but steadily growing online retail ecosystems.

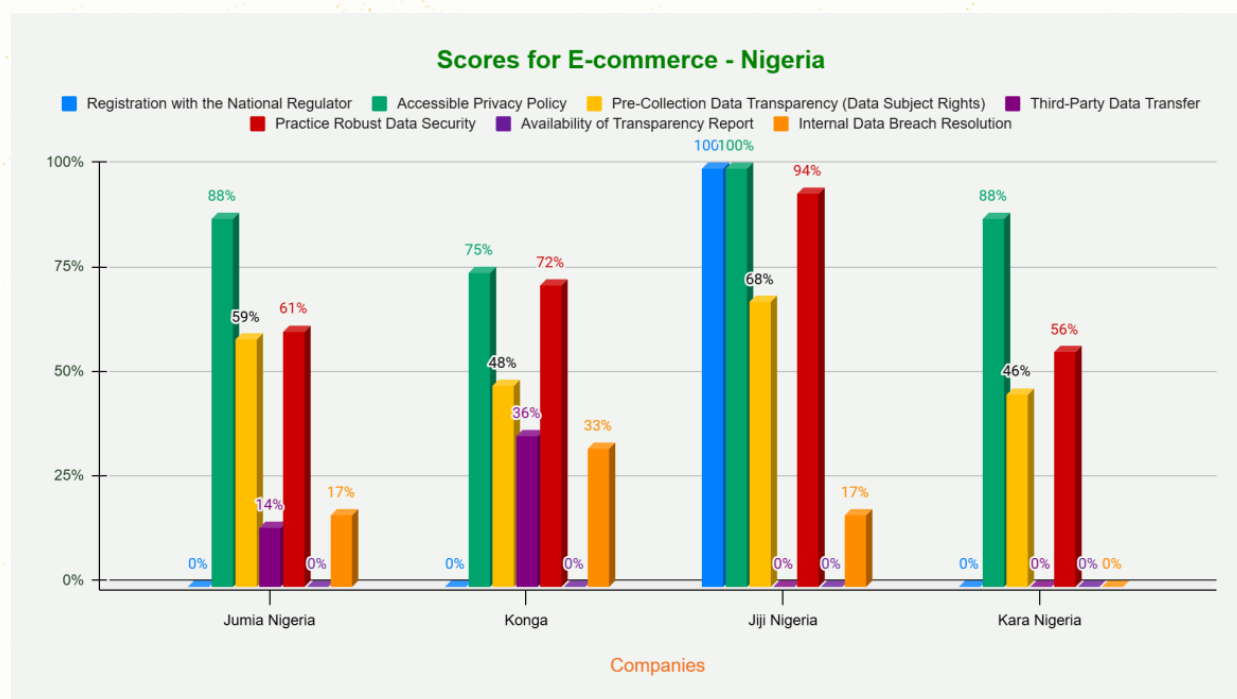
The data collectors evaluated include regional and national e-commerce platforms, digital retailers, and service providers that process large volumes of personal data, including identity, contact, payment, location, and behavioural information. As e-commerce expands, the analysis examines how these actors comply with national data protection laws, focusing on transparency, user rights, data security, and accountability in the handling of personal data.

3.4.2.2 Analysis of compliance with each criterion

This section analyses data from 36 e-commerce platforms, with four (4) platforms assessed in each country. The platforms reviewed include Jumia Nigeria, Konga, Juji Nigeria, and Kara Nigeria in Nigeria; Jumia Ghana, Tonaton Ghana, Melcom Ghana, and Kikuu Ghana in Ghana; Your Mart, Ubuy Botswana, iStore Botswana, and Apex Mart in Botswana; Murukali, Vuba Vuba, Kikuu Rwanda, and Ubuy Rwanda in Rwanda; Kikuu Tanzania, Jiji Tanzania, Inalipa, and Kupatana in Tanzania; PriceGuru, Temu Mauritius, Marideal, and Woolworths Mauritius Online in Mauritius; Ubuy Zimbabwe, Shumba Africa, Raines Africa, and Tengai Online in Zimbabwe; Jumia Kenya, Glovo Kenya, Jiji Kenya, and Kilimali in Kenya; and Jumia Uganda, Glovo Uganda, Jiji Uganda, and Kikuu Uganda in Uganda. Each of these platforms was evaluated against the assessment criteria, and their respective performance outcomes are presented below.

a. *Jumia Nigeria, Konga, Juji Nigeria and Kara Nigeria in Nigeria*

The assessment of Nigeria's e-commerce platforms reveals uneven compliance with national data protection obligations, with significant disparities in regulatory engagement, transparency, and accountability. Jiji Nigeria was the only platform found to be registered with the national data protection regulator, achieving a perfect score of 100%. No publicly available evidence of registration was identified for Jumia Nigeria, Konga, or Kara Nigeria, indicating potential non-compliance with mandatory registration requirements and gaps in formal regulatory oversight under Nigeria's data protection laws.



All assessed companies demonstrated efforts to maintain accessible privacy policies, reflecting a general recognition of transparency obligations. Jiji Nigeria again led with 100%, followed by Jumia Nigeria and Kara Nigeria (88% each), and Konga (75%). However, the variation in scores reflects differences in clarity, accessibility, technical functionality, and the overall comprehensiveness of privacy disclosures. With respect to data subject rights, performance was uneven. Jiji Nigeria ranked highest at 68%, followed by Jumia Nigeria at 59%, while Konga and Kara Nigeria scored below 50%. This suggests that several platforms do not fully enable users to exercise their statutory rights to access, correct, or delete personal data, as required under Nigeria's Data Protection Regulation (NDPR).

All platforms reported sharing personal data with third parties, yet compliance in this area was particularly weak. Konga, which led this indicator, scored only 36%, while Jumia Nigeria scored 14%. Limited transparency regarding the identities of third parties, the types of data shared, and the purposes of sharing increases the risk of unlawful processing and exposes users to potential misuse of their personal information. Efforts to ensure data security were observed across all platforms, with Jiji Nigeria leading at 94%, followed by Konga (72%), Jumia Nigeria (61%), and Kara Nigeria (56%).

While these scores indicate a degree of commitment to safeguarding personal data, gaps remain, particularly among mid-performing platforms, leaving users vulnerable to security breaches and undermining full compliance with data protection principles.

None of the platforms published transparency reports, and all recorded very low compliance with internal data breach resolution mechanisms. Konga led marginally with 33%, while Jiji Nigeria and Jumia Nigeria scored 17% each. The absence of clear procedures for breach detection, investigation, notification, and remediation highlights a systemic accountability gap that undermines both regulatory compliance and user trust.

Jiji Nigeria emerged as the strongest performer in the sector, demonstrating the closest alignment with Nigeria's data protection laws. Its privacy policy reflects a sophisticated understanding of online marketplace privacy risks, providing detailed contact information and clearly outlining extensive categories of personal data collected, including seller and buyer information, transaction records, communication logs, and behavioral analytics. The policy transparently explains purposes for data collection such as marketplace operations, fraud prevention, customer support, and service improvement and includes specific retention commitments, such as 90 days for facial verification data, enabling users to understand data lifecycle management. Jiji also demonstrates strong transparency around third-party data sharing, explicitly naming payment processors (Flutterwave, Paystack), cloud service providers (Amazon Web Services, DigitalOcean), and identity verification services, alongside safeguards. Comprehensive procedures for exercising data subject rights and clear conditions for lawful law enforcement access further strengthen its compliance posture.

Konga demonstrates moderate compliance, addressing most foundational privacy requirements but with limited depth. Its policy provides basic contact information, outlines general categories of data collected, and explains broad purposes such as order fulfilment, customer service, and marketing. While Konga implements standard data subject rights and acknowledges third-party sharing, the lack of procedural detail and specificity reduces practical accountability.

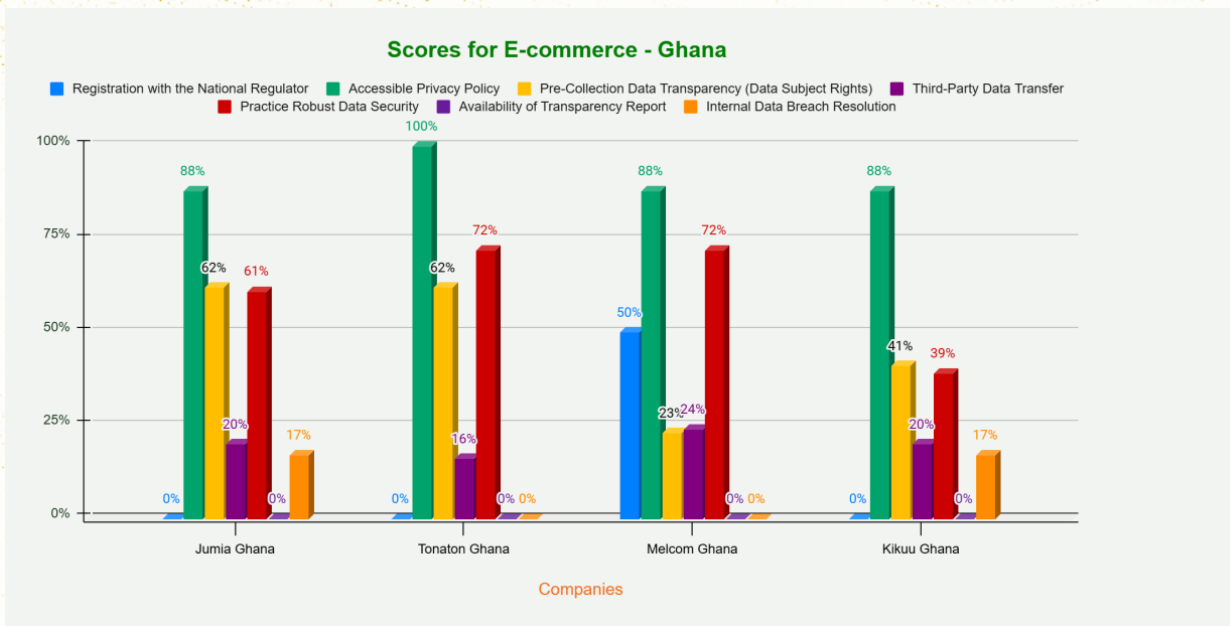
Jumia Nigeria faces significant compliance challenges due to a misalignment between its core business operations and privacy disclosures. Although it operates one of Nigeria's largest consumer e-commerce platforms, the most readily accessible privacy information focuses primarily on recruitment and job applicant data rather than consumer-facing marketplace activities. This disconnect limits customer understanding of how shopping, browsing, and transaction data are collected and used, creating transparency gaps and compliance risks under the NDPR.

Kara Nigeria records the lowest performance, largely due to technical and accessibility barriers that restrict user access to privacy information. Website functionality issues and access limitations prevented comprehensive evaluation of its privacy practices, undermining transparency and raising concerns under NDPA requirements that privacy information be easily accessible.

Overall, Jiji Nigeria sets a strong benchmark for privacy governance and compliance within Nigeria's e-commerce sector. Other platforms show partial progress, particularly in publishing privacy policies and implementing baseline security measures, but exhibit significant compliance gaps in regulatory registration, third-party data governance, and breach accountability. These weaknesses expose companies to legal and reputational risks while limiting users' ability to exercise their rights and protect their personal data, underscoring the need for stronger enforcement and improved corporate privacy governance across the sector.

b. Jumia Ghana, Tonaton Ghana, Melcom Ghana and Kikuu Ghana in Ghana

The assessment of Ghana's e-commerce sector reveals consistently weak compliance with national data protection obligations, despite the widespread publication of privacy policies. While all platforms demonstrate a baseline awareness of transparency requirements, substantive compliance with Ghana's Data Protection Act remains limited, particularly in regulatory registration, third-party data governance, and accountability mechanisms.



None of the four e-commerce platforms assessed currently maintains active registration with Ghana's Data Protection Commission. Jumia Ghana, Tonaton Ghana, and Kikuu Ghana are unregistered, while Melcom Ghana, although previously registered, allowed its certification to expire in September 2021 and has not renewed it. This widespread non-registration reflects weak regulatory engagement and places all platforms in breach of statutory registration obligations, undermining lawful data processing and regulatory oversight.

All assessed companies have publicly accessible privacy policies, indicating a foundational level of transparency. Tonaton Ghana performed strongest in this category, scoring 100% due to clearer structure and language, while Jumia Ghana, Melcom Ghana, and Kikuu Ghana each scored 88%. Readability scores (Hemingway grades 8–11) suggest moderate accessibility, and word counts ranged from 616 to over 2,200 words. While publication and visibility are strong across the sector, variations in clarity and completeness affect the practical usefulness of these policies for users.

Performance on data subject rights was mixed. Jumia Ghana and Tonaton Ghana led with scores of 62%, reflecting clearer explanations of data collection purposes, broader categories of data processed, and the inclusion of user rights such as access, correction, deletion, and complaint mechanisms. However, both fall short on specifying data retention periods and providing unconditional user control.

In contrast, Melcom Ghana scored 23%, offering vague disclosures that focus primarily on cookies, omit clear user rights and complaint channels, and provide limited transparency on data sharing. Kikuu Ghana performed slightly better at 41%, but still lacked clarity on collection purposes, offered conditional user rights, and provided only partial contact details. These disparities indicate uneven implementation of statutory obligations to uphold data subject rights, with significant gaps in user empowerment and legal compliance.

All platforms share personal data with third parties, yet compliance in this area remains consistently weak. Melcom Ghana scored highest at 24%, followed by Jumia Ghana and Kikuu Ghana (20%), and Tonaton Ghana (16%). Jumia and Tonaton permit data sharing for transactions, advertising, analytics, and law enforcement requests but fail to identify specific entities or the types of data shared. Tonaton explicitly references partners such as Facebook and Google but still lacks detailed disclosures. Melcom limits identifiable data sharing to trusted service providers under confidentiality obligations, while Kikuu allows sharing for order fulfilment and marketing support without naming recipients. Across the sector, the absence of specificity and reporting mechanisms increases the risk of unlawful processing and weakens accountability under the DPA.

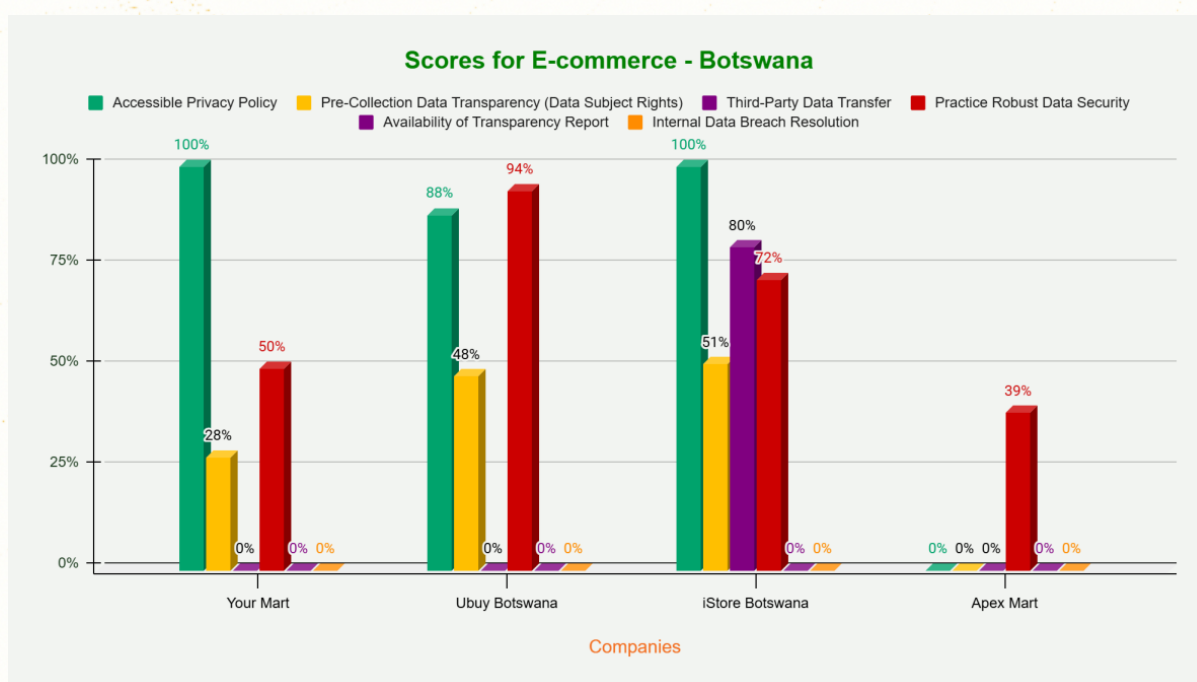
All companies demonstrate some level of technical security, particularly through SSL implementation, but overall practices remain inconsistent. Tonaton Ghana and Melcom Ghana performed best at 72%, followed by Jumia Ghana (61%) and Kikuu Ghana (39%). Strong SSL ratings are undermined by weak or failing security headers and vague policy disclosures regarding implementation. This inconsistency suggests partial compliance with data security obligations, leaving users exposed to avoidable risks.

None of the companies has published a transparency report since 2024, resulting in a 0% score across the sector. The absence of disclosures on government requests, third-party access, or content moderation significantly limits public oversight and undermines accountability.

Internal breach management remains a critical weakness. Jumia Ghana and Kikuu Ghana scored 17%, as both mention user notification only in broad terms without outlining investigation procedures, timelines, or reporting channels. Tonaton Ghana and Melcom Ghana provide no information on breach detection, notification, or resolution, scoring 0%. These gaps indicate non-compliance with accountability and risk-management requirements under the DPA.

Overall, the findings indicate that Ghanaian e-commerce platforms have made surface-level efforts toward transparency, primarily through publishing privacy policies, but fall short on substantive compliance with national data protection laws. Persistent deficiencies in regulatory registration, third-party data governance, breach accountability, and the full implementation of data subject rights expose users to privacy risks and leave companies vulnerable to legal sanctions and reputational harm. Without stronger enforcement and improved internal governance, user trust in Ghana's e-commerce sector remains fragile.

c. *Your Mart, Ubuy Botswana, iStore Botswana and Apex Mart in Botswana*



The assessment of Botswana's e-commerce sector reveals uneven privacy and data protection practices across the four companies evaluated, reflecting varying levels of compliance with national data protection obligations.

Only three companies (Your Mart, iStore Botswana, and Ubuy Botswana) had accessible privacy policies in place. Your Mart and iStore Botswana led in this category with perfect scores (100%), while Ubuy Botswana scored 88%. These same companies were also the only ones to demonstrate efforts to support data subject rights, though overall performance remained modest. iStore Botswana performed best at 51%, followed by Ubuy Botswana (48%) and Your Mart (28%), indicating partial but incomplete alignment with legal requirements to enable users to access, control, or challenge the use of their personal data.

All four companies share personal data with third parties, but compliance in this area varied significantly. iStore Botswana led with a relatively strong score of 80%, reflecting clearer restrictions on third-party data transfers, while the remaining companies recorded very low or no compliance (0%), highlighting substantial transparency and accountability gaps. These weaknesses increase the risk of unlawful data disclosures and undermine users' ability to understand how their data is used.

All companies demonstrated visible efforts to secure personal data, though performance again varied. Ubuy Botswana led with a high score of 94%, followed by iStore Botswana (72%), Your Mart (50%), and Apex Mart (39%). While these scores suggest some commitment to safeguarding user data, uneven implementation of security measures leaves certain platforms more exposed to data breaches.

None of the companies published transparency reports or had internal data breach resolution mechanisms in place. The absence of procedures for breach detection, investigation, notification, and remediation represents a critical sector-wide weakness, significantly undermining compliance with accountability and risk management obligations under data protection law.

At the company level, Your Mart demonstrated a strong commitment to transparency through a privacy policy that was clearly visible, easy to read, and detailed. The policy explained the purposes of data collection and outlined categories of personal data processed. However, it permitted data sharing with advertisers without identifying the specific third parties or the types of data shared. Additionally, the policy did not address internal data breach handling, investigation timelines, or user notification. Despite its length (over 1,200 words) and level of detail, these omissions limit its effectiveness in ensuring accountability.

Ubuy Botswana performed strongest on data security, outlining specific measures such as malware scanning, SSL encryption, and restricted staff access to personal data. Its policy also described data categories and retention practices, though retention was framed vaguely as “as long as required by law.” While Ubuy acknowledged third-party data sharing, particularly with payment and shipping providers, it failed to provide a comprehensive list of recipients. The lack of internal breach resolution mechanisms and user complaint channels further weakens its compliance posture.

iStore Botswana stood out as the only company to explicitly restrict third-party data sharing, stating that personal data would not be shared without user consent or a court order. This reflects stronger safeguards against unauthorized disclosure. However, its security provisions were broadly framed and lacked technical detail, and the policy did not include any mechanisms for managing or reporting data breaches, limiting its operational accountability.

Apex Mart ranked lowest across all indicators due to the complete absence of a privacy policy. Without any publicly available information on data collection, processing, or sharing practices, Apex Mart fails to meet even minimum transparency standards, placing users at significant risk and indicating serious non-compliance with data protection principles.

Overall, iStore Botswana emerged strongest on limiting third-party data transfers, Ubuy Botswana led in data security practices, and Your Mart excelled in policy accessibility and clarity but fell short on accountability. Apex Mart failed to meet baseline privacy requirements. Across the sector, the lack of transparency reporting and internal breach resolution mechanisms represents a critical compliance gap, exposing users to heightened privacy risks and highlighting the need for stronger enforcement and corporate accountability within Botswana’s e-commerce ecosystem.

d. *Murukali, Vuba vuba, kikuu Rwanda and Ubuy Rwanda in Rwanda*



The assessment of Rwanda’s e-commerce platforms (Murukali, Vuba Vuba, Kikuu Rwanda, and Ubuy Rwanda) shows a pattern of formal transparency without substantive accountability, largely consistent with last year’s findings, though with some incremental improvements and notable regressions.

As in the previous assessment, all companies maintained publicly accessible privacy policies, demonstrating baseline compliance with transparency obligations. Vuba Vuba again led with a perfect score (100%), supported by strong readability (Hemingway grade 9) and concise drafting (478 words). Murukali, Kikuu Rwanda, and Ubuy Rwanda each scored 88%, mirroring last year's performance, though their policies were longer (918–1,761 words) and less user-friendly. While continued availability of privacy policies reflects sustained awareness of legal requirements, accessibility alone has not translated into meaningful user protection.

Performance on data subject rights remains weak across the sector and, in some cases, has deteriorated since last year. All companies scored below 50%, indicating persistent non-compliance with statutory obligations to enable user control over personal data.

- Ubuy Rwanda led with 45%, a modest improvement from 41%, reflecting clearer articulation of data categories and purposes, but still lacking specific retention timelines, full third-party disclosure, and clear complaint mechanisms.
- Murukali declined sharply to 39% from 53%, primarily due to restrictions on rights to European residents, missing contact details, and vague treatment of complaints and law enforcement access.
- Kikuu Rwanda improved to 35% from 18%, suggesting incremental progress, though key gaps remain around retention, complaints, and third-party clarity.
- Vuba Vuba recorded a dramatic drop to 3% from 19%, offering almost no meaningful information on user rights, retention, or complaint avenues.

Overall, these results indicate that, despite having privacy policies, most platforms do not effectively operationalize user rights, undermining compliance with Rwanda's data protection framework.

As in last year's analysis, third-party data transfer remains a critical weakness. All companies share personal data with third parties, yet compliance levels remain extremely low.

- Murukali led marginally with 20% (up from 10%), allowing sharing with advertisers and analytics services such as Shopify and Google Analytics, but without specifying data types or providing breach-reporting channels.
- Kikuu Rwanda improved slightly to 10% (from 0%), though disclosures remain vague.
- Vuba Vuba and Ubuy Rwanda again scored 0%, providing little to no information on third-party recipients, purposes, or safeguards.

The persistence of these gaps suggests systemic non-compliance with transparency and accountability obligations governing data sharing and significantly heightens the risk of unlawful processing.

All companies demonstrated some effort to secure personal data, with mixed results compared to last year.

- Ubuy Rwanda strengthened its lead, scoring 94% (up from 89%), supported by strong SSL (A+), robust security headers (A), and detailed policy disclosures on encryption, access controls, malware scanning, and secure transactions.
- Murukali maintained its 56% score, with strong SSL and headers but no policy-level discussion of personal data security.
- Kikuu Rwanda remained unchanged at 39%, combining weak technical indicators with vague policy statements.
- Vuba Vuba declined significantly to 28% from 50%, due to failing security headers and the continued absence of security disclosures in its policy.

These findings show that while technical safeguards are improving for some platforms, policy transparency and consistency remain insufficient to ensure full compliance.

Consistent with last year, none of the companies published transparency reports. The continued absence of disclosures on government requests, third-party access, or enforcement actions reflects a sector-wide accountability gap and limits public oversight.

Internal breach management remains severely underdeveloped, with only marginal progress.

- Kikuu Rwanda improved to 17% (from 0%), referencing breach notification when legally required but lacking detail on procedures, timelines, or reporting channels.
- Murukali, Vuba Vuba, and Ubuy Rwanda all scored 0%, offering no guidance on breach detection, investigation, user notification, or redress.

This persistent weakness represents a clear failure to meet core accountability and risk-management obligations under data protection law.

Compared with last year, the Rwandan e-commerce sector shows incremental improvement in isolated areas, notably Kikuu's gains in user rights and Ubuy's strengthened security, but no structural shift toward full compliance. Some platforms, particularly Murukali and Vuba Vuba, have regressed on key indicators.

Overall, formal compliance (privacy policies and SSL adoption) continues to mask substantive deficiencies in user rights enforcement, third-party data governance, breach accountability, and transparency reporting. These gaps expose users to privacy risks, undermine trust, and leave companies vulnerable to regulatory sanctions. Without stronger enforcement and more deliberate investment in privacy governance, Rwanda's e-commerce sector risks entrenching a model of compliance that is largely procedural rather than rights-protective.

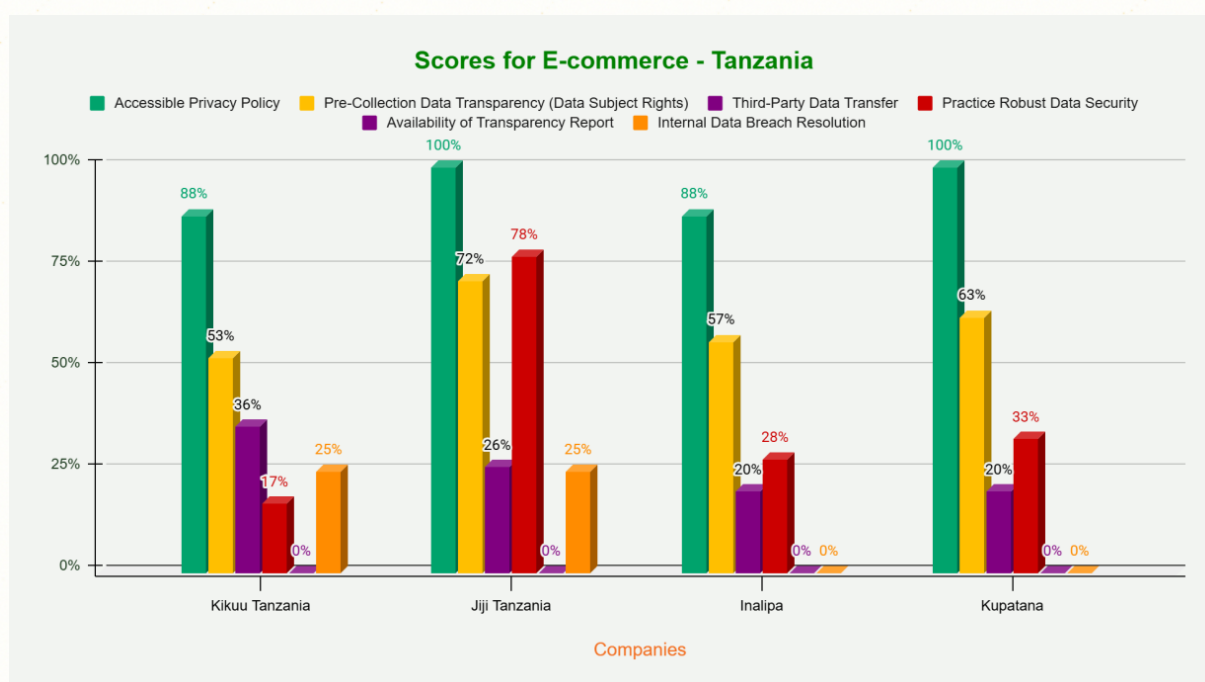
e. Kikuu Tanzania, Jiji Tanzania, Inalipa and Kupatana in Tanzania

The assessment of e-commerce platforms in Tanzania, Jiji Tanzania, Kupatana, Kikuu Tanzania, and Inalipa shows consistent performance in formal transparency measures, alongside persistent weaknesses in accountability, third-party data governance, and breach management. Overall, the findings suggest incremental improvement in user-facing disclosures but limited substantive compliance with national data protection obligations.

All assessed companies made efforts to maintain accessible and publicly available privacy policies, reflecting baseline compliance with transparency requirements. Jiji Tanzania and Kupatana again led the sector with perfect scores (100%), maintaining their positions from last year. Kikuu Tanzania and Inalipa also sustained strong performance, each scoring 88%, consistent with the previous assessment.

Jiji Tanzania's policy is prominently displayed on its website, highly readable (Hemingway grade 8), and comprehensive, with a word count of 4,080 words. Similarly, Kupatana's policy is clearly noticeable, well-structured, and accessible, with an impressive readability grade of 9 and a word count of 3,086 words. These characteristics enhance user awareness and understanding of data practices, an essential component of transparency under data protection law.

All companies demonstrated improved efforts to enable data subject rights, marking one of the more positive trends in this year's assessment.



Jiji Tanzania led with 72%, a significant improvement from 56% last year, followed by Kupatana (63%), which remained relatively stable, Inalipa (57%), up from 23%, and Kikuu Tanzania (53%), up from 47%.

Despite these gains, gaps remain. Jiji Tanzania and Kupatana, while leading, do not fully disclose company contact details, limiting users' ability to exercise rights or lodge complaints. Jiji Tanzania lists only a physical address, while Kupatana omits a full physical address and does not provide an email or phone contact. These omissions weaken practical compliance with user-rights provisions under Tanzania's data protection framework.

All companies reported sharing personal data with third parties, but compliance in this area remains consistently low, with no platform scoring above 36%. Kikuu Tanzania led with 36% (up from 22%), followed by Jiji Tanzania (26%), Inalipa (20%), and Kupatana (20%), the latter two showing only marginal changes from last year.

The low scores reflect insufficient transparency and justification for third-party data sharing, including the absence of clear consent mechanisms, limited disclosure of recipient entities, and lack of legal bases for transfers. These practices pose risks to data subject rights and raise concerns about compliance with Tanzanian data protection laws governing lawful processing and disclosure.

All companies exhibited some effort to implement technical data security measures. Jiji Tanzania performed best in this category, scoring 78%, supported by an A+ SSL rating from Qualys SSL Labs. However, despite strong technical indicators, Jiji's privacy policy lacks detailed explanations of security safeguards, limiting transparency.

The remaining companies demonstrated moderate to weak performance, indicating that while basic security controls may exist, they are not consistently documented or communicated to users. This gap undermines accountability and weakens user confidence in how personal data is protected.

None of the assessed companies has published a transparency report since 2024. The absence of such reports means users have no insight into government requests, third-party data access, or internal compliance practices. This lack of reporting significantly limits public accountability and falls short of best practices for transparency under data protection regimes.

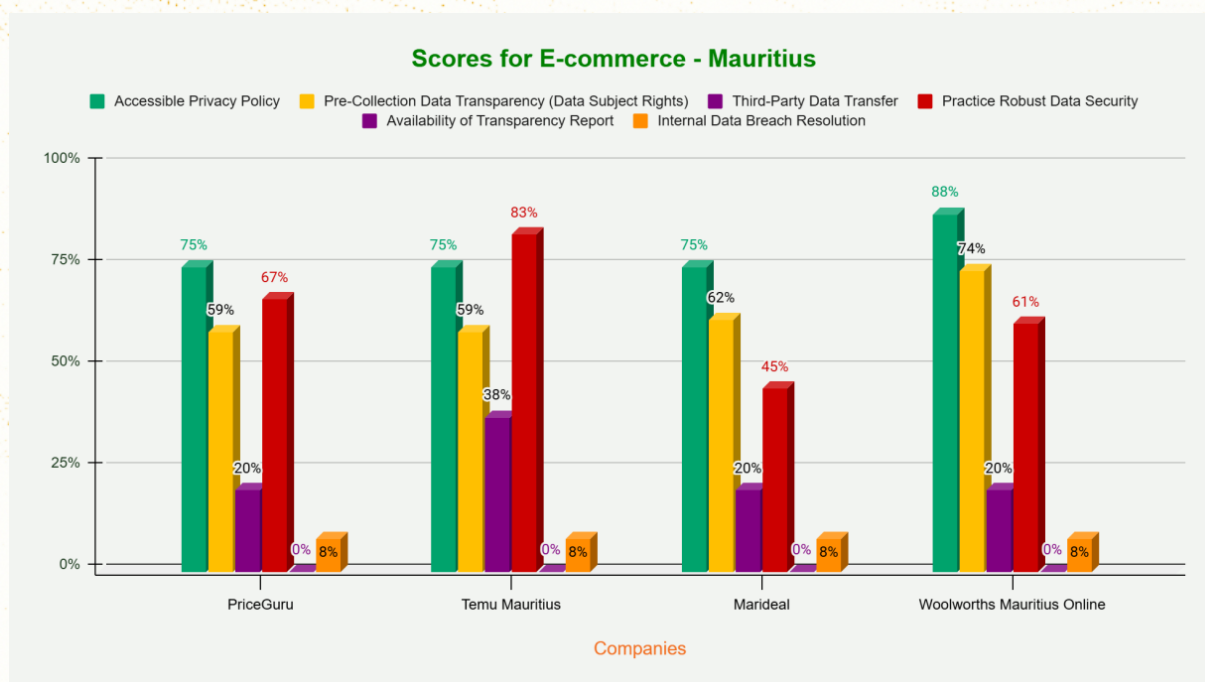
All companies recorded very poor performance in internal data breach resolution mechanisms. Jiji Tanzania and Kikuu Tanzania led marginally with scores of 25%, while Kupatana and Inalipa scored 0%. The limited disclosures provided do not specify internal procedures, reporting timelines, investigation processes, or user notification mechanisms. This represents a critical compliance gap, as effective breach management is central to accountability and risk mitigation under data protection law.

Overall, Tanzania's e-commerce sector demonstrates strong performance in policy accessibility and improving recognition of data subject rights, but continues to struggle with substantive compliance in third-party data governance, breach accountability, and transparency reporting. While incremental improvements are evident compared to last year, particularly in user-rights provisions persistent weaknesses expose users to privacy risks and leave companies vulnerable to regulatory scrutiny and reputational harm. Without clearer disclosures, stronger accountability mechanisms, and robust enforcement, compliance with Tanzania's data protection framework remains largely procedural rather than rights-protective.

f. PriceGuru, Temu Mauritius, Marideal and Woolworths Mauritius Online in Mauritius

All companies assessed have made commendable efforts to ensure the availability of accessible privacy policies. Woolworths Mauritius Online continues to lead, as in the previous year, with a score of 88%, while PriceGuru, Temu Mauritius, and Marideal each achieved 75%. Compared to last year, PriceGuru and Marideal maintained their scores, whereas Temu Mauritius experienced a slight decline from 88%. These results suggest a baseline level of transparency across all platforms, though only Woolworths demonstrates consistently high standards in policy accessibility and clarity.

In terms of respecting data subject rights, all companies showed measurable progress. Woolworths again performed best, scoring 74%, a significant increase from 57% last year. Marideal followed with 62%, up from 53%. PriceGuru and Temu Mauritius each scored 59%, reflecting a marginal decline for PriceGuru (from 60%) and a notable improvement for Temu (from 47%). This upward trend indicates growing awareness of user rights obligations, although inconsistencies remain in how these rights are operationalised and communicated.



By contrast, compliance relating to third-party data sharing remains weak across all companies. Although all platforms disclosed that they share personal data with third parties, compliance levels were low. Temu Mauritius led with 38%, improving from 16% last year, while PriceGuru, Marideal, and Woolworths each scored only 20%. While these scores represent an improvement for PriceGuru and Marideal (from 10%), Woolworths saw a sharp decline from 70%. This highlights a significant compliance gap, particularly in relation to transparency, safeguards, and user control over onward data transfers, key requirements under modern data protection frameworks.

All companies demonstrated visible efforts to strengthen data security measures. Temu Mauritius led with 83%, up from 78%, followed by PriceGuru at 67% (up from 56%), Woolworths at 61% (up from 45%), and Marideal, which maintained its previous score of 45%. These improvements reflect increased attention to technical and organisational safeguards, although disparities suggest uneven maturity in data protection practices.

As in the previous year, all companies scored poorly on transparency reporting and internal data breach resolution mechanisms, each achieving only 8%.

While this represents an improvement from 0% for PriceGuru, Temu Mauritius, and Marideal, Woolworths declined from 17%. The absence of meaningful transparency reports and clearly articulated breach response procedures raises concerns regarding accountability and preparedness, particularly given the growing regulatory emphasis on breach notification and incident management.

Under the policy indicator, PriceGuru, Temu Mauritius, and Marideal each scored 75% for accessible privacy policies, while Woolworths Mauritius Online again led with 88%. Woolworths also achieved the highest score under the pre-collection data transparency indicator, reflecting clearer communication at the point where personal data is first collected.

The privacy policies of PriceGuru and Temu clearly outline the categories of personal data collected and the purposes for which they are used, primarily to support and improve service delivery. Temu's policy is broader in scope, covering data collected directly from users (such as account details, purchases, customer support interactions, reviews, and event participation), data obtained from third parties (including social media platforms, payment processors, and marketing partners), and information collected automatically through device data, usage patterns, location data, and cookies. PriceGuru adopts a similar approach, focusing on data collected during account creation, purchases, surveys, correspondence, and through cookies or server logs.

A key distinction lies in the treatment of user rights. PriceGuru explicitly sets out mechanisms for accessing, correcting, erasing, or restricting personal data and explains how users can submit such requests. Temu, while providing detailed explanations of data categories and purposes, does not articulate procedures for exercising user rights with the same level of clarity, potentially limiting the practical enforceability of those rights.

Both policies permit sharing of personal data with third parties. PriceGuru restricts disclosure to service providers, advisors, government authorities, corporate transactions, and third parties where explicit consent has been obtained. Temu

allows a broader range of disclosures, including to affiliates, advertising and analytics partners, business partners, merchandise partners, regulators, and even other users. While both policies emphasise safeguards and necessity, Temu places greater emphasis on user control in peer-to-peer data sharing contexts, whereas PriceGuru explicitly disclaims responsibility for external websites, underscoring the fragmented nature of privacy protections once data leaves its platform.

Marideal's privacy policy closely mirrors those of PriceGuru and Temu. It covers standard categories of personal data collected during account creation, purchases, and website use, and permits account creation through third-party platforms such as Google or Facebook, involving the transfer of profile data. Its storage and security provisions follow the same general framework, referencing encryption and technical safeguards while disclaiming absolute security, a cautious stance consistent with the other platforms.

Marideal's permitted uses of data align with common e-commerce practices, including account management, order fulfilment, customer communication, and service improvement. Like PriceGuru, it prohibits the sale or rental of personal data and, like Temu, permits marketing communications subject to user consent. It also provides for disclosure in compliance with legal obligations and, notably, in the context of corporate restructuring, a provision shared with Temu but absent from PriceGuru's policy.

Where Marideal stands out is in its recognition of user rights. In addition to access, correction, and erasure, it explicitly grants users the right to delete their accounts entirely, aligning more closely with GDPR principles of user control and data minimisation. It also provides users with options to manage cookie preferences.

Woolworths' privacy policy is more formal and compliance-oriented in tone. It explicitly references the Mauritius Data Protection Act 2017 and frames data processing within a legal and accountability-driven context. The policy clearly sets out what data is collected, how it is used in everyday transactions, and the safeguards applied when data is shared, including cross-border transfers.

Unlike Temu and Marideal, Woolworths integrates its privacy notice into its terms and conditions, making it part of the contractual relationship with users. It recognises a broader range of user rights, including the right to object to processing, opt out of direct marketing, and request deletion, subject to legal requirements. While it shares common ground with the other platforms in terms of data categories collected and the use of cookies and analytics, it distinguishes itself by explicitly acknowledging technological risks and committing to inform users in the event of a data breach.

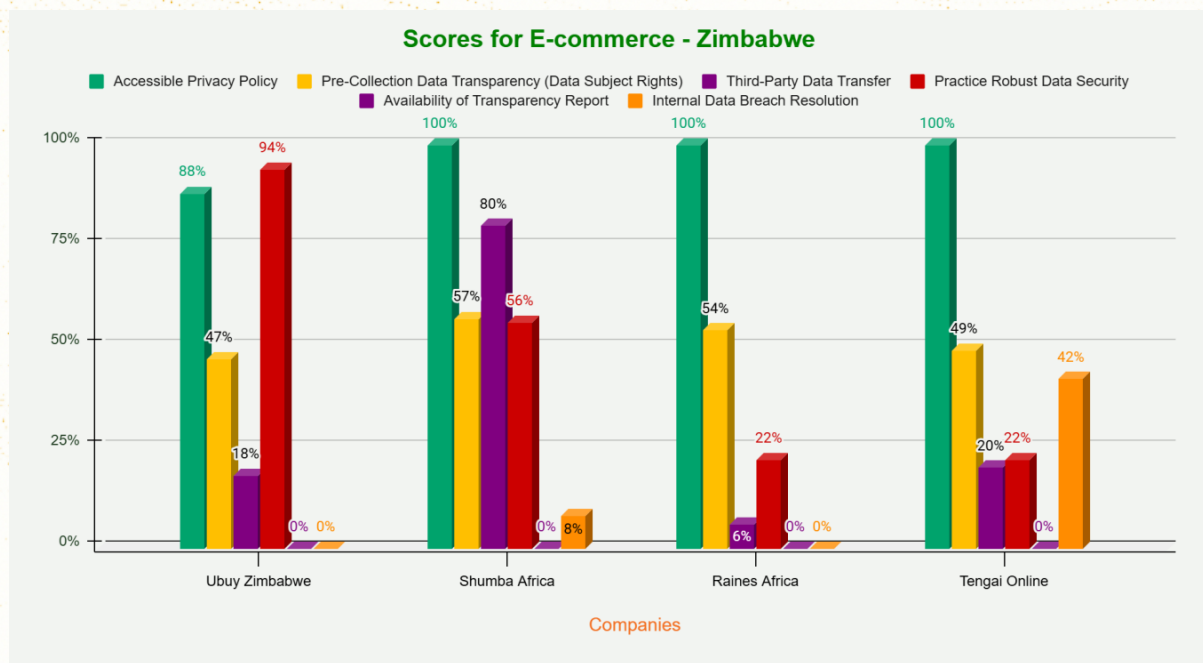
Overall, PriceGuru, Temu, and Marideal adopt broadly similar, disclosure-focused approaches to personal data processing, with variations in the scope of user rights and third-party sharing practices. Woolworths stands apart for its stronger emphasis on legal compliance, accountability, and user protections.

The findings suggest that while baseline transparency and security measures are improving across the sector, significant gaps remain in third-party data sharing compliance, breach response mechanisms, and transparency reporting. These weaknesses pose potential risks under data protection laws such as the Mauritius Data Protection Act 2017 and GDPR-aligned standards, particularly regarding accountability, lawful processing, and user empowerment.

To strengthen compliance, companies should move beyond policy disclosure toward demonstrable practices, including clearer procedures for exercising data subject rights, stricter controls and transparency around third-party data sharing, and robust, well-documented breach response and reporting mechanisms. Without these improvements, companies risk not only regulatory exposure but also erosion of user trust in an increasingly privacy-conscious digital marketplace.

g. Ubuy Zimbabwe, Shumba Africa, Raines Africa and Tengai Online in Zimbabwe

All companies assessed made efforts to ensure the availability of accessible privacy policies. Shumba Africa, Raines Africa, and Tengai Online led the group with perfect scores of 100%, indicating that their privacy policies are clearly visible, easy to locate, and highly readable. Ubuy Zimbabwe followed closely with a score of 88%, reflecting a policy that is fairly readable, with a Grade 11 readability score and a word count of 1,761 as measured by the Hemingway Editor.



Compared to last year, Shumba Africa, Tengai Online, and Ubuy Zimbabwe maintained their performance, while Raines Africa showed notable improvement, increasing from 63% to 100%. These results demonstrate growing recognition of transparency as a foundational requirement of data protection compliance.

All companies also demonstrated efforts to recognise and facilitate data subject rights, although performance levels varied. Shumba Africa led with a score of 57%, a significant improvement from 36% in the previous year. Raines Africa followed with 54%, up from 29%, while Tengai Online improved to 49% from 24%. Ubuy Zimbabwe, however, recorded a decline, scoring 47% compared to 54% last year. While the upward trend for most companies suggests increasing awareness of obligations such as access, correction, and erasure, the moderate scores indicate that mechanisms for exercising these rights are still insufficiently detailed or inconsistently implemented.

Third-party data sharing remains one of the weakest areas of compliance. With the exception of Shumba Africa, which achieved a comparatively strong score of 80% (up from 24%), all companies recorded very low levels of compliance. Ubuy Zimbabwe scored only 18%, a slight improvement from 12%, while Raines Africa improved marginally to 6% from 0%. Tengai Online declined to 20% from 24%. These results indicate that while data sharing with third parties is common, transparency around such practices, the legal basis for sharing, and the safeguards applied remains inadequate. This presents heightened compliance risks under data protection laws, which require clear disclosure, purpose limitation, and accountability in third-party processing arrangements.

In relation to data security, all companies showed some level of commitment to protecting personal data. Ubuy Zimbabwe again led with a high score of 94%, reflecting the implementation of robust and proactive security measures designed to prevent unauthorised access, misuse, loss, or breaches. Shumba Africa maintained its previous score of 56%. By contrast, Raines Africa and Tengai Online both declined significantly, scoring 22%, down from 45% and 39% respectively. These declines suggest potential gaps in the consistency or updating of technical and organisational security measures, which are critical for compliance with data protection legislation.

As in the previous year, transparency reporting remains largely absent across the sector. Tengai Online and Raines Africa performed best in this category, yet still achieved only 42%, albeit an improvement from 25%. Shumba Africa scored 8%, up from 0%, while the remaining companies maintained scores of 0%. The absence of publicly available transparency reports means that data subjects have limited visibility into how their personal data is processed, shared, protected, or breached. This undermines the principles of accountability and openness that underpin modern data protection frameworks.

Under the pre-collection data transparency indicator, Shumba Africa again performed best with a score of 57%, followed by Ubuy Zimbabwe at 47%. Despite this comparatively strong performance, Shumba Africa's policy contains notable gaps: it provides only an email address as a point of contact and does not include a physical address or telephone number. More critically, it makes no reference to the right of individuals to lodge complaints with the company itself or with a regulatory authority. Such omissions weaken compliance with data protection laws, which typically require clear identification of the data controller and accessible avenues for redress.

In the area of third-party data privacy, Shumba Africa again led with 80%, but fell short of a perfect score due to the absence of clearly defined channels for reporting data breaches. Ubuy Zimbabwe, while scoring poorly on third-party transparency, demonstrated the strongest performance in terms of robust data security practices, highlighting a disconnect between technical safeguards and broader accountability and transparency obligations.

Overall, the findings indicate that companies in this sector are increasingly attentive to the visibility and readability of privacy policies, as well as to baseline security requirements. However, significant compliance gaps persist, particularly in relation to third-party data sharing, transparency reporting, and internal data breach resolution mechanisms. The lack of published transparency reports and weak breach response frameworks mean that data subjects remain largely unaware of how their data is processed in practice and what remedies are available in the event of misuse or breaches.

From a legal perspective, these shortcomings expose companies to potential non-compliance with data protection laws, including obligations relating to accountability, lawful processing, data subject rights, and breach management under the Zimbabwe Cyber and Data Protection Act and GDPR-aligned principles. To strengthen compliance and build user trust, companies should move beyond formal policy publication and focus on implementing clear, accessible rights-request mechanisms, transparent third-party data governance frameworks, and well-documented breach response and reporting procedures.

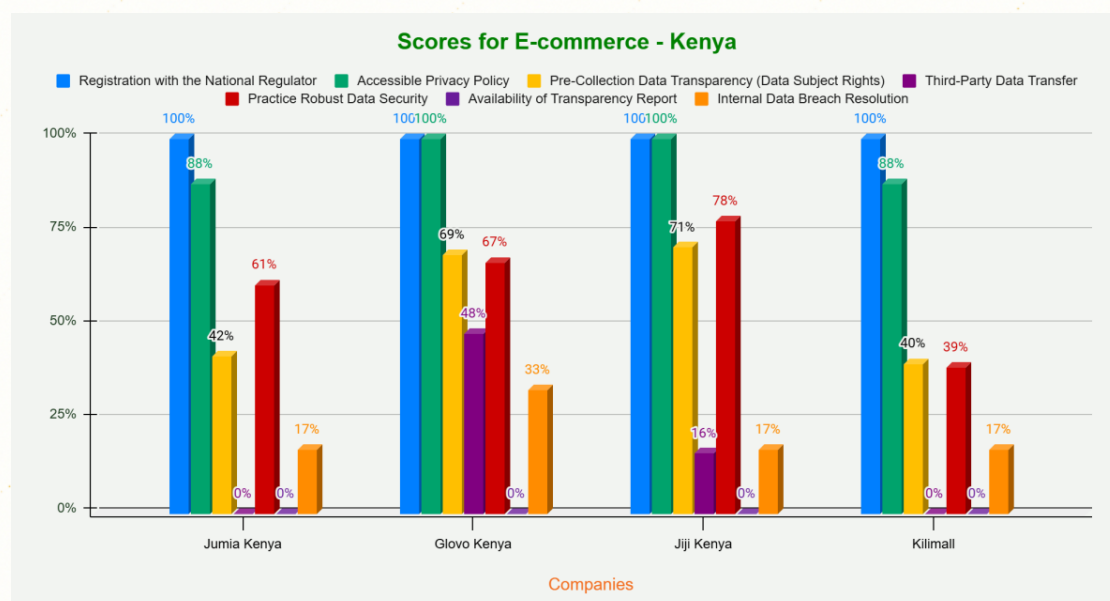
Without such measures, improvements in policy accessibility and security alone will be insufficient to demonstrate full compliance or to meet the evolving expectations of regulators and data subjects in an increasingly privacy-conscious digital environment.

h. Jumia Kenya, Glovo Kenya, Jiji Kenya and Kilimall in Kenya

As in the previous year, all companies assessed maintained full compliance with registration requirements, each achieving a perfect score of 100% for registration with the national data protection regulator. This demonstrates a shared baseline awareness of statutory obligations under Kenya's data protection framework. However, registration alone does not equate to substantive compliance, and further indicators reveal varying levels of maturity in privacy practices.

All companies also made efforts to maintain accessible privacy policies. Glovo Kenya and Jiji Kenya again led with perfect scores of 100%, reflecting policies that are clearly visible, well-structured, and easy for users to understand. Jumia Kenya and Kilimall each scored 88%. Compared to last year, Jumia maintained its score, while Kilimall showed improvement from 75%. These results suggest progress in formal transparency, particularly among platforms that had previously lagged behind.

Performance in relation to data subject rights was mixed. Jiji Kenya led with a score of 71%, improving from 66%, followed closely by Glovo Kenya at 69%. While this represents a decline from Glovo's previous score of 83%, it still reflects relatively strong mechanisms for facilitating rights such as access, correction, and erasure. Jumia Kenya recorded a notable decline to 42% from 53%, while Kilimall showed only marginal improvement, scoring 40% compared to 39% last year. These results indicate that, despite the existence of privacy policies, practical mechanisms for exercising data subject rights remain inconsistently implemented, particularly among local platforms.



All companies were found to share personal data with third parties, yet compliance in this area remains critically low. Glovo Kenya performed best, but still scored only 48%, despite a significant improvement from 20% last year. Jiji Kenya followed with a low score of 16%, declining from 26%. Jumia Kenya and Kilimall both scored 0%, representing a sharp regression from last year's scores of 10% and 20%, respectively. These findings point to serious deficiencies in transparency around third-party data sharing, including inadequate disclosure of recipients, purposes, safeguards, and legal bases for such transfers, key requirements under data protection laws.

In contrast, all companies demonstrated some commitment to data security. Jiji Kenya led with a score of 78%, a notable increase from 56%, followed by Glovo Kenya, which maintained a strong score of 67%. Jumia Kenya also maintained its score of 61%, while Kilimall remained at 39%. Although these results suggest that technical and organisational security measures are receiving attention, the uneven performance highlights disparities in risk management and security governance across platforms.

As in the previous year, transparency reporting and internal data breach resolution mechanisms remain weak across the sector. Glovo Kenya again led in this category but achieved only 33%, up from 25%. Jumia Kenya, Jiji Kenya, and Kilimall each scored just 17%. Compared to last year, Jumia Kenya maintained its score, Jiji Kenya improved from 0%, while Kilimall declined significantly from 33%. The lack of published transparency reports and clearly articulated breach response procedures undermines accountability and may hinder timely notification and remediation in the event of data breaches, as required under Kenyan law.

International e-commerce platforms significantly outperform local competitors. Glovo Kenya achieved an overall compliance score of 96%, reflecting the influence of comprehensive privacy frameworks developed for European and global markets. Its privacy policy includes detailed data retention schedules ranging from three to fifteen years depending on data categories, explicit consent mechanisms for behavioural marketing, and extensive third-party sharing disclosures covering advertising partners, payment processors, and delivery service providers. This level of detail demonstrates how compliance with international regulatory regimes can elevate privacy protection standards and deliver tangible benefits to Kenyan consumers.

Jiji Kenya's strong performance, with an overall score of 92% among domestic platforms, reflects sustained investment in privacy compliance following its expansion across multiple African markets. Its policy addresses complex issues such as cross-border data transfers, automated decision-making, and a relatively comprehensive implementation of data subject rights. However, gaps remain, particularly in relation to clearly articulated complaint procedures involving the Office of the Data Protection Commissioner and transparency around law enforcement access to personal data.

Jumia Kenya's moderate overall score of 58% highlights inconsistencies in privacy protection within established e-commerce platforms. While the company provides a basic privacy policy, significant gaps persist regarding specificity of data retention periods, comprehensive disclosure of third-party data sharing, and clear procedures for exercising data subject rights. The presence of multiple third-party trackers on Jumia's website further raises concerns about transparency in advertising partnerships and the adequacy of user consent management.

Kilimall's extremely poor overall score of 4% represents a critical compliance failure requiring urgent corrective action. The platform's privacy policy is largely inaccessible, preventing meaningful evaluation of its data protection practices and falling short of fundamental transparency requirements. This situation is particularly concerning given Kilimall's processing of sensitive financial and personal data belonging to thousands of Kenyan users, exposing both the company and data subjects to significant legal and privacy risks.

Overall, the findings reveal a clear divide between international and local e-commerce platforms in terms of privacy governance and regulatory compliance. While registration and basic policy accessibility are largely in place, substantive compliance, particularly in third-party data sharing, transparency reporting, and breach management remains uneven and, in some cases, critically deficient.

From a regulatory perspective, these shortcomings expose companies to potential enforcement action under the Kenya Data Protection Act, 2019, particularly with respect to accountability, lawful processing, user rights facilitation, and breach notification obligations. To strengthen compliance and consumer trust, companies must move beyond formal registration and policy publication toward demonstrable, operational privacy practices. This includes clearer disclosure of third-party relationships, robust consent and rights-request mechanisms, documented breach response procedures, and proactive transparency reporting.

Without such measures, improvements in security and policy visibility alone will be insufficient to meet legal requirements or to address growing consumer expectations around privacy and data protection in Kenya's digital economy.

i. Jumia Uganda, Glovo Uganda, Jiji Uganda and Kikuu Uganda

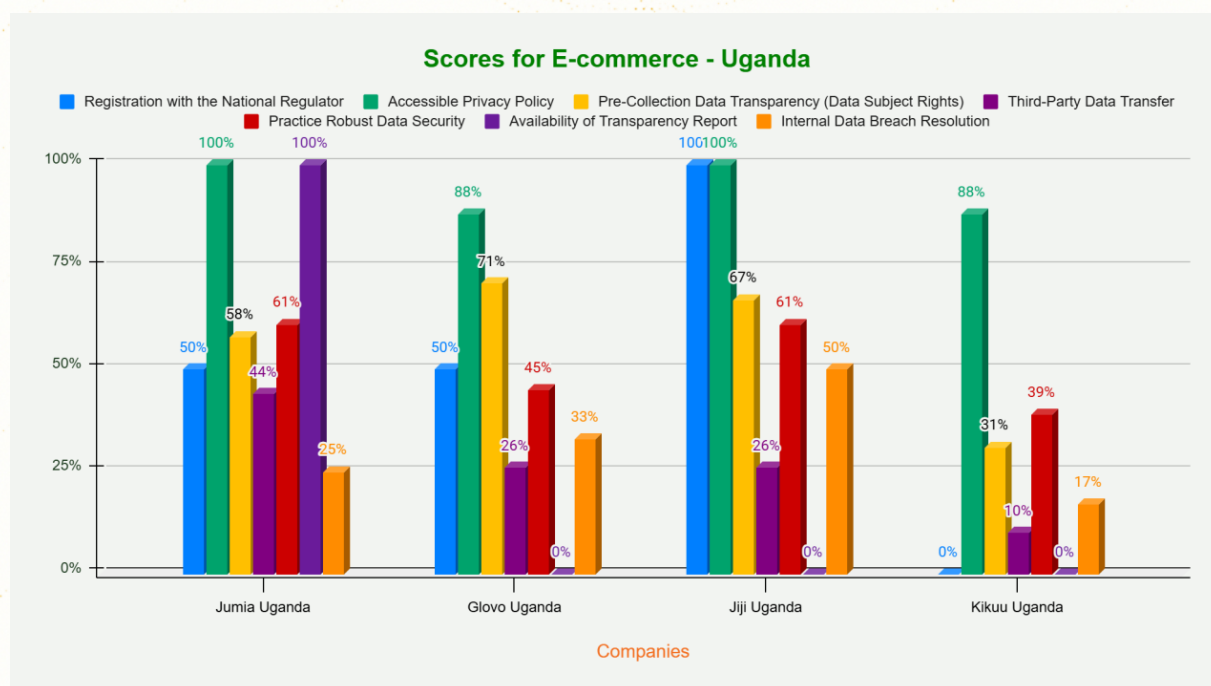
Only three of the assessed companies demonstrated efforts to comply with registration requirements with the national data protection regulator. As in the previous year, Jiji Uganda remained the clear leader, maintaining a perfect compliance score of 100%. Jumia Uganda and Glovo Uganda each scored 50%, reflecting notable improvements from last year, when Jumia scored 0% and Glovo scored 32%. Despite this progress, the limited number of registered entities indicates that regulatory registration continues to be a weak point in the sector and remains largely unchanged from last year in terms of overall participation.

All companies made efforts to ensure accessible privacy policies. Jumia Uganda and Jiji Uganda again led with perfect scores of 100%, maintaining their strong performance from last year. Glovo Uganda and Kikuu Uganda each scored 88%. While Kikuu maintained its score, Glovo declined from 100% last year, suggesting a slight regression in the visibility or clarity of its policy. Nonetheless, the widespread availability of privacy policies indicates that transparency at a basic, formal level is now well established across the sector.

Efforts to observe data subject rights showed mixed results. Glovo Uganda led with a score of 71%, though this represents a decline from 77% last year.

Jiji Uganda improved to 67% from 60%, while Jumia Uganda increased to 58% from 53%. Kikuu Uganda, however, maintained a low score of 31%, unchanged from last year. These results suggest incremental progress among most platforms, but also indicate that the practical facilitation of rights such as access, correction, deletion, and objection remains uneven and, in some cases, stagnant.

All companies were found to share personal data with third parties, yet compliance in this area remains consistently low, echoing last year's findings. Jumia Uganda performed best, scoring 44%, a significant improvement from 0% last year. Glovo Uganda and Jiji Uganda each scored 26%, with Glovo declining from 32% and Jiji improving from 16%. Kikuu Uganda scored only 10%, up slightly from 0%.



As noted in last year's analysis, third-party data sharing remains a major concern, as companies continue to allow access to personal data by advertisers and other partners without adequately specifying what data is shared, for what purposes, or under what safeguards. This persistent weakness indicates that the concerns raised last year remain largely unresolved.

There were visible efforts to improve data security. Jumia Uganda and Jiji Uganda led with scores of 61%, with Jumia maintaining its previous performance and Jiji improving from 56%. While this suggests moderate levels of technical and organisational protection, it also confirms last year's conclusion that security practices are inconsistently articulated and, in some cases, insufficiently detailed to meet best practice standards.

Transparency reporting shows the most significant change from last year. With the exception of Jumia Uganda, all companies continued to lack transparency reports. Jumia Uganda scored 100%, up from 0%, making it the only platform in

the sector to publish a transparency report for the previous year. This represents a meaningful improvement in accountability and directly addresses a key gap identified in last year's analysis, which found that no platforms had published transparency reports since 2023.

All companies made some effort to establish internal data breach resolution mechanisms. Jiji Uganda led with 50%, improving substantially from 0% last year. Glovo Uganda maintained a score of 33%, Jumia Uganda improved to 25% from 17%, and Kikuu Uganda maintained a low score of 17%. While these results show incremental progress, the overall low scores indicate that breach response frameworks remain underdeveloped across the sector.

Within the e-commerce sector, Jumia Uganda stands out for its highly accessible privacy policy and as the only company to publish a transparency report among the assessed entities. This reflects a stronger institutional commitment to accountability and aligns more closely with the requirements of the Data Protection and Privacy Act, 2019. However, despite these strengths, Jumia continues to score poorly on third-party data transfers and breach resolution mechanisms, mirroring the sector-wide weaknesses identified last year.

Jumia's privacy policy is prominently displayed on its website and uses clear, accessible language, achieving a readability score of 9 on the Hemingway Editor. The policy outlines the purposes of data collection, including order fulfilment, surveys, service improvement, and fraud detection, and provides an exhaustive list of personal data categories collected. Data retention is tied to legal requirements, and the policy allows behavioural marketing with an opt-out option. It also recognises data subject rights, including access, correction, deletion, restriction of processing, withdrawal of consent, and the right to lodge complaints via the Data Protection Officer. Law enforcement access is permitted when reasonably requested, and the publication of a transparency report further strengthens accountability. However, the policy does not clearly specify which categories of personal data are shared with third parties, leaving a critical gap in transparency.

Kikuu Uganda, by contrast, continues to perform poorly across most indicators. While its privacy policy remains accessible (88%) and fairly readable, pre-collection transparency, third-party data transfers, security measures, and breach resolution mechanisms remain weak. Kikuu has no registration with the regulator, no transparency report, and only minimal breach resolution procedures. Its policy allows data sharing with third parties and law enforcement without clearly identifying the recipients or the categories of data involved. Personal data categories are described only in general terms, no retention timelines are provided, and access to data is granted only under limited conditions. These shortcomings are largely unchanged from last year and indicate persistent non-compliance risks.

Glovo Uganda and Jiji Uganda both present relatively accessible privacy policies but continue to lack transparency reports and exhibit weaknesses in security disclosures and third-party data governance. While Jiji has improved its registration status and breach resolution mechanisms, both platforms still fall short of best practices identified in last year's assessment.

Overall, the findings confirm that many of the issues identified in last year's analysis remain relevant and unresolved. Third-party data sharing continues to be the most significant area of concern, with insufficient disclosure and weak safeguards across all platforms. While there have been modest improvements in registration, data subject rights facilitation, and breach response mechanisms, progress remains uneven and, in some cases, minimal.

From a legal perspective, these gaps expose companies to potential non-compliance with Uganda's Data Protection and Privacy Act, 2019, particularly with respect to accountability, transparency, lawful processing, and data breach management. Jumia Uganda's publication of a transparency report demonstrates that improvement is possible and sets a benchmark for the sector. However, without broader adoption of such practices, consumer data in Uganda's growing e-commerce market remains inadequately protected.

To strengthen compliance and trust, companies must move beyond formal policy publication and address the structural weaknesses repeatedly identified in successive assessments. This includes clearly specifying third-party data sharing arrangements, improving transparency reporting, strengthening breach response mechanisms, and ensuring full regulatory registration. Without these measures, the sector risks continued regulatory exposure and erosion of consumer confidence in digital commerce platforms.

3.4.2.3 Comparing companies' Performance within the sector

This analysis presents a comparative assessment across e-commerce platforms operating in multiple African jurisdictions. Drawing on companies' overall compliance scores and year-on-year performance, it evaluates how effectively these platforms align their privacy practices with national data protection laws and international principles. The analysis highlights emerging compliance leaders, persistent structural gaps, and systemic risks, while also identifying trends that remain unchanged from the previous year and their implications for consumer trust, regulatory exposure, and the maturity of privacy governance across the sector.

High-Performing Jurisdictions: Emerging Compliance Leaders (and Trajectories)

The highest-performing companies cluster within the **50–63% range**, indicating *relative* leadership rather than full compliance. These entities demonstrate stronger institutional awareness of data protection obligations, but still fall short of best-practice standards under GDPR-aligned frameworks and national data protection laws. Leading performers include; Jumia Uganda (63%), Glovo Kenya (60%), Jiji Uganda (58%), Jiji Kenya (55%), Jiji Nigeria (54%), iStore Botswana (51%),

Several of these companies were already identified as stronger performers last year, and their relative leadership remains consistent:

- **Glovo (Kenya and Uganda)** continues to perform well, reinforcing last year's finding that international platforms benefit from mature, globally driven privacy frameworks.
- **Jiji platforms across multiple jurisdictions** (Uganda, Kenya, Nigeria, Tanzania) show steady, incremental improvement, reflecting investments in scalable compliance structures as the platform expands regionally.
- **Jumia Uganda's rise** from a mid-tier position last year (40%) to sector leader (63%) is one of the most notable improvements, suggesting enhanced transparency practices, registration compliance, and accountability mechanisms.

High-performing companies are better positioned to: Demonstrate **accountability** to regulators, reduce exposure to enforcement actions, and build **consumer trust** through clearer privacy policies, stronger security measures, and partial transparency reporting. However, even these leaders remain **only partially compliant**. Persistent weaknesses particularly, around third-party data sharing transparency, breach reporting, and user rights enforcement mean that none yet meet the threshold of full compliance under modern data protection laws.

Mid-Range Performers: Partial Compliance and Structural Gaps (with Change Over Time)

The majority of companies fall within the **35–49% range**, reflecting fragmented and uneven compliance. These platforms typically meet basic requirements such as having a privacy policy but struggle with implementation, enforcement, and accountability. Representative companies include; Glovo Uganda (45%), Jumia Kenya (44%), Temu Mauritius (44%), Woolworths Mauritius Online (42%), Kilimall Kenya (41%), Ubuy Zimbabwe (41%), Tengai Online (39%), PriceGuru, Konga, Ubuy Botswana (38%), Melcom Ghana and Kikuu Tanzania (37%), Kupatana, Tonaton Ghana (36%) and Marideal and Jumia Ghana (35%).

Last year, many of these companies were already classified as *mid-tier* (e.g. Jumia Kenya, Kilimall, Woolworths Mauritius Online, Ubuy Zimbabwe), and that status has largely **not changed**. While some have improved marginally, structural issues persist:

- **Third-party data sharing remains opaque**, often undisclosed or poorly explained.
- **Transparency reporting is still largely absent**, except in isolated cases.
- **Data subject rights mechanisms exist in theory** but are difficult to exercise in practice.

Mid-range performers face a dual risk namely: **Regulatory risk**, due to partial non-compliance with lawful processing, consent, and accountability obligations; and **Reputational risk**, as increasingly privacy-aware consumers may migrate toward platforms perceived as more trustworthy.

At the same time, this group represents the **greatest opportunity for improvement**. Many already have the foundational elements in place and could significantly raise their compliance levels by: Formalising third-party data governance, publishing transparency reports, strengthening breach response procedures, and making user rights more actionable.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

Companies scoring **below 35%** demonstrate systemic weaknesses that mirror, and in some cases worsen, the risks identified in last year's analysis. These included: Murukali (34%), Jumia Nigeria (34%), Inalipa (32%), Kikuu Rwanda (32%), Raines Africa (30%), Your Mart Botswana (30%), Kikuu Ghana (29%), Kara Nigeria (27%), Kikuu Uganda (26%), Vuba Vuba (22%), and Apex Mart Botswana (7%).

This category shows the least change over time: Platforms such as Kikuu (across Uganda, Rwanda, Ghana), Raines Africa, Inalipa, and Vuba Vuba were already flagged last year as high-risk, and they remain so. Apex Mart Botswana's 7% score represents extreme non-compliance, indicating near-total absence of basic privacy safeguards. Low-performing compa-

nies face serious legal and operational risks, including: Likely violations of national data protection laws, increased exposure to data breaches and misuse of personal data, potential enforcement actions, fines, or forced corrective measures, and loss of consumer trust and competitive disadvantage. The persistence of these low scores suggests not just capacity gaps, but institutional neglect of privacy governance. Without regulatory intervention or sustained internal reform, these platforms are unlikely to improve organically.

Key Cross-Cutting Implications

- **Progress Is Incremental, Not Transformational:** While overall scores have improved slightly since last year, the **relative rankings remain largely unchanged**. Leaders remain leaders, laggards remain laggards, and systemic issues persist across the sector.
- **Third-Party Data Sharing Remains the Weakest Link:** As highlighted last year and reaffirmed this year, **undisclosed or poorly governed third-party data sharing** is the most consistent compliance failure. This directly undermines principles of transparency, purpose limitation, and accountability embedded in data protection laws.
- **Transparency Reporting Is Still Rare:** Despite regulatory expectations, transparency reports remain the exception rather than the norm. The lack of disclosure around government access requests, data breaches, and enforcement actions continues to weaken user trust and regulatory oversight.
- **International Platforms Set the Pace:** Companies with international operations (e.g. Glovo, Jiji, Jumia in some jurisdictions) consistently outperform local competitors. This reinforces last year's conclusion that **exposure to stricter foreign regulatory regimes raises compliance standards**, benefiting local consumers.
- **Registration and Policy Availability Are Not Enough:** As seen across all tiers, **formal compliance** (registration and privacy policies) does not translate into **substantive compliance**. Effective data protection requires operational controls, enforcement mechanisms, and demonstrable accountability.

Overall, the data confirms that many of last year's findings remain valid. While there has been gradual improvement among higher- and mid-tier performers, structural weaknesses particularly, around third-party data governance, transparency, and breach management persist across jurisdictions. Low-performing companies continue to present acute risks to data subjects and regulators alike. Without stronger regulatory enforcement and a shift from symbolic to operational compliance, the gap between emerging leaders and systemic laggards is likely to widen, undermining both consumer trust and the effectiveness of data protection regimes across the region.

3.4.3 Online Betting Sector Analysis

3.4.3.1 Overview of the sector and data collectors evaluated

The online betting sector across Africa has expanded rapidly in recent years, particularly in East, Southern, and parts of West Africa, with countries such as Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, Uganda, Nigeria, Ghana, and Botswana emerging as important markets. This growth has been fuelled by increased internet connectivity, widespread mobile phone adoption, digital payment systems, and a rising interest in sports betting and online casino gaming, especially among younger populations.

Although the sector is relatively new in some jurisdictions, countries like Rwanda and Botswana have taken steps to formally license operators and introduce regulatory controls to manage online sports betting and casino activities. Tanzania and Kenya represent more established markets, where football betting dominates and a mix of local and international operators operate under sector-specific regulators such as the Gaming Board of Tanzania and Kenya's Betting Control and Licensing Board. Kenya, in particular, stands out due to its advanced mobile money ecosystem, which has significantly lowered barriers to participation.

Mauritius is often regarded as a mature and well-regulated betting market, with strong institutional oversight by the Gambling Regulatory Authority and a clear emphasis on compliance, consumer protection, and ethical standards. In Zimbabwe and Uganda, online betting especially via mobile platforms continues to grow steadily, supported by regulatory frameworks overseen by the respective Lotteries and Gaming Boards. Meanwhile, Nigeria and Ghana represent some of the largest and fastest-growing betting markets in West Africa, driven by population size, high sports engagement, and increasing digital access, although regulatory enforcement and consistency remain ongoing challenges.

Across these countries, the online betting industry continues to grapple with common concerns such as problem gambling, underage participation, data protection, and regulatory enforcement. Nevertheless, demand for convenient, digitally accessible gaming services continues to drive market expansion, making effective regulation and responsible industry practices increasingly critical.

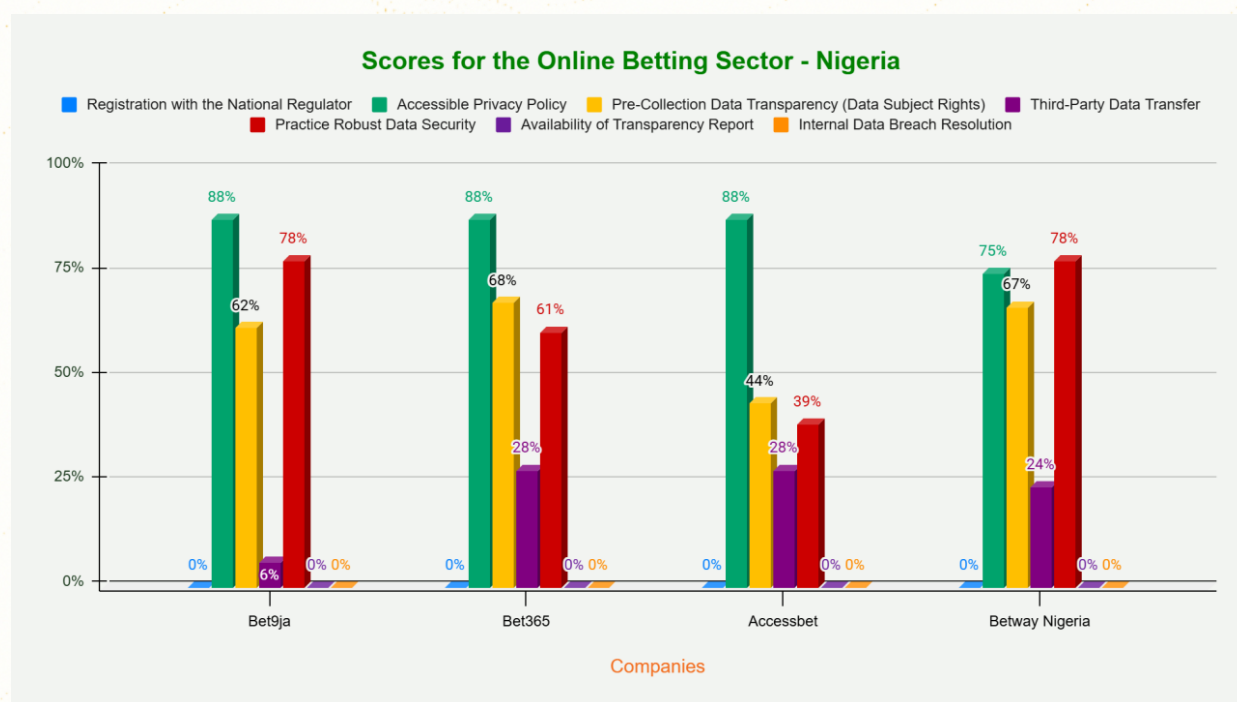
3.4.3.2 Analysis of compliance with each criterion

The report in this sector includes data from 36 companies in total, with four (4) companies chosen from each country. These consisted of: Bet9ja, Bet365, Accessbet and Betway Nigeria from Nigeria; Betpawa Ghana, 1xbet Ghana, Soccabet and Betway Ghana from Ghana; Sunbet Botswana, PstBet Botswana, SportPesa Botswana and BetXplosion in Botswana; 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. Bet9ja, Bet365, Accessbet and Betway Nigeria in Nigeria

Overall, the assessment reveals a pattern of uneven and fragmented compliance across the online betting companies reviewed. While all companies recorded very low levels of compliance with registration requirements under the national data protection regulator indicating a fundamental gap in meeting baseline legal obligations, they simultaneously demonstrated varying degrees of maturity in their internal privacy frameworks. This divergence highlights a recurring theme across the sector: strong policy design and operational controls are not consistently matched by formal regulatory compliance and accountability mechanisms.

All companies made visible efforts to maintain accessible privacy policies. Bet9ja, Bet365, and Accessbet led in this area, each scoring 88%, while Betway Nigeria followed with 75%. These high accessibility scores reflect an industry-wide recognition that privacy notices are a minimum expectation in user-facing, data-intensive services such as online betting. However, accessibility alone does not equate to legal compliance, particularly in the absence of registration and transparency reporting.



Bet9ja emerges as a notable and somewhat unexpected leader in substantive privacy practices within the sector. Despite low regulatory registration compliance, the company demonstrates advanced data governance practices that exceed those of many traditional financial and digital platforms. Its privacy policy provides extensive contact information, including a dedicated data protection email address, customer service numbers, and physical office locations, strengthening accountability and user trust.

The policy offers a detailed and granular account of the categories of personal data processed through betting operations, including identity verification documents, financial transaction records, betting history, device and location data, and behavioural analytics. Importantly, Bet9ja clearly articulates the purposes of processing, which extend beyond service delivery to include fraud prevention, anti-money laundering compliance, responsible gambling monitoring, and adherence to regulatory obligations under the National Lottery Regulatory Commission.

Bet9ja also demonstrates exceptional transparency regarding behavioural marketing, explicitly acknowledging the use of betting patterns and preferences for targeted promotions. The availability of opt-out mechanisms and clear explanations of user controls align closely with international data protection standards. Its third-party data sharing disclosures are equally robust, detailing relationships with payment processors, identity verification providers, responsible gambling organisations, regulators, and law enforcement, along with the legal justifications and safeguards governing such disclosures. The company further distinguishes itself by providing clear procedures for exercising data subject rights and escalating complaints, including pathways involving regulatory authorities.

Betway Nigeria also demonstrates relatively strong privacy compliance, with policies reflecting international best practices adapted to the Nigerian context. The company provides detailed contact information, explains the categories of data collected, and clearly links data processing to service delivery, fraud prevention, and regulatory compliance. Betway acknowledges third-party data sharing and provides users with access, correction, and complaint mechanisms. However, while its policy framework is sound, weaknesses remain in formal transparency reporting and regulatory registration, limiting full accountability.

Bet365 shows solid but less locally tailored compliance. Its privacy policy addresses most core criteria, including categories of data collected, basic third-party sharing disclosures, and standard data subject rights. However, compared to Bet9ja and Betway, Bet365 provides less Nigeria-specific detail, particularly regarding regulatory interfaces and local enforcement mechanisms. This suggests a reliance on global compliance templates rather than fully contextualised national implementation.

Despite relatively strong policy content among some operators, all companies performed poorly on third-party data sharing compliance in practice, with scores ranging from just 6% to 28%. This reflects persistent deficiencies in transparency around data flows, particularly where data is shared with advertisers, analytics providers, and external service partners. Such gaps directly undermine core data protection principles of transparency, purpose limitation, and accountability.

Similarly, while data security practices showed visible effort particularly among Bet9ja and Betway Nigeria, none of the companies published transparency reports, and all recorded very low compliance in internal data breach resolution mechanisms. The absence of documented breach response frameworks and public accountability measures raises serious concerns about preparedness to meet breach notification obligations under data protection laws.

Accessbet demonstrates only moderate compliance. While it provides basic contact information, acknowledges the collection of personal data for betting purposes, and implements fundamental data subject rights, its privacy framework lacks depth. Key gaps include the absence of clearly defined retention periods, limited detail on third-party data sharing, and weaker articulation of accountability mechanisms. These shortcomings are reflected in its lower performance across several indicators.

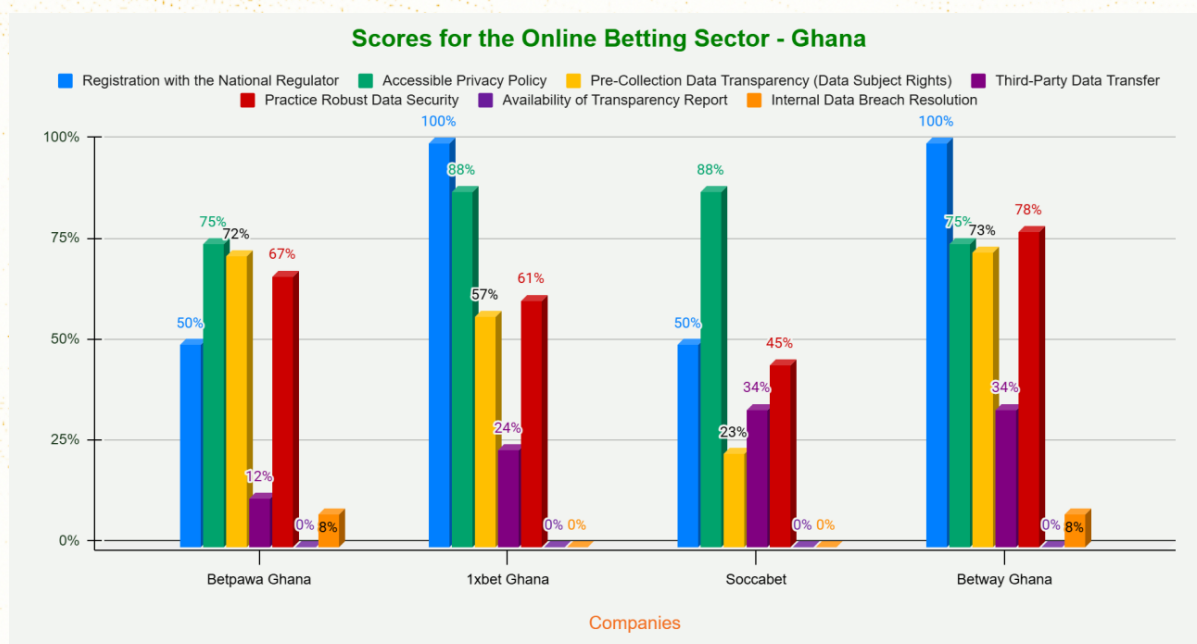
aken together, the findings indicate that the online betting sector exhibits a form of “policy-led but regulator-light” compliance. Companies such as Bet9ja and Betway have developed sophisticated internal privacy frameworks driven by operational risk management, international standards, and sector-specific regulatory pressures. However, the consistent failure to meet registration requirements, publish transparency reports, and formalise breach response processes exposes these companies to significant legal and regulatory risk.

To achieve full compliance with data protection laws, companies must align their strong internal practices with formal legal obligations, including registration with data protection authorities, clear documentation of third-party processing arrangements, and the establishment of robust breach detection, response, and notification mechanisms. Without these steps, even well-designed privacy policies will fall short of legal expectations and may not withstand regulatory scrutiny in an increasingly enforcement-driven data protection environment.

In sum, while parts of the sector demonstrate encouraging maturity in privacy governance, compliance remains partial and fragile, underscoring the need for stronger regulatory engagement and a shift from voluntary best practices to enforceable, end-to-end data protection compliance.

a. *Betpawa Ghana, 1xbet Ghana, Soccabet and Betway Ghana in Ghana*

Overall, the assessment shows uneven but emerging compliance among online betting companies operating in Ghana. While all companies demonstrated some effort to meet regulatory and privacy requirements, compliance remains fragmented, with strong performance in certain areas such as policy availability and security controls offset by persistent weaknesses in transparency, third-party data governance, and breach management.



All companies made efforts to comply with registration requirements under the national data protection framework. 1xBet Ghana and Betway Ghana are the strongest performers in this category, each achieving a perfect score of 100% and maintaining active registrations valid until 2026 and 2025 respectively. In contrast, BetPawa Ghana and Soccabet, while previously registered, currently hold inactive registration statuses due to expired certifications (November 3, 2023, and October 26, 2021, respectively), resulting in significantly lower effective compliance. This distinction has important legal implications: active registration signals formal accountability and regulatory oversight, whereas expired or inactive registrations expose companies to potential enforcement action under Ghana's Data Protection Act and weaken consumer trust.

All four companies publish privacy policies on their websites, reflecting baseline transparency. 1xBet Ghana and Soccabet lead in policy accessibility with scores of 88%, while BetPawa Ghana and Betway Ghana follow at 75%. However, visibility does not always align with usability. BetPawa Ghana's policy, while less prominent, is the most readable and concise (Hemingway grade 8; 376 words), making it more accessible to average users. By contrast, Betway Ghana's policy, though noticeable, is lengthy and difficult to read (grade 14; 3,214 words), potentially undermining meaningful user understanding. These variations highlight that accessibility and readability are as important as mere publication in meeting transparency obligations.

All companies made measurable efforts to recognise data subject rights. Betway Ghana (73%) and BetPawa Ghana (72%) performed best, offering relatively clear explanations of rights such as access, correction, and deletion. However, both impose conditions on certain rights, often linked to gambling regulations or anti-money-laundering (AML) obligations, which may limit practical enforceability. 1xBet Ghana (57%) recognises GDPR-like rights but omits key elements such as complaint mechanisms and clear retention timelines. Soccabet (23%) lags significantly, offering minimal recognition of user rights and reflecting weak alignment with data protection principles of fairness and user control.

All companies share personal data with third parties, yet compliance in this area remains consistently low, presenting one of the most significant risks under data protection law. Soccabet and Betway Ghana lead with only 34%, followed by 1xBet Ghana (24%) and BetPawa Ghana (12%). Although some companies identify categories of recipients such as payment processors, affiliates, regulators, and law enforcement, none provide comprehensive disclosure of the specific data types shared, safeguards applied, or reporting channels for misuse. This lack of transparency undermines core legal principles of purpose limitation, proportionality, and accountability under Ghana's Data Protection Act.

There were visible efforts to ensure data security across the sector. Betway Ghana performed best with 78%, supported by explicit measures including encryption, network security, authentication controls, and audits, alongside relatively strong technical indicators (B SSL rating; B security header score). BetPawa Ghana (67%) and 1xBet Ghana (61%) also demonstrate moderate security maturity, though both suffer from weak security header scores and insufficient policy detail. Soccabet, despite a strong SSL score (A), performs poorly overall (45%) due to inadequate policy disclosures and a failing security header score. These findings suggest that while encryption is widely implemented, broader security governance and transparency remain inconsistent.

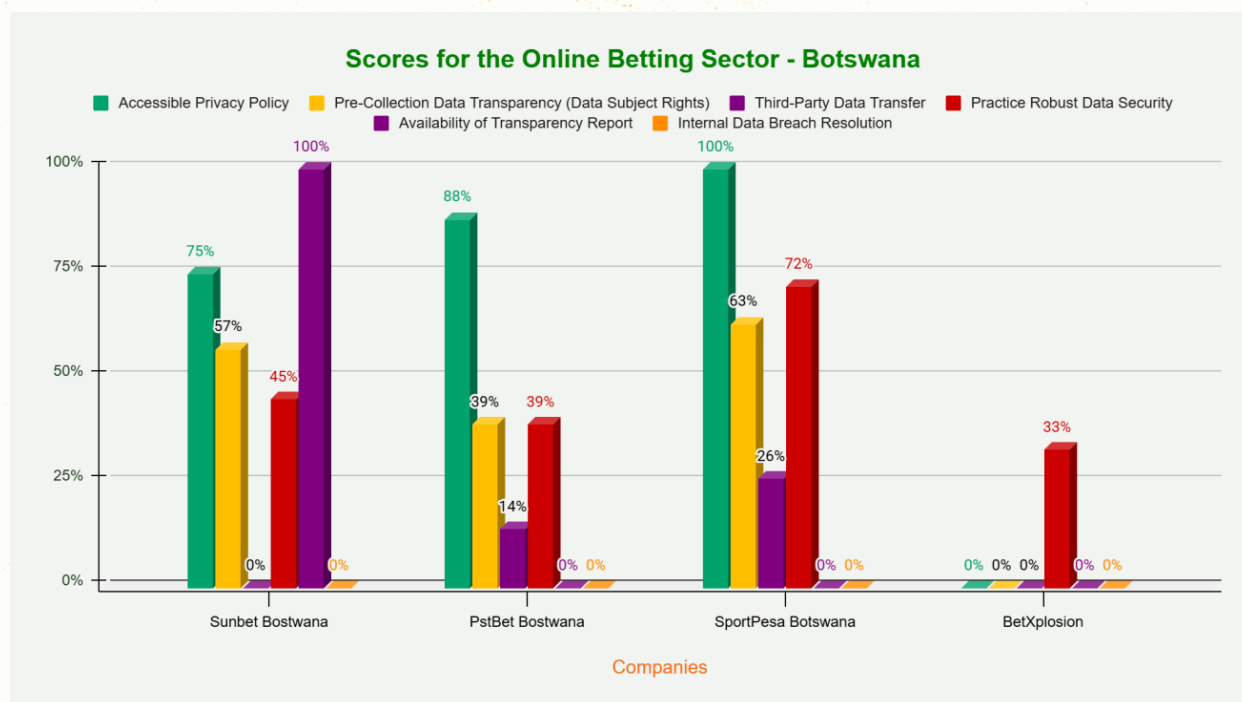
All companies scored 0% for transparency reporting, as none have published transparency reports since 2024. This absence significantly weakens accountability and deprives users and regulators of insight into government requests, enforcement actions, or data breaches. Similarly, internal data breach resolution mechanisms are underdeveloped. BetPawa Ghana and Betway Ghana scored only 8%, referencing general compliance with security and data protection laws but failing to outline clear breach notification procedures or reporting channels. 1xBet Ghana and Soccabet scored 0%, offering no meaningful breach management frameworks. These gaps directly conflict with legal obligations to detect, report, and remediate breaches in a timely and transparent manner.

Taken together, the findings indicate that Ghana's online betting companies exhibit policy-driven but incomplete compliance. While accessible privacy policies, recognition of data subject rights, and basic security measures are increasingly common, critical elements of full legal compliance active regulatory registration, transparent third-party data governance, breach response mechanisms, and public accountability remain weak or absent. From a regulatory perspective, inactive registrations, opaque data sharing practices, and the absence of transparency reporting expose companies to enforcement risks under the Data Protection Act, 2012 (Act 843). From a consumer perspective, these gaps limit users' ability to understand, control, and seek redress for the use of their personal data.

To strengthen compliance and trust, companies must move beyond surface-level transparency and invest in end-to-end privacy governance, including maintaining active registrations, clarifying third-party data flows, publishing transparency reports, and implementing robust breach response and notification procedures. Without these measures, current improvements in policy accessibility and security will remain insufficient to meet legal standards or protect users in Ghana's rapidly expanding online betting market.

b. *Sunbet Botswana, PstBet Botswana, SportPesa Botswana and BetXplosion in Botswana*

The assessment of SportPesa Botswana, Sunbet Botswana, PstBet Botswana, and BetXplosion, reveals uneven and largely incomplete compliance with data protection requirements. While some operators demonstrate partial efforts in policy accessibility, data security, and transparency, most fail to provide meaningful and comprehensive protections for users, particularly in areas central to accountability and risk management.



Visible efforts to maintain accessible privacy policies were observed among three of the four companies. SportPesa Botswana performed best with a perfect score of 100%, followed by PstBet Botswana (88%) and Sunbet Botswana (75%). These scores suggest that these operators recognise the importance of making privacy information visible and available to users. By contrast, BetXplosion scored 0%, as it provides no accessible privacy policy, representing a fundamental failure to meet basic transparency obligations under data protection laws.

All companies, except BetXplosion, made some effort to recognise data subject rights. SportPesa Botswana again led with 63%, followed by Sunbet Botswana (57%) and PstBet Botswana (39%), while BetXplosion scored 0%. Although these

results indicate some awareness of rights such as access, correction, and deletion, the moderate scores suggest that mechanisms for exercising these rights are limited, unclear, or inconsistently implemented. This undermines the principle of user control that is central to modern data protection frameworks.

All companies were found to share personal data with third parties, yet compliance in this area is critically low across the sector. SportPesa Botswana, the strongest performer, scored only 26%, while PstBet Botswana scored 14% and Sunbet Botswana and BetXplosion both scored 0%. These findings highlight a widespread lack of transparency regarding who receives user data, for what purposes, and under what safeguards. Given the volume of sensitive financial and personal data processed in online betting, such deficiencies present significant compliance and consumer protection risks.

Visible efforts to ensure data security were observed, though with varying levels of maturity. SportPesa Botswana again led with a relatively strong score of 72%, followed by Sunbet Botswana (45%), PstBet Botswana (39%), and BetXplosion (33%). While these results suggest that technical safeguards such as encryption may be in place, lower scores for several operators indicate gaps in organisational measures, documentation, and ongoing security governance.

Transparency and breach preparedness remain major weaknesses. Sunbet Botswana was the only company to publish a transparency report, while all others lacked any such disclosure. However, even Sunbet scored poorly in internal data breach resolution, and all companies registered very low levels of compliance in this area. The absence of clearly defined breach response procedures, reporting channels, and notification commitments raises serious concerns about how these companies would respond to data incidents, contrary to legal requirements under Botswana's data protection framework.

Sunbet Botswana performs relatively better in the sector. It provides an accessible privacy policy, explains data collection purposes, and demonstrates some attention to security and pre-collection disclosures. However, it scores zero on third-party transfer transparency and breach resolution, meaning users remain unprotected once data leaves its systems or in the event of a breach.

PstBet Botswana shows mixed performance. While its privacy policy is accessible, it performs poorly on transparency indicators, leaving customers largely uninformed about how their data is shared and protected. Limited disclosure of third-party transfers, weak security governance, and the absence of internal breach resolution mechanisms significantly weaken its compliance posture. SportPesa Botswana demonstrates stronger practices than most peers. It combines a fully accessible privacy policy with relatively good security measures and above-average pre-collection transparency. Nonetheless, it continues to allow poorly disclosed third-party data transfers and has not published any transparency reports since 2023. Like the other companies, it also lacks effective internal breach resolution mechanisms. BetXplosion is by far the weakest performer. It provides no accessible privacy policy, no meaningful disclosures on data processing or third-party transfers, and minimal evidence of data security measures. Its zero scores for transparency and breach resolution reflect a near-total absence of privacy governance and pose severe risks to user data.

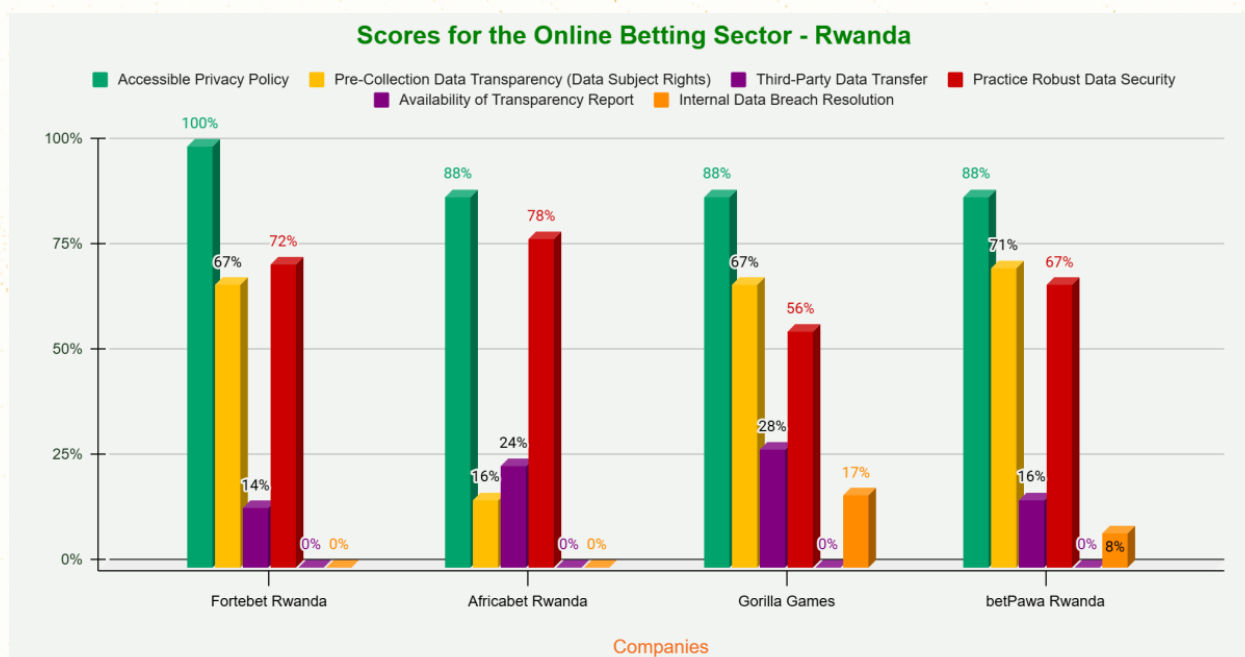
Overall, the online betting sector in Botswana is characterised by serious and systemic compliance gaps. While SportPesa and Sunbet show some effort in policy accessibility and data security, and PstBet demonstrates limited progress, these measures fall well short of the comprehensive protections required under data protection laws. BetXplosion's near-total non-compliance represents a particularly high risk for both users and regulators. Key areas requiring urgent attention across the sector include the establishment of robust internal breach resolution mechanisms, meaningful transparency reporting, and strict controls and disclosures around third-party data sharing. Without addressing these weaknesses, companies risk regulatory enforcement, reputational damage, and erosion of consumer trust in an industry that relies heavily on the processing of sensitive personal and financial data.

c. Fortebet Rwanda, Africabet Rwanda, Gorilla Games and BetPawa Rwanda in Rwanda

The current assessment shows measurable progress in policy availability, data subject rights recognition, and security disclosures, alongside persistent structural weaknesses in transparency reporting, third-party data governance, and breach management. Compared to last year, the sector demonstrates incremental maturity rather than systemic transformation, with compliance improvements concentrated among a few operators while others stagnate or regress. All companies assessed now have publicly available and noticeable privacy policies exceeding 200 words, reflecting baseline compliance with transparency obligations. ForteBet Rwanda leads with a perfect score of 100%, supported by a relatively concise and readable policy (1,133 words). Africabet Rwanda, Gorilla Games, and BetPawa Rwanda each score 88%, maintaining or improving on last year's performance, Africabet Rwanda and Gorilla Games remained consistent, while BetPawa Rwanda improved from 75%.

However, usability remains uneven. Gorilla Games and BetPawa Rwanda have extremely long policies (over 4,700 words each) with higher readability grades (12–13), which may discourage meaningful user engagement despite their comprehensiveness. This reflects a continuing trend from last year: policy availability has improved, but user-friendly transparency remains limited.

Visible improvements were observed in the recognition of data subject rights. BetPawa Rwanda now leads with 71%, a dramatic increase from 18% last year, reflecting clearer articulation of rights such as access, correction, deletion, objection, portability, and complaint mechanisms. ForteBet Rwanda and Gorilla Games follow closely at 67%, with Gorilla Games improving from 56%.



In contrast, Africabet Rwanda's score dropped sharply to 16%, marking a regression from last year's moderate performance. This decline signals a shift toward a more compliance-minimalist approach focused on legal obligations rather than user empowerment. Overall, while leading companies now provide stronger rights frameworks, implementation gaps remain, particularly where rights are conditional, poorly explained, or unsupported by clear procedures.

As in last year's analysis, third-party data sharing remains the most problematic compliance area. All companies share personal data with third parties, yet scores remain low across the board. Gorilla Games again leads at 28%, unchanged from last year, followed by Africabet Rwanda (24%), a steep decline from 70%, BetPawa (16%), and ForteBet (14%).

While BetPawa provides the most comprehensive list of third-party categories including advertisers, payment processors, affiliates, and regulators it still fails to specify the exact data types shared or breach reporting channels. ForteBet and Gorilla Games disclose broad categories of recipients but lack specificity and safeguards, while Africabet provides minimal detail. These recurring deficiencies, also highlighted in last year's assessment, continue to undermine compliance with principles of purpose limitation, transparency, and accountability under Rwandan law.

Data security practices show incremental improvement across all companies. Africabet Rwanda now leads with 78%, up from 72%, followed by BetPawa Rwanda (67%), a notable increase from 33%, ForteBet Rwanda (72%), and Gorilla Games (56%). Strong SSL ratings (A to A+) are common, and some improvement in security headers is evident.

However, as last year, most policies remain high-level and non-technical, offering general assurances rather than detailed explanations of safeguards, access controls, or monitoring mechanisms. This limits users' and regulators' ability to assess actual security effectiveness, indicating that technical maturity is advancing faster than governance transparency.

None of the companies (ForteBet Rwanda, Africabet Rwanda, Gorilla Games, or BetPawa Rwanda) have published a transparency report since 2024. This results in a 0% score across the sector, unchanged from last year. The continued absence of transparency reporting reflects limited public accountability regarding government requests, enforcement actions, or data handling practices and remains one of the most entrenched weaknesses in the sector.

Internal data breach resolution mechanisms remain poorly developed, with only marginal improvements. Gorilla Games again leads with 17%, unchanged from last year, by acknowledging that breach procedures exist and that users and regulators will be notified when legally required though without timelines or reporting channels. BetPawa Rwanda improved slightly to 8% from 0%, referencing legal compliance but offering no procedural detail. ForteBet Rwanda and Africabet Rwanda continue to score 0%, providing no guidance on breach detection, response, notification, or redress. As highlighted in last year's analysis, this deficiency poses a serious risk given the sensitive financial, identity, and behavioural data processed by betting platforms.

Taken together, the current findings indicate that Rwanda’s online betting sector is slowly consolidating baseline privacy compliance, particularly in policy availability, security measures, and data subject rights among leading operators. BetPawa Rwanda now emerges as the strongest overall performer, while ForteBet Rwanda and Gorilla Games maintain relatively solid but incomplete frameworks. Africabet Rwanda, however, shows concerning regression in user rights and transparency.

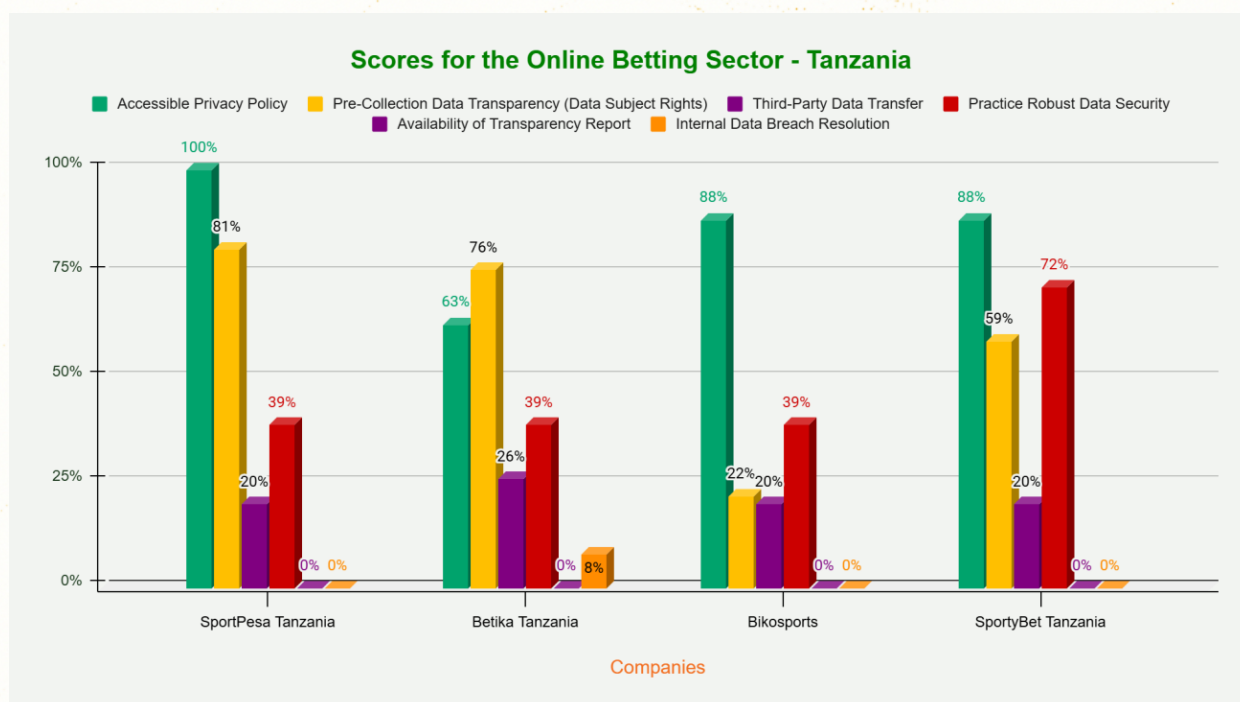
Critically, the most serious weaknesses identified last year remain unresolved: poor transparency around third-party data sharing, the absence of transparency reports, and weak or non-existent breach response mechanisms. These persistent gaps expose companies to regulatory enforcement risks under Rwanda’s Data Protection and Privacy Law and undermine consumer trust in a sector handling highly sensitive personal and financial data. To move from partial to meaningful compliance, companies must complement strong policies and security measures with clear accountability tools including transparency reporting, detailed third-party disclosures, and robust breach management procedures.

Without addressing these systemic shortcomings, progress in other areas will remain insufficient to ensure full legal compliance or effective user protection.

d. *SportPesa Tanzania, Betika Tanzania, Bikosports and SportyBet in Tanzania*

The current assessment of Tanzania’s online betting sector covering SportPesa Tanzania, Betika Tanzania, SportyBet Tanzania, and Bikosports shows continued strength in privacy policy accessibility and pre-collection transparency, alongside persistent and in some cases worsening weaknesses in third-party data sharing, transparency reporting, and breach response mechanisms. Compared with last year, the sector reflects incremental progress in user rights recognition and data security for some operators, but also regression in critical accountability indicators, suggesting uneven and fragile compliance maturity.

All companies demonstrate clear efforts to maintain accessible privacy policies. SportPesa Tanzania again leads with a perfect 100%, maintaining its top position from last year. Its policy remains highly readable (Hemingway grade 8) despite its length (3,687 words), striking a balance between comprehensiveness and usability. Bikosports and SportyBet Tanzania each score 88%, with Bikosports showing notable improvement from 63% last year, while SportyBet maintains its previous performance. Betika Tanzania continues to lag slightly at 63%, unchanged from last year.



This sustained performance indicates that baseline transparency through policy publication is now well established across the sector, representing a positive and stable compliance trend.

Considerable progress is evident in the recognition of data subject rights. SportPesa Tanzania leads with 81%, followed by Betika Tanzania at 76%, reflecting clearer articulation of rights such as access, correction, deletion, and objection. SportyBet Tanzania scores a moderate 59%, while Bikosports remains a weak outlier at 22%, suggesting minimal practical mechanisms for users to exercise their rights.

Compared to last year, this marks a general upward trajectory, particularly for SportPesa and Betika. However, the uneven performance highlights that rights recognition remains policy-dependent rather than sector-wide, limiting consistent user protection. As in last year's analysis, third-party data sharing remains the most problematic compliance area. All companies share personal data with third parties, yet none score above 26%. Betika Tanzania leads marginally at 26%, improving from 10% last year, while SportPesa Tanzania, SportyBet Tanzania, and Bikosports each score 20%.

Notably, SportPesa Tanzania declined sharply from 40% last year, and SportyBet Tanzania dropped from a relatively strong 70%, indicating regression in transparency and safeguards around third-party transfers. Although Bikosports improved from 10%, its overall performance remains weak. These trends confirm that opaque third-party data flows remain a systemic and unresolved risk, directly conflicting with the transparency and accountability requirements of Tanzania's data protection law.

In the area of data security, SportyBet Tanzania emerges as the strongest performer at 72%, improving significantly from 50% last year, supported by an A+ SSL rating. However, even SportyBet's policy remains high-level, lacking detailed explanations of technical and organisational safeguards. SportPesa Tanzania, Betika Tanzania, and Bikosports each score 39%, unchanged from last year, indicating stagnation in security governance despite handling sensitive financial and identity data. This pattern suggests that while technical infrastructure may be adequate, policy-level transparency and accountability around security controls remain underdeveloped. As in the previous assessment, none of the companies have published a transparency report, resulting in a 0% score across the sector. This ongoing absence indicates limited public accountability regarding data requests, enforcement actions, or internal compliance practices.

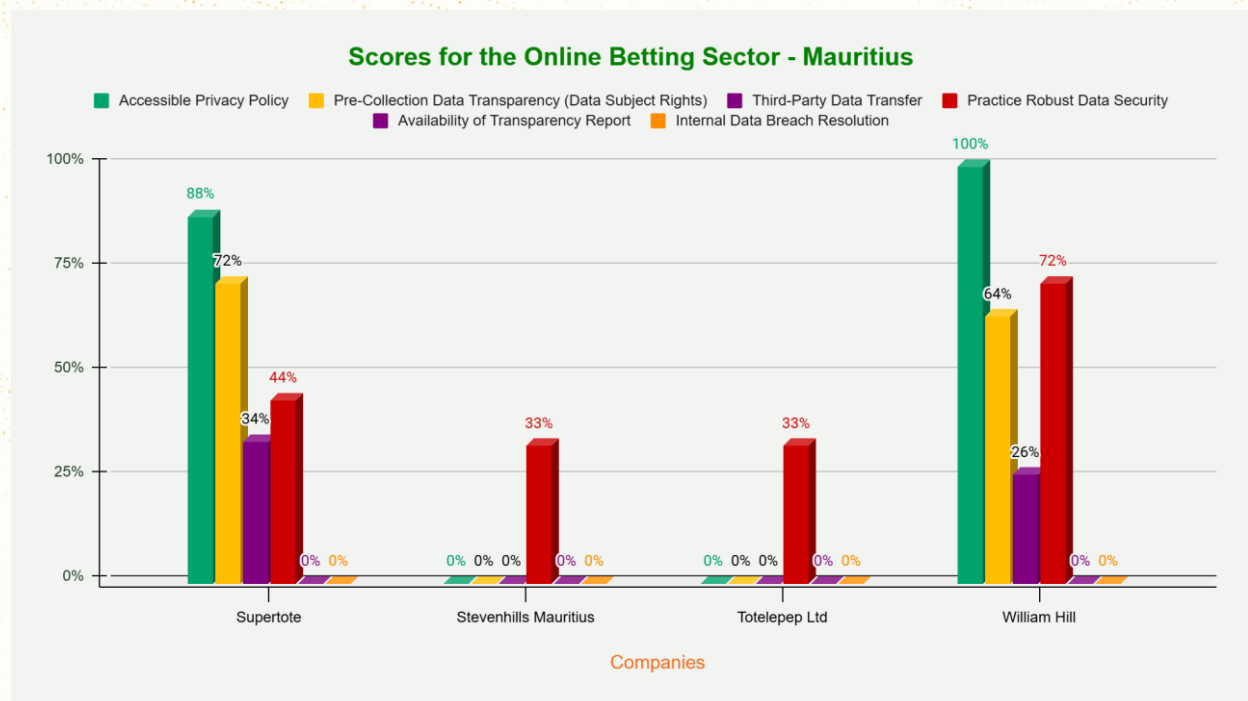
Similarly, internal data breach resolution mechanisms remain extremely weak. Only Betika Tanzania references data breaches in its privacy policy, but without clear procedures, timelines, or reporting channels. The remaining companies make no meaningful provision for breach management. This lack of progress mirrors last year's findings and represents a serious compliance gap under Tanzania's Personal Data Protection Act, particularly given the sensitivity of betting-related personal and financial data.

Overall, Tanzania's online betting sector demonstrates strong and stable performance in privacy policy accessibility and pre-collection transparency, with incremental improvements in data subject rights and security among leading operators. SportPesa Tanzania and Betika Tanzania continue to set the pace in user-facing compliance, while SportyBet Tanzania shows meaningful improvement in security practices. However, the most critical weaknesses identified last year remain largely unchanged and in some cases have worsened, notably in third-party data sharing transparency, breach preparedness, and public accountability through transparency reporting.

These persistent gaps expose operators to regulatory enforcement risks and undermine user trust in an industry that processes highly sensitive personal and financial data. To achieve full and durable compliance, companies must move beyond accessible policies and technical safeguards to implement robust accountability mechanisms, including detailed third-party disclosures, clear breach response frameworks, and regular transparency reporting. Without addressing these systemic shortcomings, progress in other compliance areas will remain insufficient to meet the requirements of Tanzania's evolving data protection regime.

e. Supertote, Stevenhills Mauritius, Totelepep Ltd and William Hill in Mauritius

The current assessment of Mauritius' online betting sector covering William Hill Mauritius, Supertote, Stevenhills Mauritius, and Totelepep Ltd reveals a persistent compliance divide between internationally established operators and smaller or less transparent platforms. Compared with last year, leading companies have consolidated their strengths in policy accessibility and security, while structural weaknesses remain entrenched across the sector, particularly in transparency reporting, third-party data governance, and breach response mechanisms. As in the previous assessment, William Hill Mauritius and Supertote continue to lead in making privacy policies accessible to users, scoring 100% and 88% respectively. These results reflect sustained compliance and align with last year's findings, where both companies already outperformed their peers.



In contrast, Stevenhills Mauritius and Totelepep Ltd once again recorded 0%, indicating that neither company has a publicly available privacy policy. This unchanged outcome underscores a continuing failure to meet even the most basic transparency requirements under data protection law.

Performance on data subject rights largely mirrors last year's trends. Supertote and William Hill maintained relatively strong scores at 72% and 64% respectively, reflecting ongoing recognition of rights such as access, rectification, erasure, objection, and complaint mechanisms. Their policies provide at least one clear channel typically via a Data Protection Officer for users to exercise these rights.

By contrast, Stevenhills Mauritius and Totelepep Ltd continue to show no meaningful recognition of data subject rights, reinforcing their overall non-compliance. The lack of progress in this area signals a continued risk of rights violations and regulatory exposure.

All companies assessed share personal data with third parties, yet compliance remains weak across the sector, consistent with last year's findings. William Hill Mauritius improved slightly to 26% from 22%, while Supertote declined to 34% from 48%, indicating reduced clarity or safeguards around data sharing arrangements. The remaining companies again scored 0%, reflecting either non-disclosure or the absence of documented controls. Although William Hill and Supertote both outline categories of third parties such as service providers, regulators, financial institutions, and auditors the disclosures remain broad. They generally fail to specify the exact data shared, individual recipients, or robust accountability measures, limiting compliance with the principles of transparency and purpose limitation.

Data security remains one of the stronger areas of compliance, with William Hill Mauritius improving to 72% from 61%, demonstrating increased attention to technical and organisational safeguards. Supertote, however, declined to 44% from 61%, suggesting stagnation or reduced emphasis on security governance. Stevenhills Mauritius and Totelepep Ltd each scored 33%, reflecting slight improvement or maintenance compared to last year but still indicating inadequate protection for sensitive betting and financial data.

While leading companies reference encryption, safeguards, and compliance frameworks, policy disclosures remain high-level, offering limited insight into internal security controls, monitoring, or incident response preparedness. As in last year's assessment, none of the companies have published a transparency report, resulting in a 0% score across the sector. This persistent absence highlights limited public accountability regarding government requests, data access, or enforcement actions.

Similarly, internal data breach resolution mechanisms remain severely underdeveloped. Neither William Hill nor Supertote provides clear internal procedures, notification timelines, or multi-channel reporting mechanisms for data breaches. Stevenhills Mauritius and Totelepep Ltd offer no guidance at all. This unchanged situation represents a significant compliance gap under Mauritius' Data Protection Act, particularly given the sensitive nature of gambling-related personal and financial data.

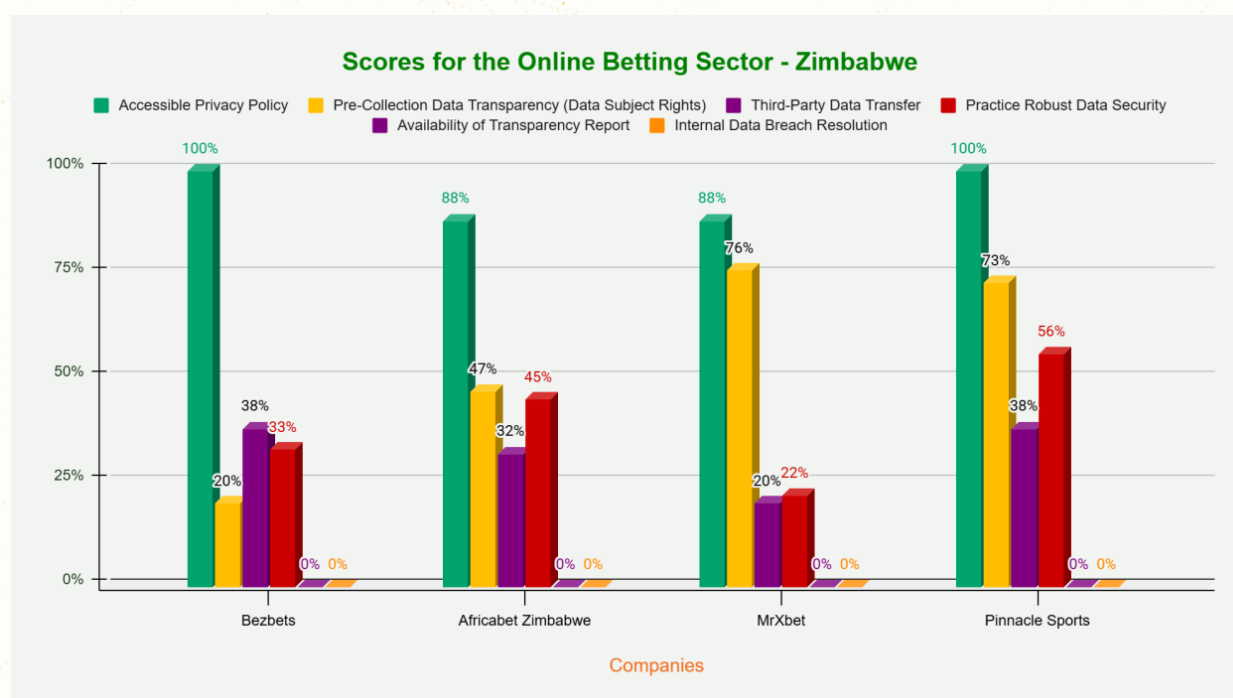
Overall, the Mauritian online betting sector continues to exhibit a two-tier compliance landscape. William Hill Mauritius and Supertote demonstrate relatively mature privacy governance, with accessible policies, recognised user rights, defined retention periods, and references to legal safeguards. However, even these leading companies fall short in critical accountability areas, notably third-party data transparency, breach management, and public reporting.

Conversely, Stevenhills Mauritius and Totelep Ltd remain largely non-compliant, with no visible progress since last year. Their continued failure to publish privacy policies, recognise user rights, or demonstrate security and accountability mechanisms exposes users to significant privacy risks and places the companies at high risk of regulatory enforcement and reputational harm.

In sum, while there has been incremental improvement among top performers, the core weaknesses identified in last year's analysis remain unresolved. Meaningful compliance will require not only accessible policies and security assurances, but also robust accountability frameworks, including transparency reporting, detailed third-party disclosures, and clearly defined breach response procedures. Without these reforms, user trust and lawful data processing in Mauritius' online betting sector will remain fragile.

f. *Bezbets, Africabet, Mrbet and Pinnacle Sports in Zimbabwe*

The analysis shows incremental but uneven progress across all four companies in strengthening their privacy practices and alignment with data protection principles. As in the previous year, all companies demonstrated efforts to maintain accessible privacy policies, an essential baseline for transparency and lawful processing. Bezbets and Pinnacle Sports remain the clear leaders, sustaining perfect scores of 100%, consistent with last year's findings and reflecting mature disclosure practices. Africabet Zimbabwe maintained its strong position at 88%, while Mr Xbet recorded a notable improvement, rising from 63% to 88%, indicating a significant enhancement in the accessibility and clarity of its privacy policy documentation.



More substantive gains were observed in the area of data subject rights, which is central to compliance with modern data protection laws. Mr Xbet now leads in this category with a score of 76%, up from 64%, suggesting strengthened mechanisms for rights such as access, correction, and deletion. Pinnacle Sports also improved, moving from 68% to 73%, maintaining its consistently strong performance. Africabet Zimbabwe showed meaningful progress, increasing from 28% to 47%, though implementation remains partial. In contrast, Bezbets experienced a slight decline from 23% to 20%, highlighting a relative stagnation in operationalising user rights despite its strong policy transparency. This divergence suggests that policy availability is not always matched by effective rights enablement.

All companies continued to share personal data with third parties, yet compliance in this area remains weak overall, posing ongoing risks under data protection frameworks that require purpose limitation, accountability, and safeguards for onward transfers. While Bezbets and Pinnacle Sports jointly lead at 38%, this still represents less than half of expected compliance, despite improvement from last year's 24%.

Africabet Zimbabwe and Mr Xbet also improved (from 10% to 32% and 20% respectively), but the low scores across the board indicate insufficient disclosure, contractual controls, or user-facing transparency around third-party data sharing.

With respect to data security, performance remained largely static. Pinnacle Sports continues to lead at 56%, consistent with last year and suggesting relatively stable technical and organisational safeguards. Africabet Zimbabwe experienced a regression from 50% to 45%, while Bezbets (33%) and Mr Xbet (22%) showed no measurable improvement. These results point to limited advancement in documented security measures, staff accountability, or risk management practices, which are core obligations under data protection laws.

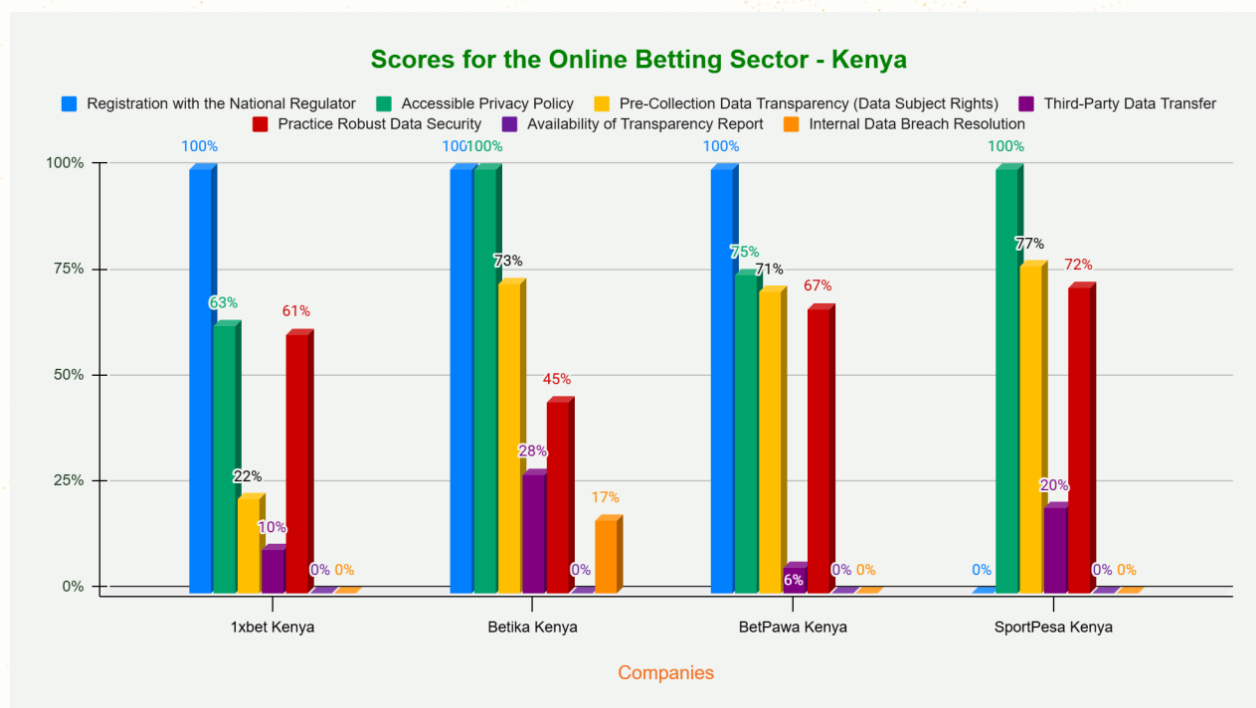
Critically, and unchanged from last year, none of the companies published transparency reports or demonstrated the existence of internal data breach detection and resolution mechanisms. This persistent gap represents a major compliance and accountability weakness, particularly in light of regulatory expectations for breach preparedness, notification, and auditability.

Overall, while the year-on-year analysis reflects modest improvements, especially in privacy policy accessibility and data subject rights, the companies' privacy practices remain largely compliance-driven at a surface level. Deeper operational measures, particularly around third-party data sharing, security governance, and breach response, remain underdeveloped. Without addressing these structural deficiencies, the companies continue to face elevated legal, regulatory, and reputational risks under applicable data protection laws.

g. *Ixbet Kenya, Betika Kenya, BetPawa Kenya and SportPesa Kenya in Kenya*

The assessment reflects a mixed compliance trajectory among the four Kenyan betting companies, with notable progress in regulatory registration and selective improvements in privacy governance, alongside persistent structural gaps that continue to undermine full compliance with data protection laws.

A significant positive development compared to last year is compliance with national regulatory registration requirements. 1Xbet Kenya, Betika Kenya, and BetPawa Kenya each scored 100%, marking a substantial improvement from 0% previously. This shift indicates increased regulatory engagement and alignment with licensing obligations, which strengthens accountability and provides a foundation for lawful personal data processing. SportPesa Kenya, however, did not demonstrate similar progress in this area, suggesting continued regulatory risk.



All companies continued to make efforts to maintain accessible privacy policies, reinforcing baseline transparency obligations. Betika Kenya and SportPesa Kenya now lead with perfect scores of 100%, reflecting improved clarity and accessibility compared to last year, when Betika scored 88% and SportPesa already led the category. BetPawa Kenya maintained its position at 75%, while 1Xbet Kenya remained unchanged at 63%. While these scores suggest that privacy notices are largely in place, they do not, on their own, guarantee effective implementation of data protection principles.

More meaningful progress was observed in the operationalisation of data subject rights. SportPesa Kenya leads this category with 77%, up from 63%, indicating strengthened mechanisms for enabling user rights such as access, rectification, and deletion. Betika Kenya also improved slightly, rising from 69% to 73%. BetPawa Kenya recorded the most significant year-on-year improvement, increasing from 19% to 71%, suggesting substantial investment in rights management processes. In contrast, 1Xbet Kenya's score dropped sharply from 41% to 22%, highlighting a regression that raises concerns about the consistency and effectiveness of its rights-handling procedures.

As in the previous year, all companies shared personal data with third parties but demonstrated very low levels of compliance in this area. Overall performance either stagnated or declined, underscoring a persistent weakness in transparency, safeguards, and accountability for data transfers. Betika Kenya leads marginally at 28%, down from 30%, followed by SportPesa Kenya at 20%, also down from 30%. 1Xbet Kenya remained unchanged at 10%, while BetPawa Kenya declined further to 6%. These results point to ongoing risks related to inadequate disclosure of third-party relationships, insufficient contractual controls, and limited user awareness, all of which are critical requirements under data protection laws.

Efforts to ensure data security remained comparatively stronger, though performance was uneven. SportPesa Kenya continues to lead at 72%, despite a decline from 83%, suggesting that while safeguards exist, continuous improvement may be lacking. BetPawa Kenya showed marked progress, doubling its score from 33% to 67%, indicating enhanced technical or organisational security measures. Betika Kenya also improved modestly from 39% to 45%, while 1Xbet Kenya remained static at 61%. These results suggest that while data security receives greater attention than other compliance areas, it is not being uniformly strengthened across all companies.

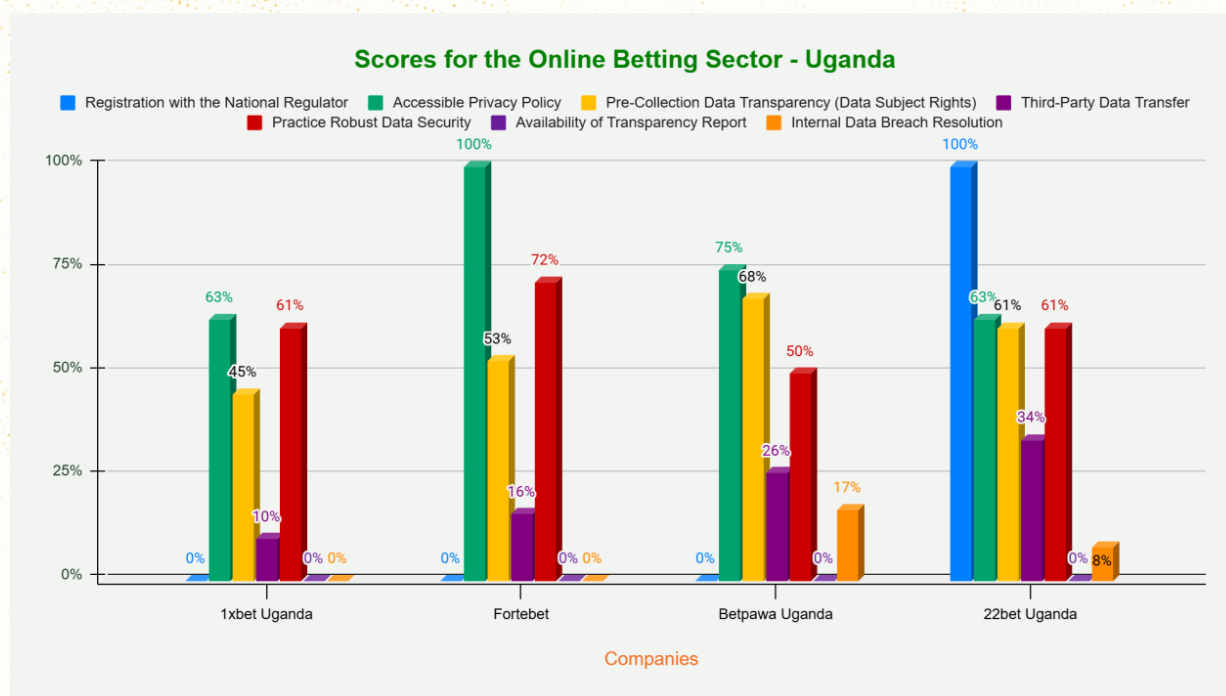
Notably, and unchanged from last year, none of the companies published transparency reports or demonstrated internal data breach detection and resolution mechanisms. This ongoing absence represents a critical compliance gap, particularly given legal obligations around breach preparedness, notification, and accountability. The lack of progress in these areas significantly undermines overall privacy governance maturity.

In summary, the year-on-year comparison reveals tangible progress in regulatory registration, privacy policy accessibility, and, for some companies, data subject rights and security. However, persistent deficiencies in third-party data sharing practices, breach management, and transparency reporting continue to expose the companies to legal and regulatory risks. To achieve meaningful compliance with data protection laws, future efforts will need to move beyond formal documentation and address the operational and accountability mechanisms that underpin effective privacy protection.

h. Ixbet Uganda, Forbet, BetPawa Uganda and 22bet Uganda in Uganda

The performance of Ugandan betting companies reveals limited but notable progress in specific compliance areas, alongside persistent and systemic weaknesses that continue to undermine effective adherence to data protection laws. While incremental improvements are evident compared to last year, overall privacy governance across the sector remains underdeveloped.

A key development is progress in regulatory registration. Unlike last year, when none of the companies demonstrated compliance, 22Bet Uganda achieved full compliance with national regulatory registration requirements, scoring 100%. This marks a significant improvement from 0% and indicates increased regulatory accountability and a stronger legal basis for personal data processing. However, the remaining companies, Fortebet, BetPawa Uganda, and 1Xbet Uganda continue to score 0%, suggesting ongoing non-compliance and heightened regulatory risk.



With respect to accessible privacy policies, performance remained largely unchanged from last year. Fortebet continues to lead with a perfect score of 100%, reflecting sustained transparency in policy availability. BetPawa Uganda maintained its score of 75%, while 1Xbet Uganda and 22Bet Uganda remained at 63%. These stable scores suggest that while baseline transparency through published privacy policies is established, progress has stalled, and accessibility alone has not translated into broader compliance improvements.

More encouraging developments were observed in the implementation of data subject rights. BetPawa Uganda recorded the most substantial improvement, rising from 29% to 68%, indicating enhanced recognition of user rights such as access, correction, and deletion. 22Bet Uganda also improved from 41% to 61%, suggesting more structured rights-handling processes. In contrast, Fortebet and 1Xbet Uganda experienced slight declines, falling to 53% (from 55%) and 45% (from 51%) respectively. These mixed results indicate uneven institutional commitment to embedding data subject rights into operational practices.

All companies continued to share personal data with third parties, but compliance in this area remains weak, despite some year-on-year improvements. 22Bet Uganda now leads with 34%, up from 10%, followed by BetPawa Uganda at 26% (up from 24%). Fortebet improved marginally from 0% to 16%, while 1Xbet Uganda declined significantly from 34% to 10%. The persistently low scores reflect insufficient transparency around the nature, purpose, and safeguards of third-party data sharing, posing ongoing risks under data protection laws that require accountability and user awareness.

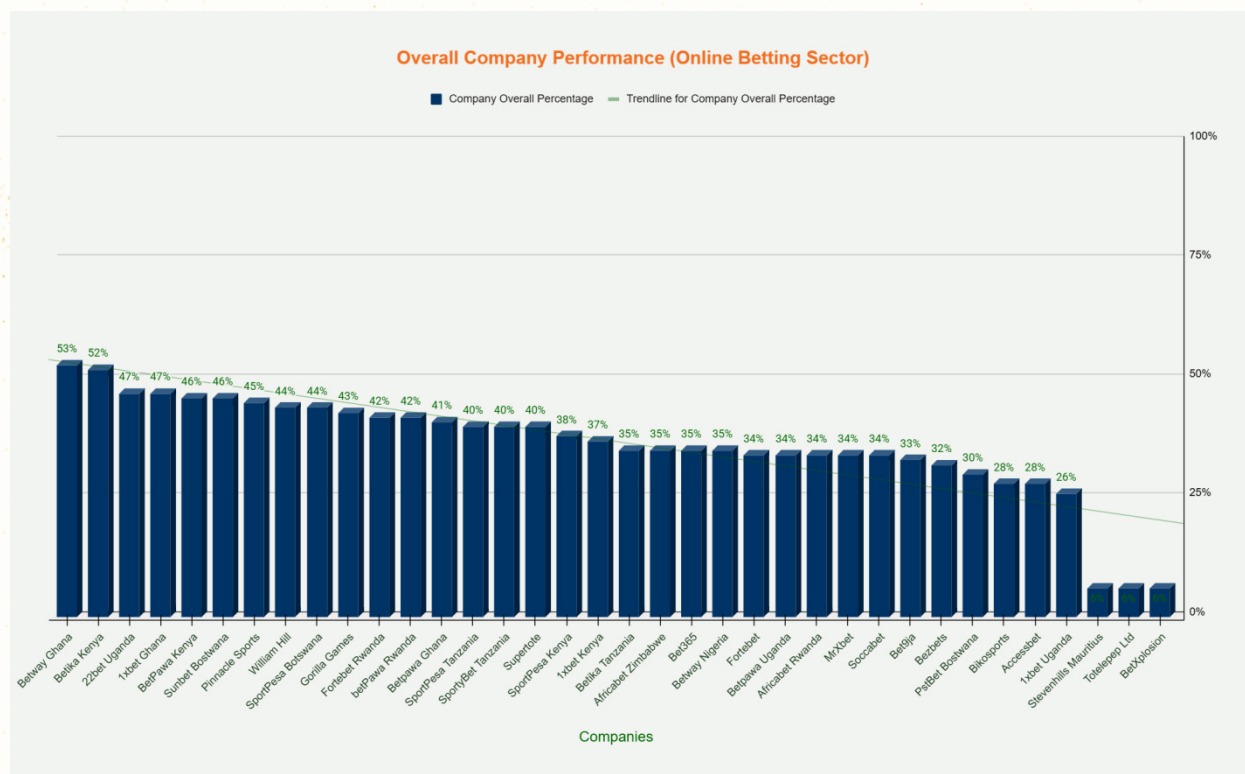
Data security remains one of the stronger areas, though recent declines are notable. Fortebet maintained its lead at 72%, consistent with last year, suggesting relatively stable technical and organisational safeguards. However, both 1Xbet Uganda and 22Bet Uganda dropped sharply from 78% to 61%, raising concerns about stagnation or reduced emphasis on security measures. BetPawa Uganda improved from 33% to 50%, indicating increased attention to basic data protection controls, though gaps remain.

Despite these improvements, transparency and accountability mechanisms continue to be largely absent. None of the companies published transparency reports, and compliance with internal data breach detection and resolution mechanisms remains extremely low. BetPawa Uganda leads marginally at 17% (up from 0%), followed by 22Bet Uganda at 8% (up from 0%), while Fortebet and 1Xbet Uganda scored 0%. This persistent deficiency is particularly concerning given legal obligations related to breach notification, incident management, and accountability.

Overall, the year-on-year comparison demonstrates modest progress, particularly in regulatory registration, data subject rights, and limited aspects of third-party data sharing. However, these gains are outweighed by enduring weaknesses in regulatory compliance, breach preparedness, and transparency reporting. To meaningfully align with Uganda's data protection laws, companies will need to move beyond static policy disclosures and invest in robust governance structures, clearer third-party data controls, and effective incident response mechanisms. Without such reforms, user privacy remains insufficiently protected in a rapidly expanding digital betting market.

3.4.3.3 Comparison of companies/entities within the sector

A comparison of the companies' performance reveals a modest improvement at the top end, but overall confirms that privacy and data protection compliance remains weak and uneven. Average overall scores remain low, with no company exceeding 53%, indicating that even sector leaders are only partially compliant with core data protection principles.



High-Performing Jurisdictions(Emerging Compliance Leaders and Trajectories)

A small number of jurisdictions are beginning to demonstrate comparatively stronger alignment with data protection obligations, although none yet approach full compliance. Ghana and Kenya emerge as the leading jurisdictions based on average company performance. Betway Ghana (53%) and Betika Kenya (52%) top the sector, reflecting relatively stronger privacy governance frameworks, including clearer privacy disclosures, improved recognition of data subject rights, and more consistent security measures.

Compared to last year, both jurisdictions show upward trajectories. Ghanaian operators, including 1Xbet Ghana (47%) and Betpawa Ghana (41%), have improved from earlier mid-range scores, suggesting a gradually maturing compliance environment. Kenya shows the clearest internal differentiation: while Betika Kenya has progressed significantly from the mid-30% range last year, BetPawa Kenya (46%) has also improved from the low-20% range. These gains point to increased regulatory engagement and growing awareness of data protection requirements, though compliance remains partial and uneven.

Despite these improvements, even the strongest performers remain below 60%, indicating that progress is incremental rather than transformative. High-performing jurisdictions still struggle with accountability-driven obligations such as third-party data governance, breach preparedness, and transparency reporting.

Mid-Range Performers (Partial Compliance and Structural Gaps,Change Over Time)

The majority of jurisdictions fall within a mid-range performance band, typically scoring between 40% and 47%. This group includes Uganda, Zimbabwe, Tanzania, Rwanda, Botswana, and parts of Mauritius. Companies such as 22Bet Uganda (47%), Pinnacle Sports Zimbabwe (45%), William Hill Mauritius (44%), SportPesa Botswana (44%), Gorilla Games Rwanda (43%), and SportPesa Tanzania (40%) illustrate partial compliance with core data protection principles.

Year-on-year comparisons show modest improvement in several cases. Uganda, for example, has seen 22Bet Uganda rise from the high-20% range to 47%, reflecting gains in regulatory registration and data subject rights. Similarly, some Tanzanian and Rwandan operators have consolidated earlier improvements, maintaining scores around 40–43%. Zimbabwe's leading operators have also improved slightly compared to last year, though progress remains slow.

However, structural gaps persist across this group. Improvements tend to be concentrated in easily observable measures such as privacy policy publication and basic security safeguards. More complex obligations, particularly transparency around third-party data sharing, internal breach response mechanisms, and public accountability remain underdeveloped. As a result, compliance gains have plateaued, with many companies showing limited year-

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

At the lower end of the spectrum are jurisdictions and operators exhibiting systemic compliance failures. Several companies in Mauritius (Stevenhills Mauritius and Totelepep Ltd at 6%) and Botswana (BetXplosion at 6%) remain effectively non-compliant, showing little or no improvement from last year. Similarly, operators such as 1Xbet Uganda (26%), Bikosports Tanzania (28%), Accessbet Nigeria (28%), and PstBet Botswana (30%) continue to score well below acceptable thresholds.

In some cases, regression is evident. Companies that previously demonstrated moderate performance have stagnated or declined, indicating weak institutionalisation of privacy practices. These consistently low scores reflect the absence of fundamental compliance structures, including regulatory registration, meaningful data subject rights mechanisms, security governance, and breach response processes. In such environments, privacy compliance appears reactive or symbolic rather than embedded in operational practice.

Key Cross-Cutting Implications

Across all jurisdictions, several consistent patterns emerge. First, no company exceeds 53%, underscoring that sector-wide compliance with data protection laws remains superficial. Privacy policies are widely present, but their existence is not matched by robust implementation or accountability.

Second, improvements over time are uneven and often concentrated in low-cost, highly visible measures. High-risk obligations, such as third-party data sharing controls, internal breach resolution mechanisms, and transparency reporting, remain the weakest areas across all performance tiers. These gaps significantly increase legal, regulatory, and reputational risks for companies operating in the sector.

Third, jurisdictional context matters, but it is not determinative. Even in stronger regulatory environments, companies within the same country exhibit divergent performance, suggesting that corporate governance and internal commitment play a decisive role in compliance outcomes.

Overall, the findings indicate that while incremental progress is occurring, the online betting sector has yet to internalise data protection as a core governance and risk-management function. Without stronger regulatory enforcement and deeper operational reforms, improvements are likely to remain fragmented, leaving user data inadequately protected across much of the sector.

3.4.4 Banks and Finance Sector Analysis

3.4.4.1 Overview of the sector and data collectors evaluated

The banking and finance sector remains a cornerstone of economic activity, underpinning access to savings, credit, payments, and investment services. Given the volume and sensitivity of personal and financial data processed by banks and other financial institutions, effective compliance with data protection laws and robust data security practices are fundamental. The sector therefore carries a heightened responsibility to safeguard customer information against misuse, unauthorized access, and data breaches, particularly as financial services become increasingly digitised.

In East Africa, countries such as Uganda, Kenya, and Tanzania host relatively mature banking ecosystems comprising both domestic and multinational institutions. Kenya continues to stand out for its leadership in digital and mobile financial services most notably through platforms such as M-Pesa which have significantly expanded financial inclusion while simultaneously increasing the scale and complexity of personal data processing. Rwanda's banking sector has also expanded rapidly in recent years, supported by regulatory reforms and state-led digitalisation efforts aimed at modernising financial services. Mauritius maintains its position as a regional financial hub, with a well-established and internationally oriented banking sector that attracts cross-border investment and operates within a comparatively structured regulatory environment.

The inclusion of Nigeria and Ghana broadens the assessment to West Africa's largest and most dynamic financial markets. Nigeria's banking sector is among the most developed on the continent, characterised by large, technology-driven institutions with extensive digital banking platforms and regional footprints. Ghana similarly hosts a growing and competitive financial services sector, supported by regulatory reforms and increased adoption of digital banking and payment systems.

Botswana adds a Southern African perspective marked by a relatively stable financial system and a strong presence of regional and international banks operating under evolving data protection frameworks.

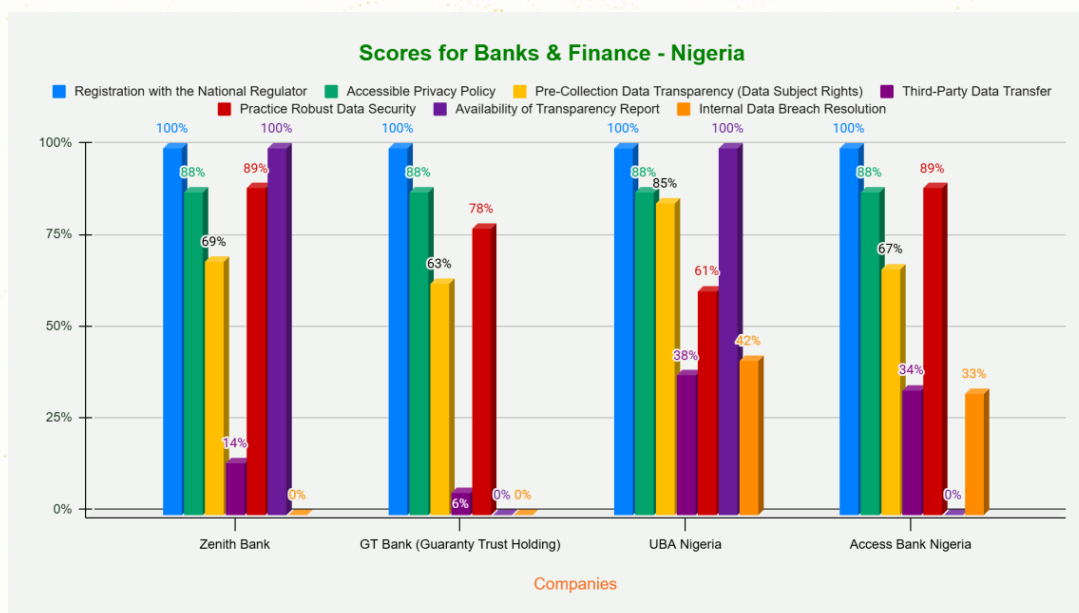
Zimbabwe's banking sector continues to operate under challenging economic conditions, including currency volatility and constrained consumer confidence. Despite these pressures, financial institutions remain central to domestic and cross-border financial transactions, making the protection of personal and financial data especially critical in a fragile operating environment.

Across all assessed countries, the banking and finance sector is increasingly prioritising digital service delivery, regulatory compliance, and data governance as core components of consumer trust and market stability. This evaluation examines a cross-section of banks and financial institutions, focusing on transparency, regulatory adherence, and the strength of privacy and data protection practices. In the context of an increasingly data-driven financial ecosystem, the findings provide insight into how effectively institutions are protecting customer privacy, where progress has been made, and where further reforms are necessary to align practices with national data protection laws and evolving global standards.

3.4.4.2 Analysis of compliance with each criterion

The assessment for this sector draws on data from a total of 36 companies, with four (4) companies selected from each participating country. These included: Zenith Bank, GT Bank (Guaranty Trust Holding), UBA Nigeria and Access Bank Nigeria from Nigeria; Eco Bank Ghana, GCB Ghana, Stanbic Ghana and ABSA Ghana from Ghana; First national Bank, Absa Botswana, Stanbic Bank Botswana and Standard Chartered Bank from Botswana from Botswana; Bank of Kigali, Access Bank Rwanda, Equity Bank Rwanda and Ecobank Rwanda from Rwanda; NMB Bank, Equity Bank Tanzania, Stanbic Bank Tanzania and NBC Bank Tanzania from Tanzania; ABSA Bank Mauritius, Swan Life Limited, SBM Bank (Mauritius) Limited and Bank of Baroda Mauritius from Mauritius; Empower Bank, CBZ Bank, Stanbic Bank Zimbabwe and NMB Bank from Zimbabwe; Stima Sacco, Equity Bank Kenya, ABSA Kenya and KCB Bank from Kenya and; Stanbic Bank Uganda, Pride microfinance, ABSA Bank Uganda and Centenary Bank from Uganda.

a. Zenith Bank, GT Bank (Guaranty Trust Holding), UBA Nigeria and Access Bank Nigeria from Nigeria



All assessed banks demonstrated full compliance with registration requirements under the national data protection regulator, each attaining a perfect score (100%). This reflects a strong baseline commitment to formal regulatory compliance and provides an important foundation for lawful personal data processing. In addition, all institutions showed considerable effort in making their privacy policies accessible, with each scoring 88%. While this indicates a shared recognition of transparency obligations, accessibility alone does not necessarily translate into comprehensive or user-friendly disclosure of data practices.

With respect to data subject rights, performance varied more noticeably across the banks. UBA Nigeria emerged as the strongest performer (85%), suggesting relatively clearer mechanisms for enabling customer rights such as access, correction, and deletion of personal data. Zenith Bank (69%), Access Bank Nigeria (67%), and GT Bank (63%) followed, indicating moderate but uneven implementation of rights-based safeguards. These results imply that, although awareness of data subject rights exists across the sector, their practical enforcement remains inconsistent, potentially limiting customers' ability to exercise rights guaranteed under data protection laws.

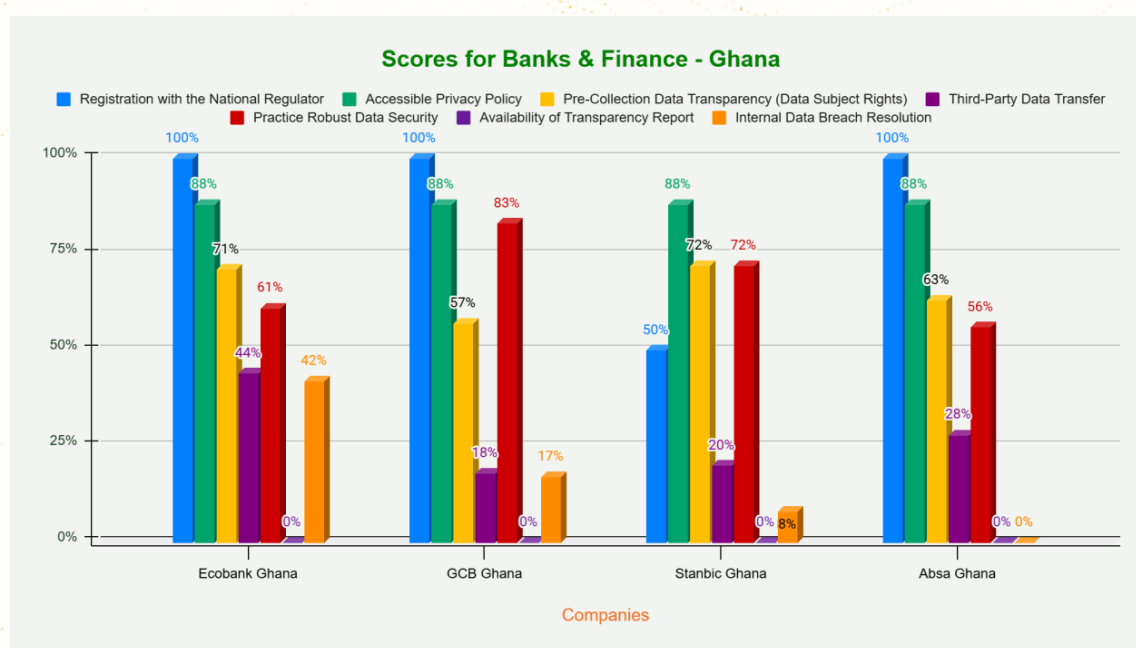
All banks were found to share personal data with third parties, a common practice in the financial sector given outsourcing, partnerships, and regulatory reporting obligations. However, compliance in this area was notably weak. UBA Nigeria, despite leading, achieved only 38%, followed by Access Bank Nigeria (34%), Zenith Bank (14%), and GT Bank (6%). These low scores point to insufficient transparency around the scope, purpose, and safeguards governing third-party data transfers, raising concerns about accountability and lawful processing, particularly where cross-border data flows may be involved.

In contrast, data security emerged as a relative strength. Zenith Bank and Access Bank Nigeria both scored highly (89%), reflecting robust technical and organizational measures to protect personal and financial data. GT Bank also performed well (78%), while UBA Nigeria lagged comparatively at 61%. Strong security controls are critical for the banking sector, and these results suggest that most institutions prioritize protection against unauthorized access and breaches, even where other aspects of compliance are weaker.

Transparency reporting and breach governance, however, remain significant gaps. Only Zenith Bank and UBA Nigeria had published transparency reports, indicating limited sector-wide commitment to proactive accountability and public disclosure of data handling practices. Moreover, all banks showed very low compliance with internal data breach resolution mechanisms. UBA Nigeria led with 42%, followed by Access Bank Nigeria at 33%, while the remaining banks scored 0%. This suggests that, despite strong security measures, most institutions lack clear, documented procedures for detecting, managing, and notifying stakeholders of data breaches, a core requirement under data protection laws.

Overall, the findings indicate that while Nigerian banks perform strongly in regulatory registration, privacy policy accessibility, and data security, substantial compliance gaps persist in third-party data sharing, breach response, and accountability mechanisms. These weaknesses expose institutions to regulatory risk and may undermine customer trust. Strengthening internal breach management frameworks, improving transparency around data sharing, and operationalizing data subject rights are essential steps for aligning sector practices with both national data protection laws and emerging global standards.

b. *Eco Bank Ghana, GCB Ghana, Stanbic Ghana and ABSA Ghana from Ghana*



All assessed banks demonstrated compliance with registration requirements under the national data protection regulator, with Ecobank Ghana, GCB Ghana, and Absa Ghana achieving perfect scores (100%). This indicates strong formal adherence to statutory registration obligations and reflects a baseline level of institutional awareness of data protection laws. Stanbic Ghana, however, scored 50%, suggesting partial compliance and a need to strengthen alignment with regulatory requirements to ensure lawful data processing.

Similarly, all institutions showed consistent effort in making their privacy policies accessible, each scoring 88%. This points to a shared commitment to transparency at the policy level and ensures that customers can at least locate information about how their personal data is handled. Nevertheless, accessibility alone does not guarantee that privacy notices are sufficiently detailed, clear, or comprehensive to meet substantive legal standards.

In terms of data subject rights, performance was more differentiated. Stanbic Ghana led with a score of 72%, closely followed by Ecobank Ghana (71%), indicating relatively stronger mechanisms for enabling rights such as access, correction, and objection. Absa Ghana (63%) and GCB Ghana (57%) demonstrated moderate compliance, suggesting that while rights are acknowledged, their practical implementation may be limited or uneven. These variations highlight differing levels of maturity in translating legal rights into operational processes that customers can easily exercise.

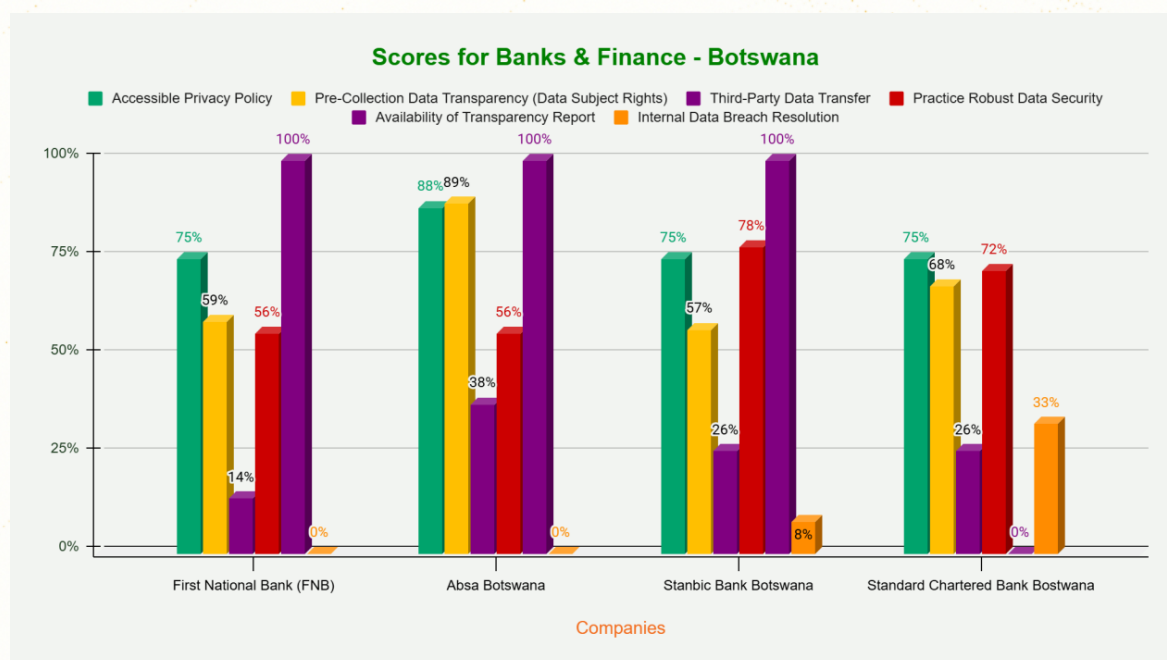
All banks were found to share personal data with third parties, which is typical in the banking sector due to service outsourcing and regulatory obligations. However, compliance in this area was notably weak across the board. Ecobank Ghana, despite leading, achieved only 44%, followed by Absa Ghana (28%), Stanbic Ghana (20%), and GCB Ghana (18%). These low scores indicate insufficient transparency and safeguards around third-party data sharing, raising concerns about accountability, purpose limitation, and potential risks to customer data, particularly where onward transfers are involved.

Overall, the findings suggest that while Ghanaian banks perform relatively well in regulatory registration and policy-level transparency, significant gaps remain in third-party data governance and the consistent operationalization of data subject rights. Addressing these weaknesses through clearer disclosures, stronger contractual controls with third parties, and more user-friendly rights-request mechanisms will be essential for achieving fuller compliance with Ghana's data protection framework and reinforcing customer trust in the sector.

c. *First national Bank (FNB), Absa Botswana, Stanbic Bank Botswana and Standard Chartered Bank from Botswana*

The assessment indicates that Botswana's banks have made demonstrable efforts to establish accessible privacy policies, suggesting an acknowledgment of their obligations under data protection and privacy principles. Absa Botswana performed strongest in this area, scoring 88%, while First National Bank, Stanbic Bank Botswana, and Standard Chartered Bank Botswana each achieved 75%. This reflects a generally positive baseline commitment to transparency, although accessibility alone does not guarantee substantive compliance.

In relation to the observance of data subject rights, performance was mixed. Absa Botswana again led with a high score of 89%, indicating comparatively stronger alignment with core data protection requirements such as access, correction, and consent. Standard Chartered Bank Botswana followed at 68%, while First National Bank (59%) and Stanbic Bank Botswana (57%) recorded moderate compliance. These results suggest that, although mechanisms to uphold data subject rights exist, their implementation may be uneven and, in some cases, insufficiently robust.



All assessed banks disclosed that they share personal data with third parties; however, compliance in this area was notably weak. Even the highest-performing institution, Absa Botswana, scored only 38%, while Stanbic Bank Botswana and Standard Chartered Bank Botswana each scored 26%, and First National Bank lagged significantly at 14%. This raises concerns regarding transparency, lawful basis, and safeguards surrounding third-party data sharing, which are critical elements of data protection laws and pose heightened risks to customer privacy.

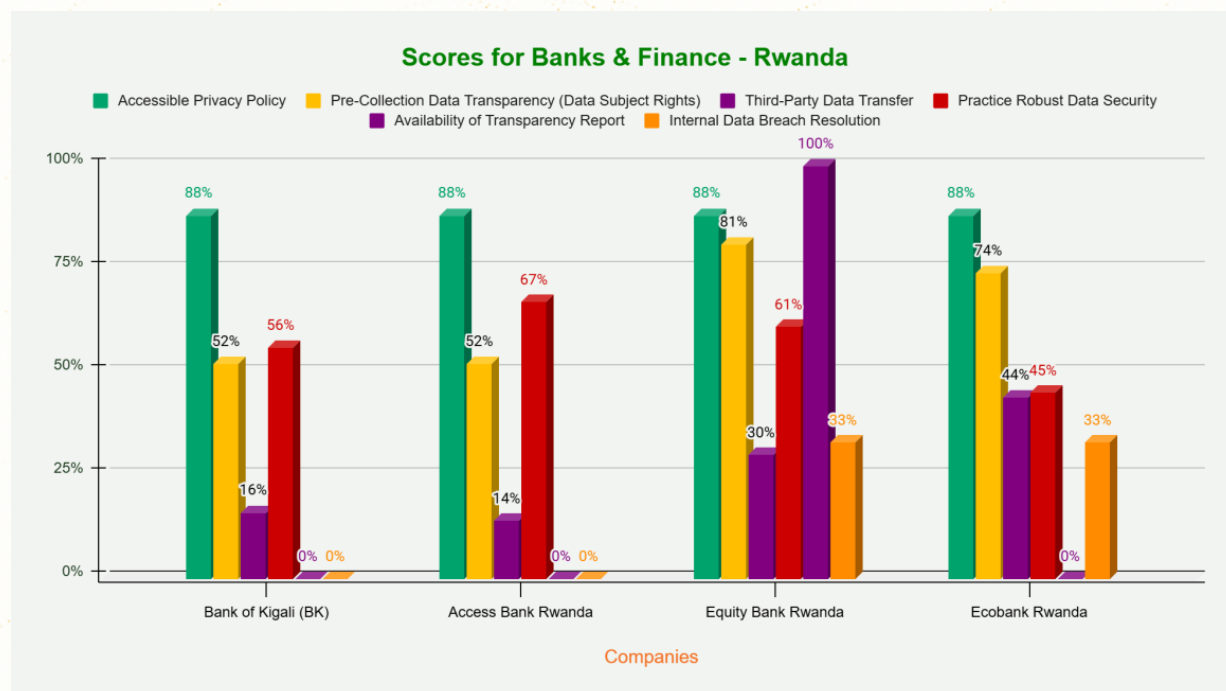
With respect to data security measures, the banks demonstrated stronger performance overall. Stanbic Bank Botswana led with a score of 78%, followed by Standard Chartered Bank Botswana at 72%. First National Bank and Absa Botswana both scored 56%, indicating moderate but potentially inadequate protection against data breaches and unauthorized access. While these results suggest awareness of security obligations, they also highlight the need for continuous improvement in technical and organizational safeguards.

Transparency reporting emerged as a major area of weakness. Only First National Bank, Absa Botswana, and Stanbic Bank Botswana published transparency reports, and even then, compliance levels were extremely low in respect of internal data breach resolution mechanisms. Standard Chartered Bank Botswana led marginally with 33%, followed by Stanbic Bank Botswana at 8%, while First National Bank and Absa Botswana scored each 0%. This lack of meaningful transparency undermines accountability and limits public trust, particularly in relation to government requests, data sharing practices, and internal compliance oversight.

Overall, the findings indicate that while Botswana's banks show awareness of privacy obligations and have taken initial steps toward compliance, significant gaps remain. Weaknesses in third-party data sharing practices and transparency reporting suggest partial rather than comprehensive compliance with data protection laws. To strengthen privacy governance and legal compliance, the banks must move beyond policy availability and invest in enforceable practices, clearer disclosures, and stronger accountability mechanisms across all aspects of personal data processing.

d. *Bank of Kigali, Access Bank Rwanda, Equity Bank Rwanda and Ecobank Rwanda in Rwanda*

Overall, the current assessment shows incremental but uneven progress in privacy practices among Rwandan banks when compared to last year. While foundational elements such as privacy policy availability and data security remain relatively strong and stable, critical accountability mechanisms particularly third-party data transfers, transparency reporting, and internal data breach resolution continue to exhibit persistent weaknesses, raising concerns about full compliance with data protection laws.



All four assessed banks (Bank of Kigali, Access Bank Rwanda, Equity Bank Rwanda, and Ecobank Rwanda) have made demonstrable efforts to maintain accessible and publicly available privacy policies, with each institution scoring 88%, reflecting parity across the sector. This represents no change from last year for Bank of Kigali, Equity Bank Rwanda, and Ecobank Rwanda, while Access Bank Rwanda improved from 75% to 88%, indicating progress in policy publication and visibility.

All policies exceed 200 words and are easily noticeable on bank websites, ensuring a baseline level of transparency. However, readability remains a concern. With readability grades ranging from 12 to 13, the policies may be difficult for the average user to fully understand, potentially undermining meaningful transparency. Word counts vary substantially from 1,905 words at Access Bank Rwanda to 5,766 words at Equity Bank Rwanda suggesting comprehensive coverage but at the cost of clarity. Consequently, while policy availability strongly supports formal compliance with data protection requirements, linguistic complexity continues to limit effective user comprehension.

The banks demonstrate notable improvement in the observance of data subject rights compared to last year, indicating growing awareness of legal obligations under data protection frameworks. Equity Bank Rwanda leads with a score of 81%, a substantial increase from 57% last year, reflecting enhanced disclosure of collected data types, retention practices, third-party sharing, and recognition of user rights, including complaint mechanisms. Ecobank Rwanda follows with 74%, up from 41%, reflecting clearer articulation of collection purposes, supported rights, and limitations on third-party sharing, though gaps remain in contact disclosure and precise retention periods.

Bank of Kigali and Access Bank Rwanda both scored 52%. Bank of Kigali improved from 41%, while Access Bank declined from 57%, suggesting stagnation or regression in transparency efforts. Both banks demonstrate moderate compliance by outlining collection purposes, general categories of personal data, and basic user rights, but they continue to omit explicit contact details, detailed retention timelines, and clear complaint procedures. Access Bank Rwanda additionally lacks clarity on law enforcement access. While the upward trend indicates progress toward compliance, persistent gaps in complaint mechanisms, retention specificity, and contact transparency limit users' ability to effectively exercise their rights, weakening accountability.

All assessed banks continue to share personal data with third parties, but compliance levels remain low, despite modest year-on-year improvements.

This area remains one of the most significant compliance risks under data protection laws. Ecobank Rwanda leads with 44%, improving from 34%, followed by Equity Bank Rwanda at 30% (up from 10%). Access Bank Rwanda scored 14%, and Bank of Kigali 16%, both improving slightly from 10% last year. Despite these gains, disclosures remain incomplete across the sector. Most banks fail to specify all third-party entities, exact categories of shared data, conditions for law enforcement access, or comprehensive breach-reporting mechanisms. These deficiencies suggest partial compliance at best and expose customers to heightened privacy risks due to limited oversight and transparency in data-sharing arrangements.

Data security practices remain largely consistent with last year's findings, indicating stability but limited advancement. Access Bank Rwanda again leads with 67%, followed by Equity Bank Rwanda at 61%, and Bank of Kigali maintaining 56%. Ecobank Rwanda scored 45%, reflecting mixed technical performance. While most banks demonstrate strong SSL ratings and reference organizational, technical, and physical safeguards, policies generally lack detailed explanations of specific security measures. This limits the ability of users and regulators to assess whether protections meet legal standards for adequacy and proportionality. The results suggest that while banks recognize their duty to safeguard personal data, transparency around implementation remains insufficient.

Transparency reporting remains a critical weakness. Only Equity Bank Rwanda has published a transparency report since 2024. Bank of Kigali, Access Bank Rwanda, and Ecobank Rwanda have not issued any transparency reports, mirroring last year's findings. The continued absence of transparency reports undermines public accountability, particularly regarding government data requests, third-party disclosures, and internal compliance oversight. This persistent gap reflects limited alignment with international best practices in privacy governance.

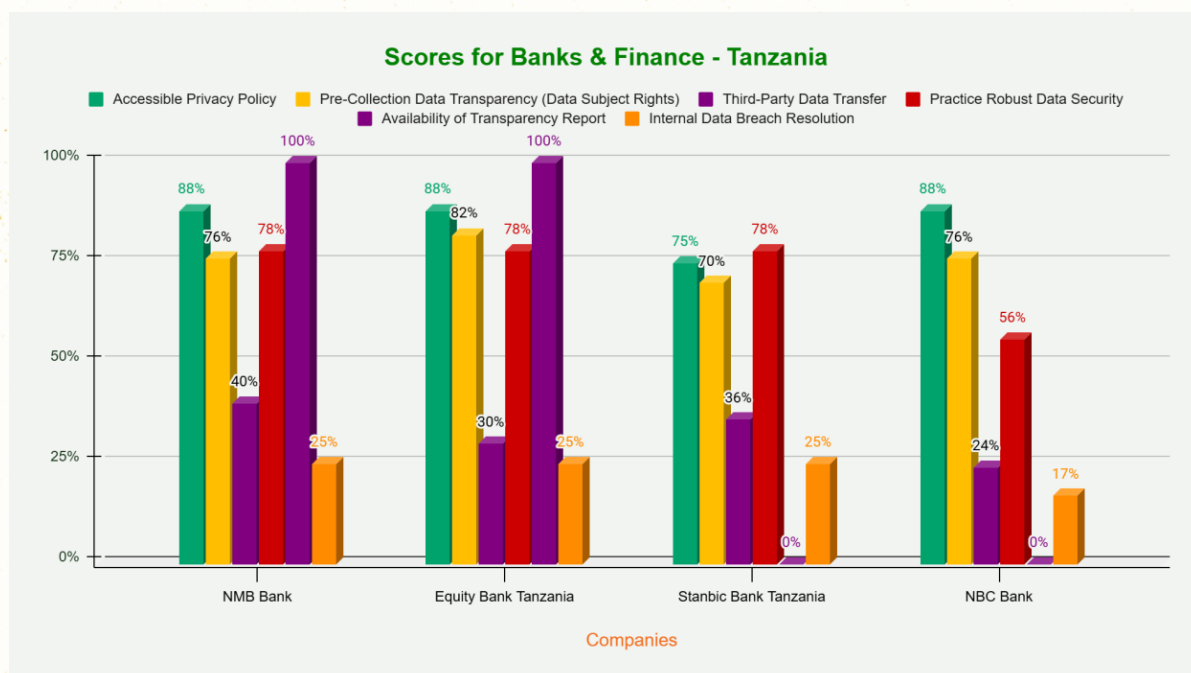
Internal data breach resolution remains largely unchanged and inadequate, signaling ongoing non-compliance with core data protection principles related to accountability and user protection. Bank of Kigali and Access Bank Rwanda each scored 0%, as their policies provide no meaningful guidance on breach identification, investigation, resolution, user notification, or reporting channels unchanged from last year. Equity Bank Rwanda and Ecobank Rwanda show partial improvement, each scoring 33%, by acknowledging breach handling procedures and providing limited reporting channels. However, both lack detailed internal processes, clear timelines, and guarantees of fair and impartial investigations.

The continued weakness in breach response frameworks represents a significant compliance risk, particularly given statutory obligations to notify regulators and affected individuals within defined timeframes.

Compared to last year, the current analysis reveals incremental progress in transparency and data subject rights, particularly by Equity Bank Rwanda and Ecobank Rwanda. However, improvements remain largely procedural rather than structural. Persistent deficiencies in third-party data governance, transparency reporting, and breach management indicate that compliance with data protection laws remains partial and uneven across the sector. To achieve stronger compliance and build public trust, Rwandan banks must move beyond policy availability and baseline security measures toward clearer disclosures, enforceable internal procedures, and robust accountability mechanisms, particularly in areas involving third-party data sharing and breach response.

e. *NMB Bank, Equity Bank Tanzania, Stanbic Bank Tanzania and NBC Bank Tanzania in Tanzania*

The current assessment of Tanzanian banks indicates measured progress in several areas of privacy governance, particularly in data subject rights, data security, and limited accountability mechanisms, when compared to last year's findings. However, despite these improvements, systemic weaknesses persist, especially in third-party data transfers and internal data breach resolution, which continue to undermine full compliance with data protection laws.



All assessed banks continue to demonstrate strong performance in the accessibility of their privacy policies, reflecting stability and sustained commitment in this foundational area. NMB Bank, Equity Bank Tanzania, and NBC Bank Tanzania each maintained a score of 88%, consistent with last year's results, while Stanbic Bank Tanzania again scored 75%. This consistency indicates that the banks' privacy policies remain publicly available, easily noticeable on their websites, and written in fairly readable language, as confirmed by favorable readability grades using the Hemingway Editor. From a compliance perspective, this supports baseline transparency requirements under data protection laws. However, as in previous assessments, accessibility does not necessarily translate into substantive compliance across all privacy obligations.

The observance of data subject rights shows clear improvement overall, suggesting increasing awareness of statutory obligations relating to lawful processing, transparency, and user control. Equity Bank Tanzania leads with a score of 82%, up from 78% last year, although it still falls short by permitting data sharing with third-party advertisers without providing a comprehensive list of those entities. NMB Bank and NBC Bank Tanzania each scored 76%. Notably, NMB Bank recorded a substantial improvement from 38% last year, while NBC Bank maintained its previous performance level. These results reflect stronger disclosures regarding purposes of data collection, categories of personal data processed, and recognition of key data subject rights. Nevertheless, gaps in advertiser transparency and consent mechanisms limit full compliance and expose users to uncertainty regarding how their personal data is further processed.

Despite modest improvements, third-party data sharing remains one of the weakest areas across the sector and continues to pose significant compliance risks. All assessed banks share personal data with third parties but demonstrate very low levels of compliance. NMB Bank leads with 40%, a notable increase from 10% last year, followed by Equity Bank Tanzania at 30% (up from 10%). NBC Bank Tanzania maintained a low score of 24%, showing no improvement since the previous assessment. The continued lack of detailed disclosure regarding third-party recipients, specific categories of shared data, consent mechanisms, and lawful bases for transfer constitutes a violation of core data protection principles. These deficiencies undermine data subject rights and weaken the duties of data controllers and processors to ensure lawful and fair data sharing.

Data security practices show mixed but generally positive trends when compared to last year. NMB Bank, Stanbic Bank Tanzania, and Equity Bank Tanzania each scored 78%. For NMB Bank, this reflects an improvement from 72%, while Stanbic Bank maintained its previous strong performance and Equity Bank Tanzania improved from 61%. In contrast, NBC Bank Tanzania scored 56%, representing a decline from 72% last year.

These results suggest that most banks have strengthened or maintained technical and organizational security measures such as encryption, secure transmission, and access controls. However, the decline at NBC Bank Tanzania raises concerns about the sustainability of data security practices and highlights the need for continuous monitoring and investment to meet legal standards for data protection.

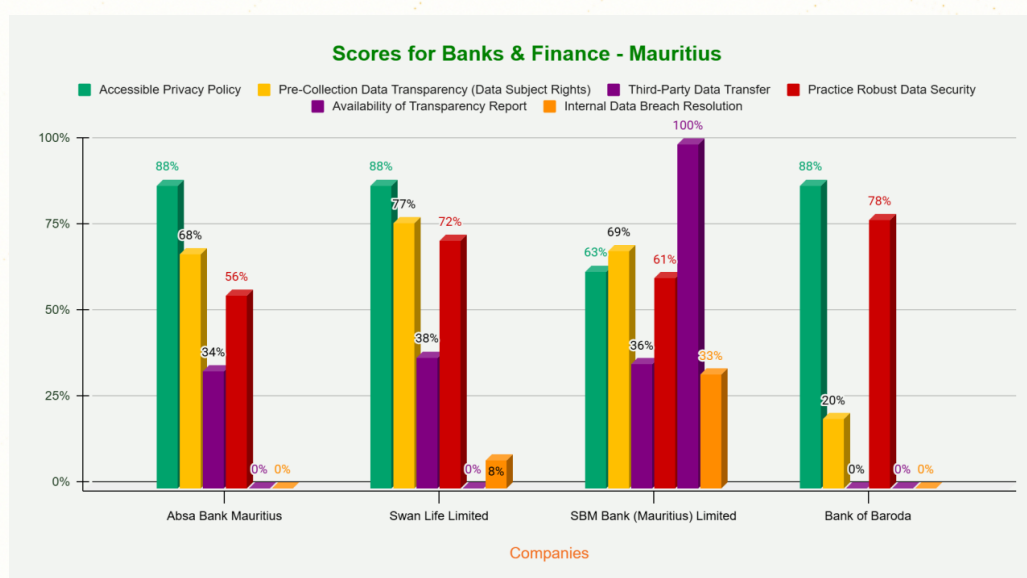
Accountability through transparency reporting has improved slightly but remains uneven across the sector. Only NMB Bank and Equity Bank Tanzania have published transparency reports on their websites, each achieving a 100% score under this metric. This marks a significant improvement from last year, when none of the assessed banks had published transparency reports. Stanbic Bank Tanzania and NBC Bank Tanzania continue to lack transparency reports, limiting public insight into government data requests, third-party disclosures, and internal oversight mechanisms.

Internal data breach resolution remains a critical area of weakness, despite marginal improvements across all institutions. All banks recorded very low compliance levels. NMB Bank, Equity Bank Tanzania, and Stanbic Bank Tanzania each scored 25%, while NBC Bank Tanzania scored 17%. Although these scores are low, they represent an improvement from 0% across all banks last year, indicating early recognition of the need for breach response mechanisms. Nonetheless, the absence of clear internal procedures, defined reporting timelines, guaranteed user notification, and accessible reporting channels suggests that banks may struggle to detect, report, and remedy data breaches in a timely and lawful manner, as required under data protection laws.

Compared to last year, the Tanzanian banking sector demonstrates incremental progress in privacy governance, particularly in data subject rights, data security, and limited transparency reporting. However, improvements remain uneven and largely procedural. Persistent shortcomings in third-party data transfers and internal data breach resolution indicate that full compliance with data protection laws has not yet been achieved. To strengthen privacy practices and regulatory alignment, banks must move beyond accessible policies and technical safeguards toward comprehensive accountability frameworks, including lawful data-sharing controls, effective breach management systems, and consistent transparency reporting.

f. ABSA Bank Mauritius, Swan Life Limited, SBM Bank (Mauritius) Limited and Bank of Baroda Mauritius in Mauritius

The current assessment of banks and financial institutions in Mauritius reflects a mixed trajectory in privacy governance when compared with last year's findings. While strong performance in the accessibility of privacy policies has largely been sustained, progress in other critical areas particularly third-party data transfers, transparency reporting, and internal data breach resolution remains uneven and, in some cases, has deteriorated. These patterns have direct implications for compliance with Mauritius' data protection framework and for institutional accountability.



All assessed institutions (Absa Bank Mauritius, Swan Life Limited, SBM Bank, and Bank of Baroda) continue to demonstrate effort in maintaining accessible privacy policies. Absa Bank Mauritius, Swan Life Limited, and Bank of Baroda each maintained a high score of 88%, consistent with last year's results, indicating sustained compliance with baseline transparency obligations. In contrast, SBM Bank's score declined to 63% from 75% last year, suggesting reduced accessibility or clarity of its published privacy information. While overall policy availability remains strong across the sector, this decline highlights the need for consistent maintenance and updating of privacy disclosures to meet legal transparency standards.

Observance of data subject rights shows both improvement and regression across institutions, resulting in an uneven compliance landscape. Swan Life Limited leads with a score of 77%, improving from 66% last year, reflecting stronger disclosure of lawful processing bases, clearer articulation of user rights, and improved complaint mechanisms.

SBM Bank also demonstrated notable progress, scoring 69%, up from 52%, positioning it as one of the stronger performers in this category. Absa Bank Mauritius recorded a slight decline to 68% from 71%, while Bank of Baroda scored 20%, down from 25%, indicating persistent weaknesses in rights recognition and user redress mechanisms. These findings suggest that while some institutions are strengthening alignment with data protection principles such as lawfulness, fairness, and transparency, others risk non-compliance by failing to adequately inform users of their rights or provide effective means of exercising them.

All assessed institutions share personal data with third parties; however, compliance levels remain low, despite incremental improvements by some banks. Swan Life Limited leads with 38%, improving from 24%, followed closely by SBM Bank at 36%, also up from 24%. Absa Bank Mauritius improved to 34% from 14%, reflecting better disclosure and safeguards, though still below acceptable compliance thresholds. Bank of Baroda again scored 0%, unchanged from last year, indicating a complete lack of transparency or safeguards around third-party data sharing. The continued inadequacy in this area poses significant compliance risks, as data protection laws require clear disclosure of third-party recipients, lawful bases for sharing, and appropriate safeguards. Weak performance undermines data subject trust and increases regulatory exposure.

Performance in data security reflects stagnation and regression, rather than consistent improvement. Bank of Baroda again leads with a score of 78%, maintaining its performance from last year. Swan Life Limited maintained 72%, indicating stable implementation of technical and organizational safeguards. In contrast, SBM Bank's score declined to 61% from 72%, and Absa Bank Mauritius fell to 56% from 72%, raising concerns about the adequacy and consistency of their security practices. These declines suggest that while some institutions maintain robust safeguards, others may not be sufficiently updating or documenting security measures to meet evolving legal and operational risks.

Transparency reporting remains a major area of divergence across the sector.

All institutions except SBM Bank lack transparency reports. SBM Bank scored 100%, a significant improvement from 0% last year, demonstrating enhanced accountability regarding data disclosures and oversight. Absa Bank Mauritius, Swan Life Limited, and Bank of Baroda continue to provide no transparency reports, mirroring last year's shortcomings and limiting public insight into data access requests and disclosure practices.

Internal data breach resolution remains critically underdeveloped across the sector. All institutions registered very low compliance levels. Swan Life Limited scored 8%, while Absa Bank Mauritius, SBM Bank, and Bank of Baroda each scored 0%, showing no improvement from last year. The absence of clear internal procedures, reporting timelines, and guaranteed user notification mechanisms indicates weak accountability and exposes institutions to legal and reputational risks in the event of a data breach.

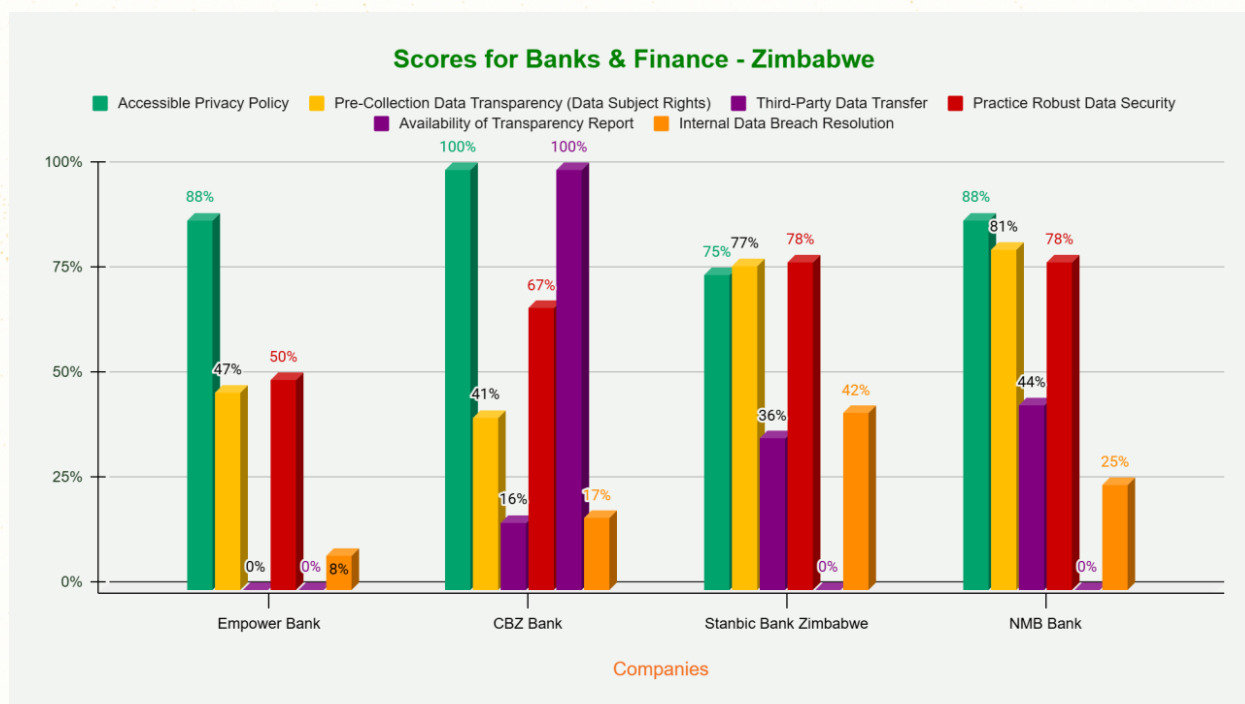
A closer review of policy content reinforces these findings. Absa Bank's policy is comprehensive in scope, clearly defining data categories, processing purposes, lawful bases, and data subject rights, including complaint mechanisms, although its slight decline in scores suggests potential gaps in implementation or clarity. Swan Life Limited's policy is detailed and rights-forward, particularly regarding consent, cross-border transfers, and protections against automated decision-making. SBM Bank's policy demonstrates strong safeguards and clearly articulated user rights, supported by full Data Protection Officer contact details, aligning well with legal requirements. By contrast, Bank of Baroda's policy lacks essential elements such as contact details, complaint mechanisms, and consent withdrawal rights, contributing to its persistently low performance in key compliance areas.

Compared to last year, the Mauritian banking sector shows selective progress rather than systemic improvement. Gains in data subject rights and transparency reporting by certain institutions are offset by declines in data security and persistent weaknesses in third-party data sharing and breach management. While most institutions meet baseline transparency requirements through accessible privacy policies, full compliance with data protection laws remains uneven. To strengthen privacy governance, banks must prioritize robust third-party data controls, comprehensive breach response frameworks, and consistent transparency reporting to enhance accountability, regulatory compliance, and customer trust.

g. *Empower Bank, CBZ Bank, Stanbic Bank Zimbabwe and NMB Bank in Zimbabwe*

The current assessment of Zimbabwean banks shows measurable improvement in several areas of privacy governance compared to last year, while also revealing persistent structural weaknesses that continue to limit full compliance with data protection laws. Overall, banks demonstrate growing awareness of privacy obligations, but accountability mechanisms remain underdeveloped.

As was the case last year, all assessed banks continue to demonstrate strong performance in the accessibility of their privacy policies. CBZ Bank again leads with a perfect score of 100%, while Empower Bank and NMB Bank each maintained scores of 88%, and Stanbic Bank Zimbabwe maintained 75%. This consistency indicates that privacy policies remain publicly available, visible on institutional websites, and generally readable. From a compliance perspective, this satisfies baseline transparency requirements under data protection laws. However, as in previous assessments, policy accessibility alone does not ensure substantive compliance across other dimensions of data protection.



The observance of data subject rights shows significant improvement across all institutions, representing one of the most notable areas of progress since last year. NMB Bank leads with 81%, a substantial increase from 36%, indicating enhanced disclosure of processing purposes and stronger recognition of user rights. Stanbic Bank Zimbabwe follows with 77%, improving from 72%, while Empower Bank scored 47%, up from 37%, and CBZ Bank scored 41%, up from 36%. These improvements suggest increasing alignment with legal requirements relating to lawful processing, transparency, and user control. Nevertheless, moderate-to-low scores for some institutions indicate that gaps remain in areas such as complaint mechanisms, detailed retention practices, and clarity of consent withdrawal procedures.

Despite modest gains, third-party data sharing remains a critical area of weakness, with all banks recording low compliance levels. NMB Bank leads with 44%, up from 24%, followed by Stanbic Bank Zimbabwe at 36%, a notable increase from 10%. CBZ Bank scored 16%, reflecting a decline from 24%, while Empower Bank maintained a score of 0%, unchanged from last year. These results indicate that although some institutions have improved disclosure and safeguards, third-party data transfers continue to fall short of data protection standards. Insufficient transparency around third-party recipients, data categories shared, and lawful bases for transfer undermines data subject rights and exposes banks to regulatory and reputational risk.

Data security practices remain relatively strong overall, though performance is uneven compared to last year. Stanbic Bank Zimbabwe and NMB Bank jointly lead with 78%. Stanbic Bank maintained its score, while NMB Bank improved from 72%.

CBZ Bank maintained a stable score of 67%, indicating consistency in security practices. In contrast, Empower Bank's score declined to 50% from 78%, raising concerns about the sustainability or documentation of its technical and organizational safeguards. These findings suggest that while most banks recognise their obligation to protect personal data, continuous investment and transparency around security measures are necessary to ensure ongoing compliance.

Transparency reporting remains largely unchanged and limited. As in last year's assessment, CBZ Bank is the only institution with a transparency report, maintaining a perfect score of 100%. NMB Bank, Stanbic Bank Zimbabwe, and Empower Bank continue to publish no transparency reports. The absence of transparency reports restricts public and regulatory insight into data access requests, third-party disclosures, and internal oversight, weakening accountability across the sector.

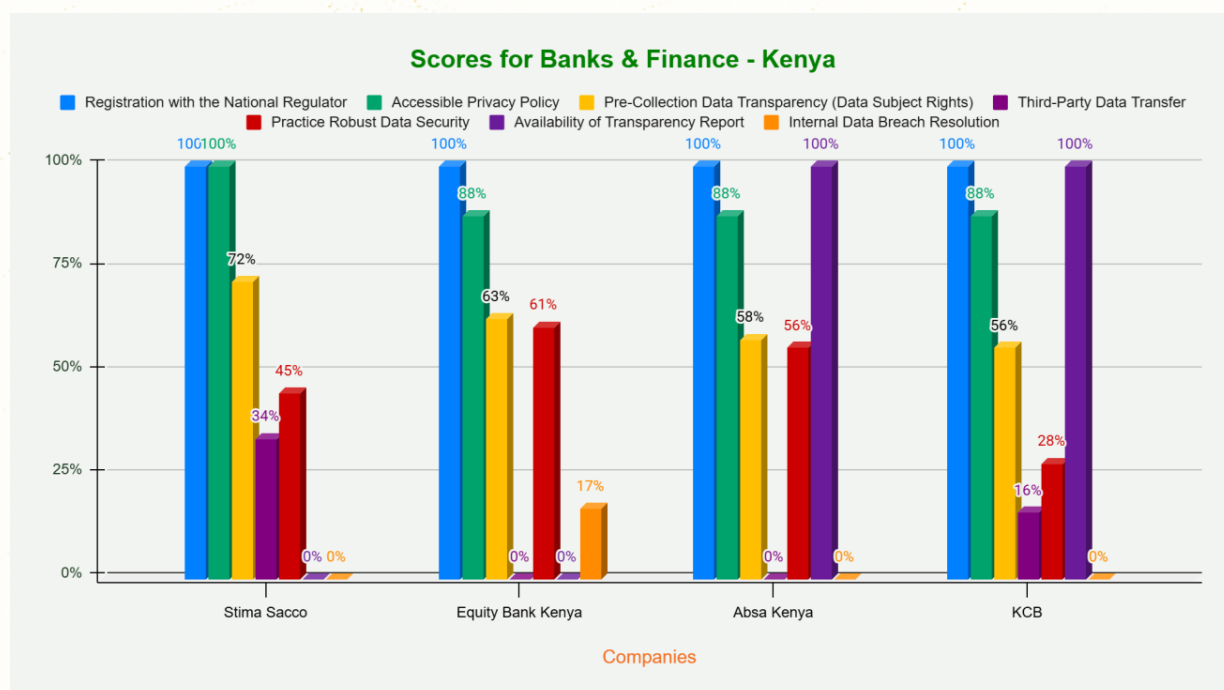
Internal data breach resolution shows incremental improvement, though compliance levels remain low overall. All banks recorded scores above zero for the first time. Stanbic Bank Zimbabwe leads with 42%, followed by NMB Bank at 25%, CBZ Bank at 17%, and Empower Bank at 8%. While these scores are modest, they represent a clear improvement from 0% across all institutions last year. This progress suggests emerging recognition of breach management obligations. However, the continued absence of clear internal procedures, defined reporting timelines, guaranteed user notification, and accessible reporting channels indicates that breach response frameworks remain insufficient to meet legal standards.

Compared to last year, Zimbabwe's banking sector demonstrates meaningful progress in data subject rights and internal breach awareness, alongside stable performance in privacy policy accessibility and data security. However, third-party data transfers and transparency reporting remain persistent areas of non-compliance, and improvements in breach resolution mechanisms are still at an early stage. Overall, while banks have strengthened certain aspects of their privacy practices, full compliance with data protection laws remains uneven. To advance toward stronger privacy governance, institutions must prioritise lawful and transparent third-party data sharing, institutionalise effective breach response systems, and expand transparency reporting to reinforce accountability and public trust.

h. *Stima Sacco, Equity Bank Kenya, ABSA Kenya and KCB Bank in Kenya*

The current assessment indicates continued regulatory compliance and incremental progress in certain privacy dimensions, alongside persistent weaknesses that constrain full alignment with data protection laws.

Compared to last year, improvements are evident in accessibility of privacy policies, observance of data subject rights, and data security for some institutions, while compliance relating to third-party data sharing remains weak and, in some cases, has deteriorated.



As in the previous assessment, all evaluated banks fulfilled registration requirements with the national data protection regulator, each scoring 100%. This consistency reflects strong baseline compliance with statutory obligations and demonstrates sector-wide awareness of regulatory oversight as a foundational requirement for lawful personal data processing.

There was demonstrable effort across all institutions to maintain accessible privacy policies. Stima Sacco emerged as the leading institution with a score of 100%, improving from 88% last year, indicating enhanced visibility and clarity of its privacy disclosures. Equity Bank Kenya, Absa Kenya, and KCB Kenya each maintained scores of 88%, unchanged from last year.

These results suggest that privacy policies remain publicly available, easily noticeable, and generally readable, satisfying core transparency requirements under Kenya's Data Protection Act. However, accessibility alone does not necessarily equate to comprehensive compliance, particularly where substantive rights and safeguards are insufficiently implemented.

The observance of data subject rights shows mixed progress compared to last year. Stima Sacco leads with a score of 72%, improving from 60%, reflecting stronger disclosure of processing purposes and better recognition of user rights. Equity Bank Kenya scored 63%, representing a slight decline from 66% last year, suggesting stagnation or minor regression in this area. Overall, these scores indicate that institutions are increasingly acknowledging data subject rights such as access, correction, and objection. However, inconsistencies in facilitating these rights, including complaint mechanisms and clarity around consent withdrawal, limit full compliance and effective user empowerment.

All assessed institutions continue to share personal data with third parties, but compliance levels remain low and, in several cases, have declined. Stima Sacco leads with 34%, down from 44% last year, followed by KCB Kenya at 16%, a decline from 30%. Equity Bank Kenya and Absa Kenya again scored 0%, unchanged from last year. These results highlight ongoing deficiencies in transparency regarding third-party recipients, categories of shared data, and lawful bases for transfer. Such shortcomings directly undermine data subject rights and contravene the duties of data controllers and processors under data protection laws, exposing institutions to regulatory and reputational risks.

Data security practices show gradual improvement overall, though performance varies across institutions. Equity Bank Kenya leads with 61%, maintaining its score from last year, followed by Absa Kenya at 56%, also unchanged. Stima Sacco improved to 45%, up from 28%, and KCB Kenya increased slightly to 28% from 22%. These trends indicate growing recognition of technical and organizational security obligations, particularly among smaller institutions. However, the relatively low scores for some banks suggest that security measures may still lack sufficient depth, documentation, or transparency to fully meet legal standards.

Beyond aggregate scores, institutional privacy frameworks reveal important distinctions. KCB Kenya demonstrates strong privacy compliance awareness, achieving 92% compliance through a comprehensive framework that includes explicit seven-year data retention periods, detailed third-party sharing disclosures (including credit bureaus and regulators), and structured procedures for facilitating data subject rights. Nonetheless, gaps remain in behavioral marketing consent mechanisms and transparency around law enforcement access.

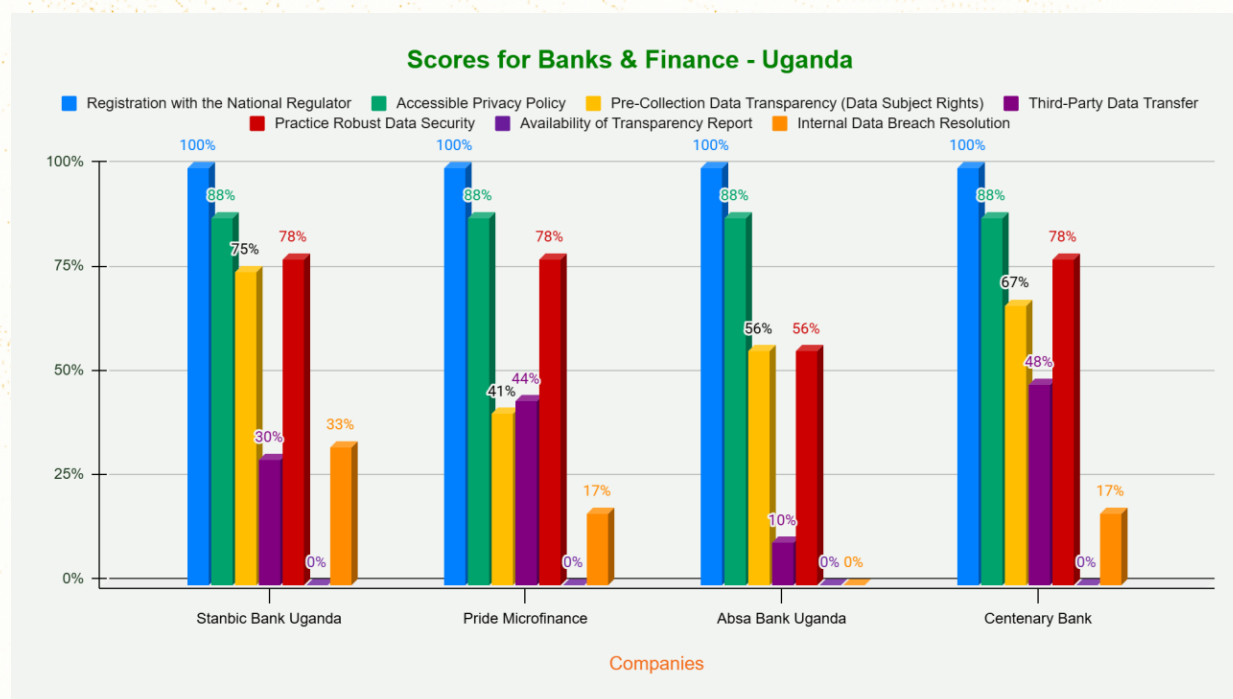
Absa Bank Kenya, with an overall performance of 79%, reflects the application of international banking group standards within the Kenyan context. Its policy addresses cross-border data transfers, automated credit decision-making, and financial data security, though more specific retention disclosures and enhanced third-party transparency would strengthen compliance.

By contrast, Stima Sacco's overall performance of 50% highlights the challenges faced by cooperative financial institutions. While improvements are evident in policy accessibility and data subject rights, significant gaps remain in retention specificity, third-party transparency, and rights facilitation, underscoring the need for targeted guidance and capacity-building support for smaller institutions.

Compared to last year, the assessment shows incremental but uneven progress in privacy governance. Regulatory registration and policy accessibility remain strong, and some institutions have improved in data subject rights and security practices. However, third-party data sharing continues to represent a systemic compliance weakness, and improvements in this area have been limited or reversed.

Overall, while awareness of data protection obligations is evident, full compliance with data protection laws has not yet been achieved across the sector. Strengthening lawful third-party data governance, enhancing security implementation, and improving practical mechanisms for exercising data subject rights will be critical to advancing accountability, regulatory compliance, and public trust.

i. *Stanbic Bank Uganda, Pride microfinance, ABSA Bank Uganda and Centenary Bank in Uganda*



Bottom of Form

The current assessment of Ugandan banks shows overall stability in baseline compliance with data protection requirements, alongside incremental improvements in certain substantive areas and persistent weaknesses in accountability mechanisms. Compared with last year, banks continue to demonstrate awareness of privacy obligations, but progress remains uneven across key compliance indicators.

As in last year's assessment, all assessed banks fulfilled registration requirements with the national regulator (NITA-U), each scoring 100%. This reflects continued compliance with statutory registration obligations and confirms that all institutions remain under formal regulatory oversight for personal data processing. All banks again demonstrated effort to maintain accessible privacy policies, with each institution scoring 88%, except Pride Microfinance, whose score declined from 100% to 88%. The remaining institutions (Stanbic Bank Uganda, Centenary Bank, and Absa Bank Uganda) maintained their scores from last year.

These results indicate that privacy policies remain publicly available, easily noticeable, and generally readable, supporting baseline transparency requirements under Uganda's data protection framework. However, as in previous assessments, accessibility alone does not guarantee comprehensive compliance in practice.

Observance of data subject rights shows mixed movement, with notable improvements by some institutions and declines by others. Stanbic Bank Uganda leads with a score of 75%, improving from 72%, reflecting clearer articulation of user rights and processing practices. Centenary Bank scored 67%, representing a decline from 77%, while Absa Bank Uganda improved slightly to 56% from 53%. Pride Microfinance also improved to 41%, up from 38%. These results suggest a general strengthening of recognition of data subject rights such as access, correction, deletion, and complaint mechanisms. However, uneven performance indicates that facilitation of these rights particularly clarity of procedures, conditions, and timelines remains inconsistent across institutions.

All assessed banks share personal data with third parties, but compliance levels remain low, despite some improvement compared to last year. Centenary Bank leads with 48%, up from 40%, followed by Pride Microfinance at 44%, a substantial increase from 10%. Stanbic Bank Uganda scored 30%, improving from 26%, while Absa Bank Uganda declined to 10% from 24%. While these improvements suggest growing awareness of disclosure obligations, the continued lack of detailed information on third-party recipients, categories of shared data, and lawful bases for transfer undermines data subject rights and remains inconsistent with data protection law requirements.

All banks demonstrated effort to comply with data security obligations, with performance remaining relatively stable overall. Stanbic Bank Uganda, Pride Microfinance, and Centenary Bank each scored 78%. Stanbic and Centenary maintained their scores from last year, while Pride Microfinance improved significantly from 45% to 78%. Absa Bank Uganda maintained a score of 56%, unchanged from last year. These scores indicate reasonable implementation of technical and

organizational security measures. However, the lack of accompanying transparency and breach response detail limits the ability to assess the effectiveness of these safeguards in practice.

As in last year's assessment, none of the banks have published transparency reports. The continued absence of transparency reporting restricts public insight into government data requests, third-party disclosures, and internal oversight, weakening institutional accountability. Internal data breach resolution shows incremental improvement, though compliance remains low overall.

Stanbic Bank Uganda leads with 33%, up from 8%, followed by Pride Microfinance and Centenary Bank at 17% each, while Absa Bank Uganda scored 0%, unchanged from last year. Although these scores represent progress compared to last year's uniformly poor performance, the absence of clear breach notification requirements, defined investigation timelines, and guarantees of fair and impartial processes indicates that breach response frameworks remain inadequate under data protection laws.

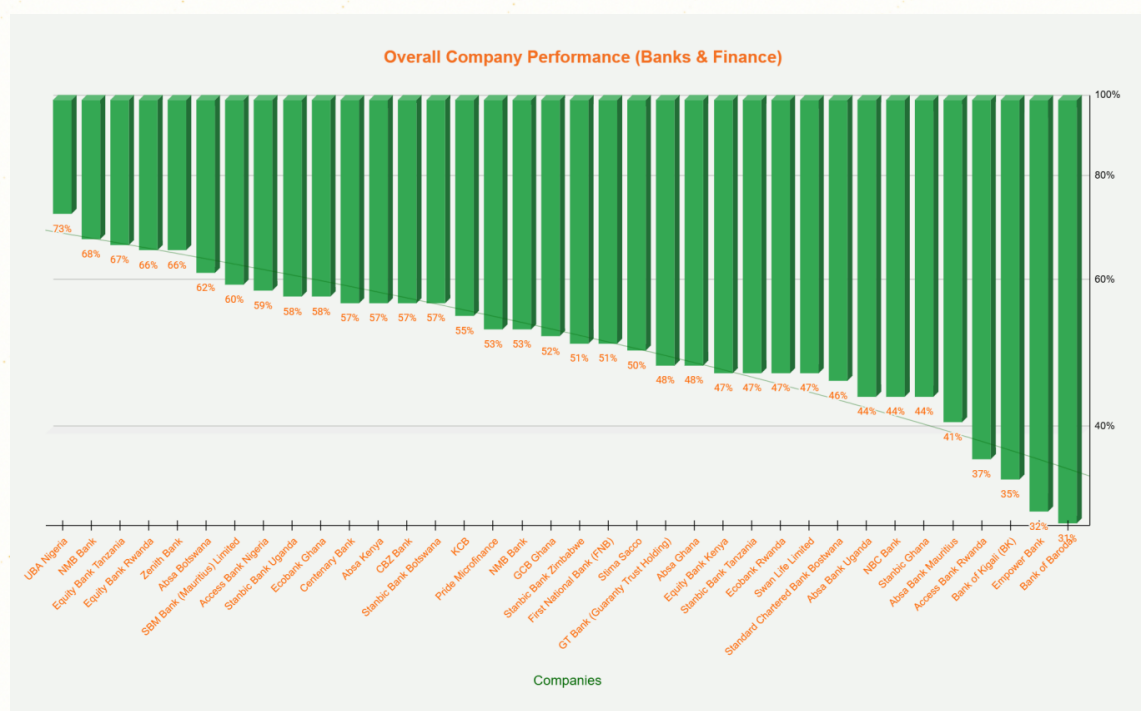
Banks and financial institutions continue to perform better than most other sectors assessed. Stanbic Bank Uganda remains the strongest overall performer, with relatively high scores in pre-collection transparency and internal breach response. Its privacy policy is prominently displayed and fairly readable, provides multiple complaint channels, and recognises key data subject rights. However, it lacks a transparency report and does not clearly outline breach notification obligations, investigation timelines, or user notification requirements.

Centenary Bank performs well on third-party data transfer practices, allowing data sharing with defined categories of professional and regulatory entities and offering multiple reporting channels, including references to NITA-U. However, it does not specify the exact data types shared with third parties. Absa Bank Uganda records the lowest scores in third-party data transfer, data security transparency, and breach resolution. While its privacy policy clearly outlines purposes of data collection and recognises several data subject rights, it is largely silent on breach handling procedures and provides limited clarity on complaint escalation pathways.

Compared with last year, Uganda's banking sector demonstrates incremental progress in data subject rights recognition, data security, and early breach response awareness, while maintaining strong performance in regulatory registration and policy accessibility. However, persistent weaknesses remain in third-party data governance, transparency reporting, and comprehensive breach management.

Overall, while banks show growing awareness of data protection obligations, full compliance with Uganda's data protection laws has not yet been achieved. Strengthening lawful third-party data sharing controls, institutionalising clear and enforceable breach response frameworks, and improving transparency reporting will be critical to enhancing accountability, regulatory compliance, and public trust.

3.4.4.3 Comparison of companies/entities within the sector



High-Performing Jurisdictions: Emerging Compliance Leaders and Trajectories

A small group of jurisdictions and institutions now demonstrate comparatively stronger privacy governance, signalling emerging leadership in data protection compliance within the banking and finance sector. Nigeria and Tanzania stand out most clearly in this category.

Nigeria leads overall, with UBA Nigeria achieving the highest sector score at 73%, followed by Zenith Bank (66%) and Access Bank Nigeria (59%). Compared to last year, when Nigerian banks clustered around the mid-to-high 40% range, these results reflect meaningful progress. The improved scores suggest stronger institutionalisation of privacy practices, including clearer governance structures, improved data security controls, and more consistent implementation of data subject rights. While not yet exemplary, these banks are moving closer to alignment with data protection laws and supervisory expectations.

Tanzania also shows a strong upward trajectory. NMB Bank Tanzania (68%) and Equity Bank Tanzania (67%) now rank among the sector's top performers, representing a marked improvement from last year, when Tanzanian banks were among the weakest performers, with scores in the mid-30% to low-40% range. This shift suggests enhanced regulatory engagement, stronger internal controls, and greater prioritisation of privacy compliance, particularly in security and policy implementation.

Rwanda's Equity Bank Rwanda (66%) similarly reflects notable progress compared to last year's generally weak performance in the country. This improvement suggests that targeted institutional reforms can significantly elevate compliance outcomes even in jurisdictions previously characterised by low sector-wide performance.

Despite these gains, it is notable that only one institution exceeds 70%. This indicates that even in high-performing jurisdictions, compliance remains partial, with unresolved gaps in accountability-focused obligations such as transparency reporting and third-party data governance.

Mid-Range Performers: Partial Compliance and Structural Gaps (Change Over Time)

Most jurisdictions fall within a mid-range performance band, typically between 50% and 59%, reflecting partial compliance with data protection requirements alongside persistent structural weaknesses.

Countries such as Uganda, Ghana, Kenya, Zimbabwe, and Botswana largely populate this category. In Uganda, Stanbic Bank Uganda (58%) and Centenary Bank (57%) have maintained their relative positions, showing modest improvement but limited upward movement beyond last year's levels. Pride Microfinance (53%) shows incremental progress, suggesting gradual uptake of baseline privacy practices.

However, Absa Bank Uganda (44%) remains below the mid-range threshold, indicating uneven compliance within the same regulatory environment.

Kenya's performance is similarly mixed. Absa Kenya and KCB (both at 57% and 55% respectively) show improvement compared to last year's mid-40% scores, suggesting growing attention to privacy governance. However, Equity Bank Kenya (47%) lags behind its regional peers, highlighting inconsistencies in implementation even among large financial institutions.

Ghana shows moderate consolidation rather than acceleration. Ecobank Ghana (58%) and GCB Ghana (52%) have improved slightly, while Absa Ghana (48%) remains just below the mid-range band. These results indicate steady but cautious progress, with compliance efforts focused more on formal requirements than on deeper accountability mechanisms.

Across this group, improvements over time tend to concentrate on visible compliance measures such as privacy policy availability, security controls, and basic rights recognition. Structural gaps remain in areas requiring sustained governance investment, including third-party data management, internal breach resolution procedures, and transparency reporting.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

At the lower end of the performance spectrum are institutions and jurisdictions exhibiting systemic compliance challenges, with scores consistently below 45%. These include parts of Rwanda, Zimbabwe, and Mauritius.

In Rwanda, despite improvements by Equity Bank Rwanda and Ecobank Rwanda (47%), Access Bank Rwanda (37%) and Bank of Kigali (35%) continue to underperform. While these scores represent marginal gains over last year, they remain indicative of weak privacy governance structures and limited operationalisation of data protection principles.

Zimbabwe shows a similar pattern. While CBZ Bank (57%) performs relatively well, Empower Bank (32%) continues to score poorly, with limited evidence of improvement over time. This divergence within the same jurisdiction suggests uneven regulatory enforcement and inconsistent institutional commitment to privacy compliance.

Mauritius presents persistent compliance challenges at the lower end. Bank of Baroda (31%) remains the weakest performer, with minimal improvement from last year, while Absa Bank Mauritius (41%) and Swan Life Limited (47%) occupy the lower mid-range. These scores point to enduring gaps in governance, particularly around accountability, breach preparedness, and transparency obligations.

Overall, low-performing jurisdictions tend to exhibit stagnation rather than rapid regression, but the lack of meaningful upward movement suggests that privacy compliance remains a low institutional priority in many cases.

Key Cross-Cutting Implications

Several cross-cutting themes emerge across all performance tiers. First, while the banking and finance sector outperforms other digital sectors in average scores, no institution demonstrates full compliance with data protection laws. Even the strongest performers show only partial alignment with legal and regulatory expectations.

Second, year-on-year improvements are uneven and often driven by enhancements in easily auditable or externally visible measures. High-risk and accountability-based obligations such as third-party data sharing oversight, internal breach resolution mechanisms, and public transparency reporting remain the weakest areas across jurisdictions.

Third, jurisdictional context influences performance, but institutional governance plays a decisive role. Significant performance variation within the same country indicates that compliance outcomes are shaped as much by internal leadership and risk culture as by national regulatory frameworks.

In conclusion, the updated performance status suggests that while the banking and finance sector is gradually strengthening its privacy practices, compliance remains incomplete and fragile. Without deeper investment in governance, accountability, and enforcement-driven reforms, current gains risk plateauing, leaving institutions exposed to legal, operational, and reputational risks under evolving data protection regimes.

3.4.5 Insurance Sector Analysis

3.4.5.1 Overview of the sector and data collectors evaluated

The insurance sector across East, Southern, and parts of West Africa continues to expand steadily, driven by rising awareness of insurance as a risk management tool, growing middle-class populations, increased mobile phone penetration, and the rapid digitisation of financial services. In countries such as Kenya, Tanzania, Uganda, Zimbabwe, Nigeria, Ghana, and Botswana, the market now comprises both long-established insurers and a growing number of technology-driven providers, including insurtech startups that use digital platforms to deliver more flexible and affordable insurance products.

Although growth has been notable, insurance penetration across the region remains below global averages, particularly in low- and middle-income markets. Nonetheless, improving economic conditions, expanding urban populations, and increased financial literacy are contributing to rising demand for both life and non-life insurance products. In West African markets such as Nigeria and Ghana, digital channels and mobile money ecosystems have accelerated the uptake of micro-insurance, health insurance, and usage-based products, while Botswana has seen steady development in more traditional insurance offerings supported by a relatively stable financial regulatory environment.

Digital transformation is now a defining feature of the sector. Insurers increasingly rely on mobile applications, web platforms, digital onboarding tools, and electronic payment systems to reach customers and streamline service delivery. Insurtech innovations including pay-as-you-go insurance, mobile health coverage, and embedded insurance products have expanded access, particularly for underserved populations. However, this shift has also intensified the collection and processing of personal and sensitive data, amplifying privacy and data protection risks.

Insurance providers routinely collect large volumes of personal information, including names, identification details, contact information, employment status, and financial data. For underwriting and claims management, insurers also process highly sensitive data, such as medical records, health histories, biometric identifiers, and claims histories. With increased digitalisation, data is often collected through mobile devices, online forms, and, in some cases, biometric verification tools such as facial recognition or fingerprints, particularly in mobile-based insurance services.

Customer data is frequently shared with third parties, including reinsurers, healthcare providers, claims assessors, payment processors, and analytics service providers. While such data sharing is integral to insurance operations, inadequate safeguards, limited transparency, or weak contractual controls can expose customers to privacy violations, data misuse, or security breaches.

Regulatory environments across the assessed countries vary significantly. Some jurisdictions, such as South Africa, Kenya, Nigeria, and Uganda, have enacted comprehensive data protection laws, while others including parts of Southern Africa and West Africa are still strengthening enforcement mechanisms and regulatory capacity. Ghana and Botswana, for instance, have established legal frameworks for data protection but continue to face challenges related to enforcement consistency and institutional oversight. As a result, compliance levels among insurers vary, and accountability for data misuse is uneven across the region.

Consumer trust remains a critical challenge for the insurance sector. In many countries, insurance is still perceived as costly or unnecessary, and concerns about fraud, opaque practices, and poor service delivery persist. These perceptions directly affect consumers' willingness to share personal data and engage fully with insurance providers. Compounding this issue is limited public awareness of data protection rights; many customers do not fully understand how their data is collected, used, shared, or retained, nor how to seek redress when their rights are violated.

Cybersecurity risks further complicate the landscape. As insurers increasingly rely on digital infrastructure, the sector faces growing exposure to cyberattacks, system vulnerabilities, and internal data breaches. Smaller insurers and insurtech startups, particularly in emerging markets, may lack the technical resources and expertise required to implement robust security controls, making them especially vulnerable.

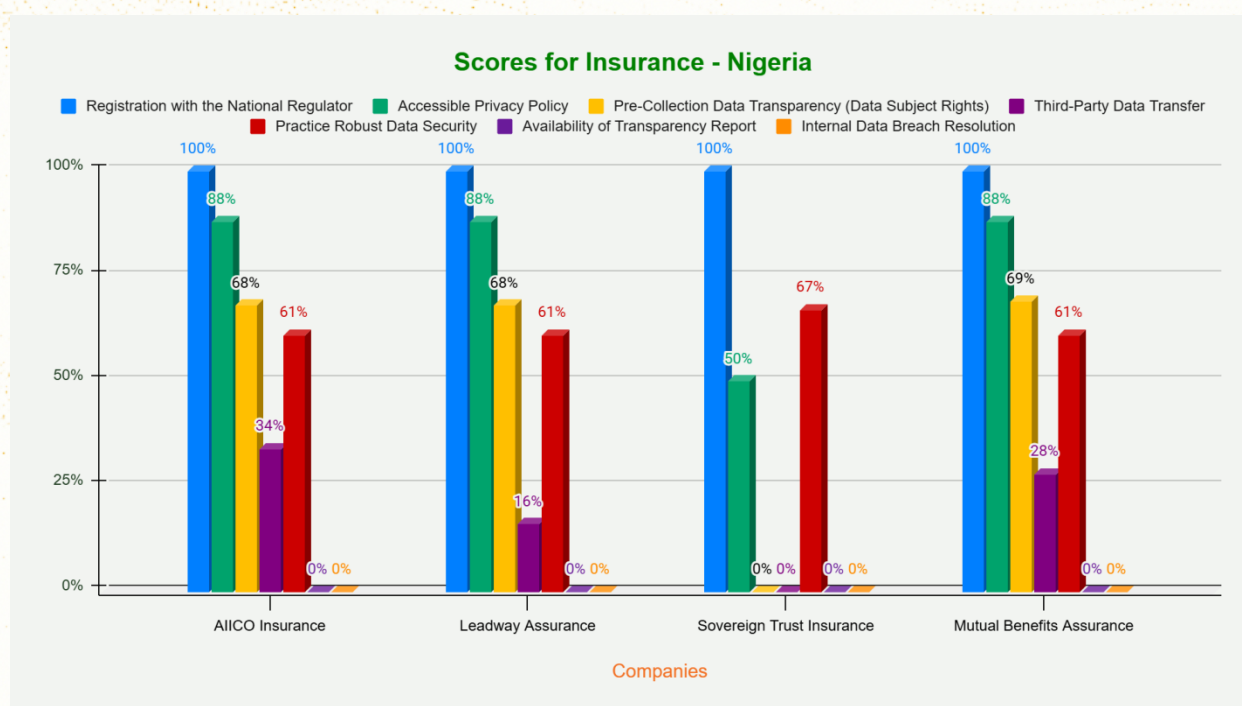
Overall, the insurance sector is undergoing rapid transformation, marked by innovation, market expansion, and increasing reliance on personal data. However, this growth has not always been matched by equivalent advances in privacy governance, data protection compliance, and transparency. Given the sensitive nature of the data involved, insurers must prioritise strong legal compliance, effective data security measures, and clear communication with customers. Strengthening privacy practices through compliance with national data protection laws, adoption of best practices for data security, responsible third party data sharing, and improved consumer awareness will be essential for building trust, reducing regulatory risk, and supporting the long-term sustainability of the insurance sector across the region.

3.4.5.2 Analysis of compliance with each criterion

This sectoral evaluation draws on a sample of 36 companies, with four (4) companies assessed per participating country, namely: AllCO Insurance, Leadway Assurance, Sovereign Trust Insurance and Mutual Benefits Assurance from Nigeria; Enterprise Insurance Company Limited, Star Assurance Limited, Hollard Insurance Ghana Limited and Vanguard Assurance Company Limited from Ghana; Botswana Life Insurance, Metropolitan Botswana, Hollard Botswana and Botswana Insurance Company from Botswana; Britam Rwanda, Old Mutual Rwanda, Prime Insurance and BK Insurance Rwanda from Rwanda; Jubilee Life Insurance Tanzania, NIC Tanzania, Britam Insurance Tanzania and Heritage Insurance Tanzania from Tanzania; Sicom–State Insurance Company of Mauritius Ltd, Jubilee Allianz General Insurance Mauritius Ltd, Eagle Insurance and Mauritius Union Assurance from Mauritius; Old Mutual Zimbabwe, Zimnat Lion Insurance, Alliance Insurance and Cell Insurance from Zimbabwe; Jubilee Insurance Kenya, Britam Insurance Kenya, ICEA Lion Insurance and CIC Kenya in Kenya; and UAP Old Mutual Uganda, Sanlam, Britam Uganda and Jubilee Insurance Uganda in Uganda.

a. AllCO Insurance, Leadway Assurance, Sovereign Trust Insurance and Mutual Benefits Assurance in Nigeria

All assessed insurance companies fulfilled the registration requirements with the national data protection regulator, with each institution achieving a perfect score of 100%. This reflects sector-wide compliance with baseline regulatory obligations and indicates formal recognition of oversight responsibilities in relation to the processing of personal data. The companies also demonstrated varying levels of effort in ensuring the availability of accessible privacy policies. AllCO Insurance, Leadway Assurance, and Mutual Benefits Assurance performed strongest in this area, each scoring 88%, suggesting that their privacy policies are publicly available and reasonably accessible to customers. In contrast, Sovereign Trust Insurance scored 50%, indicating limited accessibility and raising concerns about transparency and user awareness of data processing practices.



With respect to the observance of data subject rights, performance across the sector was mixed. Mutual Benefits Assurance leads with a score of 69%, followed closely by AllCO Insurance and Leadway Assurance, each scoring 68%. These results suggest moderate alignment with data protection principles related to user rights such as access, correction, and complaint mechanisms.

Sovereign Trust Insurance scored 0%, reflecting a failure to meaningfully recognise or facilitate data subject rights, which presents a significant compliance gap.

All assessed insurers reported sharing personal data with third parties; however, compliance in this area remains low across the sector. Even the highest-performing institution, AllCO Insurance, scored only 34%, followed by Mutual Benefits Assurance at 28% and Leadway Assurance at 16%. These low scores indicate insufficient transparency regarding third-party recipients, data categories shared, and safeguards applied, which undermines core obligations of lawfulness, fairness, and accountability under data protection laws.

In terms of data security practices, the insurers demonstrated moderate effort. Sovereign Trust Insurance led with a score of 67%, while AllCO Insurance, Leadway Assurance, and Mutual Benefits Assurance each scored 61%. These results suggest the presence of basic technical and organisational safeguards, although the absence of detailed disclosures limits the ability to assess the robustness and effectiveness of these measures.

Notably, none of the assessed insurance companies published transparency reports, and all recorded 0% compliance for internal data breach resolution mechanisms. The absence of clear procedures for detecting, reporting, and resolving data breaches along with a lack of user notification frameworks represents a critical weakness in accountability and poses significant risks to regulatory compliance and consumer trust.

Mutual Benefits Assurance emerges as the strongest performer in the sector, supported by a relatively comprehensive privacy policy. The company provides detailed contact information, including dedicated customer service channels, and clearly identifies the categories of personal data collected, such as policyholder information, claims data, medical records, and financial details. Its policy outlines defined purposes for data processing including underwriting, claims management, fraud prevention, and regulatory compliance and offers reasonable transparency around data retention and third-party sharing. Importantly, the policy recognises key data subject rights, including access, correction, and complaint procedures, contributing to stronger alignment with data protection requirements.

AllCO Insurance demonstrates solid, though less comprehensive, privacy compliance. The company provides basic contact information and describes general categories of personal data collected through insurance operations. While AllCO acknowledges standard data subject rights and offers some transparency regarding third-party data sharing, gaps remain in specifying retention periods and detailing the nature of third-party arrangements, limiting full compliance.

Leadway Assurance shows moderate compliance, with privacy policies addressing fundamental requirements such as data collection purposes and basic data subject rights. However, the lack of detailed retention timelines and limited clarity around third-party sharing practices reduce the effectiveness of its privacy framework and weaken accountability.

Sovereign Trust Insurance faces the most significant compliance challenges. Limited accessibility of privacy information and insufficient detail regarding data processing practices restrict customer understanding and expose the company to heightened regulatory risk. The absence of meaningful recognition of data subject rights and internal breach response mechanisms further compounds these concerns.

Overall, the assessment indicates that while insurance companies in this sector demonstrate awareness of regulatory registration obligations and have taken initial steps toward transparency and data security, compliance with data protection laws remains partial and uneven. Persistent weaknesses in third-party data governance, transparency reporting, and internal breach response mechanisms highlight the need for stronger accountability frameworks. To improve compliance and build consumer trust, insurers must move beyond baseline measures and adopt clearer disclosures, enforceable data protection practices, and effective breach management systems.

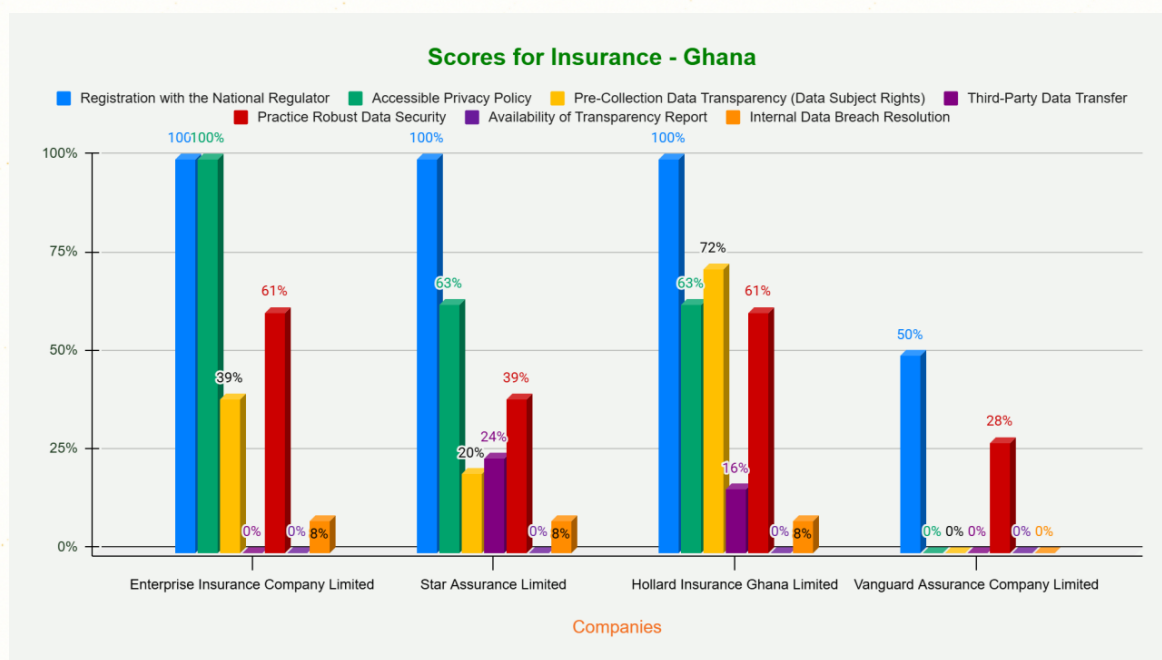
b. Enterprise Insurance Company Limited, Star Assurance Limited, Hollard Insurance Ghana Limited and Vanguard Assurance Company Limited in Ghana

The assessed insurance companies in Ghana demonstrated varying levels of compliance with data protection requirements, with notable strengths in regulatory registration but significant gaps in transparency, third-party data governance, and breach management.

Most of the reviewed insurers demonstrated compliance with registration requirements under Ghana's data protection framework. Enterprise Insurance Company Limited, Star Assurance Limited, and Hollard Insurance Ghana Limited achieved full compliance, each scoring 100%, reflecting active registration with the national regulator. Their certifications remain valid until April 30, 2026, August 7, 2026, and April 12, 2027, respectively.

In contrast, Vanguard Assurance Company Limited scored 50%, as its registration expired on May 29, 2023, exposing the company to regulatory and accountability risks.

The sector displays uneven performance in the availability and accessibility of privacy policies. Enterprise Insurance Company Limited leads with a score of 100%, indicating that its privacy policy is prominently displayed and reasonably accessible to users. Star Assurance Limited and Hollard Insurance Ghana Limited each scored 63%, reflecting the existence of published policies, albeit with lower visibility and reduced clarity. Vanguard Assurance Company Limited scored 0%, as it does not provide a publicly accessible privacy policy, creating a significant transparency and accountability gap. Readability analysis shows variability across available policies, with Hemingway grades ranging from 8 to 11, indicating moderate clarity but room for improvement. Word counts exceed 200 words for all companies except Vanguard, suggesting relatively comprehensive disclosures where policies exist. However, limited visibility and accessibility undermine their effectiveness in informing data subjects.



In terms of pre-collection data transparency and respect for data subject rights, performance across the sector remains inconsistent. Hollard Insurance Ghana Limited leads with a score of 72%, demonstrating a comparatively strong framework that includes full contact details, detailed categories of personal data collected, defined retention periods, extensive third-party disclosures, recognition of core data subject rights, and accessible complaint mechanisms. This positions Hollard as the sector's strongest performer and a reference point for best practice.

Enterprise Insurance Company Limited scored 39%, reflecting basic compliance through clearly stated purposes for data processing and defined retention periods ranging from six months to seven years. However, its policy lacks sufficient detail on third-party disclosures, deletion rights, and complaint procedures, limiting full alignment with data protection principles. Star Assurance Limited scored 20%, indicating weak compliance. Its policy contains vague retention timelines, limited specificity regarding data categories collected, minimal recognition of data subject rights, and poor transparency in relation to third-party data sharing. Vanguard Assurance Company Limited scored 0%, as the absence of any privacy policy leaves users without information on how their personal data is collected, used, or protected.

All assessed companies engage in third-party data sharing, but compliance levels remain very low across the sector. Star Assurance Limited leads marginally with a score of 24%, followed by Hollard Insurance Ghana Limited at 16%, while Enterprise Insurance Company Limited and Vanguard Assurance Company Limited each scored 0%. Enterprise permits sharing of personal data with third-party processors and group companies for service delivery, account management, and marketing, including advertising. However, it fails to identify specific third parties, clarify the types of data shared, or outline conditions for law enforcement access and reporting mechanisms, resulting in weak compliance.

Star Assurance allows data sharing for standard business operations and excludes advertisers, but the lack of clear reporting channels and limited disclosure on data categories shared reduces transparency and user protection. Hollard shares data with a wide range of third parties, including brokers, agents, reinsurers, and potential acquirers, with marketing-related sharing subject to user consent. Nevertheless, the absence of clarity on the specific data shared and limited breach reporting channels weakens accountability. Vanguard provides no disclosures due to the absence of a privacy policy.

Moderate effort was observed in relation to data security. Enterprise Insurance Company Limited and Hollard Insurance Ghana Limited lead with scores of 61% each. Enterprise achieves an A SSL rating and a C security headers score, and its privacy policy references storage safeguards and protective measures. Hollard scores B for both SSL and security headers, with its policy outlining precautionary measures and periodic security testing.

Star Assurance Limited scored 39%, reflecting a B SSL rating but an F security headers score, alongside general assurances about data protection without meaningful technical detail. Vanguard Assurance Company Limited scored 28%, despite holding an A SSL rating, due to the absence of a privacy policy addressing data security and a failing security headers score.

None of the assessed insurance companies publish transparency reports. Performance in this area is uniformly poor, signalling limited prioritisation of openness, weak accountability practices, and misalignment with national data protection expectations and international best practices. All companies registered very low levels of compliance in relation to internal data breach resolution. Enterprise Insurance Company Limited, Star Assurance Limited, and Hollard Insurance Ghana Limited each scored 8%, while Vanguard Assurance Company Limited scored 0%.

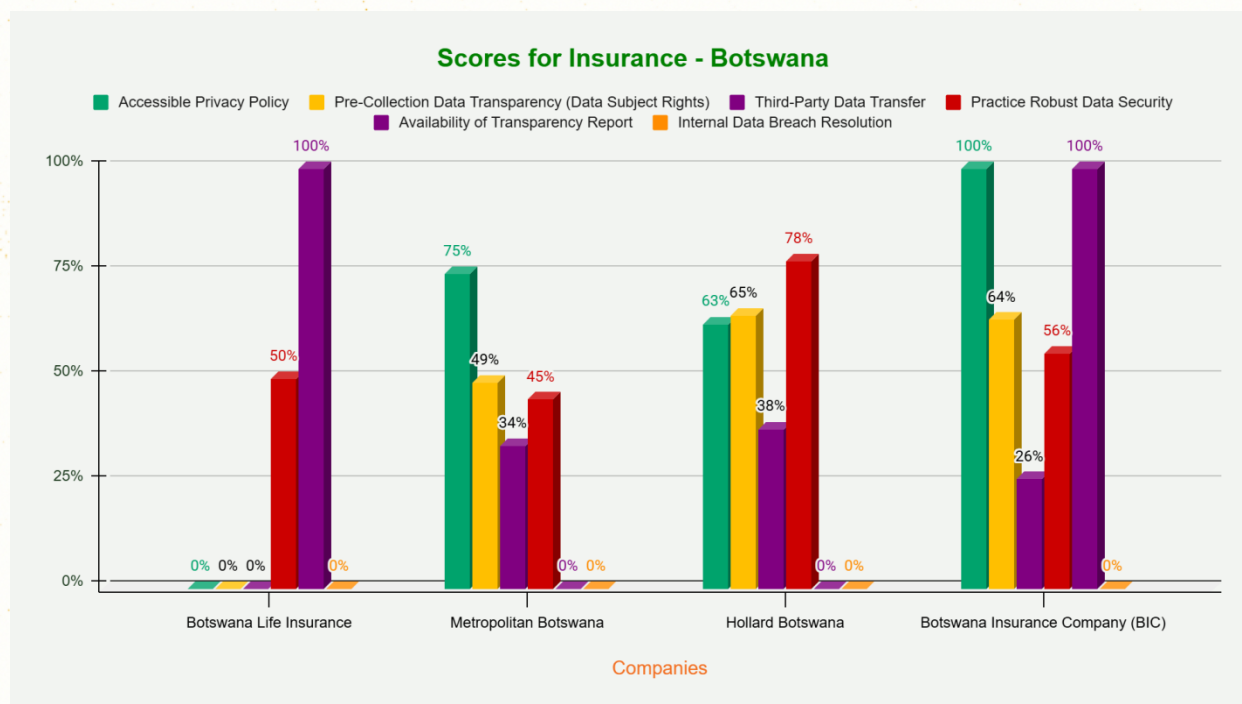
Enterprise acknowledges the right of users to be notified if personal data is accessed without authorisation but does not define internal procedures, investigation standards, reporting timelines, or clear channels for escalation. Star Assurance references general data protection obligations but lacks detail on breach notification, investigation processes, or user reporting mechanisms. Hollard similarly emphasises general security measures but fails to outline specific breach management procedures or notification frameworks. Vanguard provides no information due to the absence of a privacy policy.

Overall, the assessment indicates that while most insurance companies in Ghana demonstrate compliance with registration requirements and have taken initial steps toward transparency and data security, substantive gaps persist in third-party data governance, transparency reporting, and breach response mechanisms. The absence of comprehensive breach handling frameworks and limited disclosure of third-party data sharing practices pose significant risks to regulatory compliance and consumer trust. Strengthening these areas is essential for aligning insurance sector practices with data protection laws and for ensuring meaningful protection of policyholders' personal and sensitive data.

c. Botswana Life Insurance, Metropolitan Botswana, Hollard Botswana and Botswana Insurance Company in Botswana

The assessed insurance companies in Botswana demonstrate uneven performance in relation to privacy practices and compliance with data protection requirements, with notable disparities across key indicators such as policy accessibility, data subject rights, third-party data sharing, and internal breach response mechanisms.

The companies made varying efforts to ensure the availability of accessible privacy policies. Botswana Insurance Company (BIC) performed strongest in this area, scoring 100%, indicating that its privacy policy is clearly published and readily accessible. Metropolitan Botswana followed with a score of 75%, while Hollard Botswana scored 63%, reflecting moderate accessibility. In contrast, Botswana Life Insurance scored 0%, as no accessible privacy policy was identified, raising significant transparency and accountability concerns.



With respect to the observance of data subject rights, Hollard Botswana leads with a score of 65%, followed closely by Botswana Insurance Company at 64%. Metropolitan Botswana scored 49%, indicating partial recognition of user rights. Botswana Life Insurance again scored 0%, suggesting a failure to meaningfully acknowledge or facilitate data subject rights such as access, correction, deletion, or complaint mechanisms. These gaps directly affect individuals' ability to exercise control over their personal data, a core requirement under data protection laws.

All assessed companies were found to share personal data with third parties; however, compliance levels in this area remain very low across the sector. Hollard Botswana leads with a score of 38%, followed by Metropolitan Botswana at 34% and Botswana Insurance Company at 26%, while Botswana Life Insurance scored 0%. These low scores reflect insufficient disclosure regarding the categories of data shared, the identities of third-party recipients, and the legal safeguards governing such transfers, exposing customers to heightened risks of misuse and unlawful processing.

Demonstrable efforts were observed in relation to data security. Hollard Botswana recorded the strongest performance with a score of 78%, suggesting relatively robust technical and organisational safeguards. This was followed by Botswana Insurance Company at 56%, Botswana Life Insurance at 50%, and Metropolitan Botswana at 45%. While these results indicate some awareness of data security obligations, inconsistencies in policy disclosures limit transparency around how effectively these safeguards are implemented.

Only Botswana Life Insurance and Botswana Insurance Company published transparency reports, with each scoring 100% in this category. The absence of such reports from Hollard Botswana and Metropolitan Botswana highlights a lack of sector-wide commitment to proactive disclosure and public accountability regarding government requests, data access, or systemic privacy risks.

All assessed insurers registered very low levels of compliance with respect to internal data breach resolution mechanisms. The absence of clearly defined procedures for detecting, reporting, investigating, and remedying data breaches significantly undermines accountability and poses compliance risks, particularly given the volume and sensitivity of personal data processed within the insurance sector.

Overall, most insurance companies in Botswana score poorly on the accessibility of privacy policies, internal breach resolution, and the extent of customer control over personal data. While insurers routinely collect and process large volumes of sensitive personal information, their governance frameworks are often insufficiently transparent and not customer-centric.

Botswana Life Insurance emerges as a relatively stronger performer in certain respects, particularly in transparency and pre-collection disclosure. Its policy explains the categories of personal data collected, the purposes of processing, and provides some clarity on third-party transfers and data security. However, significant weaknesses remain, including the absence of an internal breach resolution framework, limited complaint mechanisms, and no explicit guarantee of data deletion rights, which undermine otherwise detailed disclosures.

Botswana Insurance Company demonstrates moderate performance, with strengths in articulating the purposes of data collection and outlining basic data security measures. It provides partial rights of access and correction but lacks clear retention timelines, user-friendly complaint mechanisms, and procedures for withdrawal of consent. These shortcomings limit customer control over personal data and weaken compliance with data protection principles.

Metropolitan Life Insurance performs weakly across most indicators. Although it scores relatively well on certain transparency measures, its low accessibility score, absence of meaningful data subject rights (including deletion and complaint mechanisms), lack of an internal breach response system, and sharing of personal data with advertisers significantly heighten privacy risks.

Hollard Botswana has an accessible privacy policy and demonstrates the strongest data security practices within the sector. However, like its peers, it lacks adequate internal data breach resolution mechanisms. While it recognises partial rights of access and correction and records the highest score for third-party data sharing, compliance remains below average due to the failure to specify the types of personal data shared and the absence of clear channels for individuals to report data breaches.

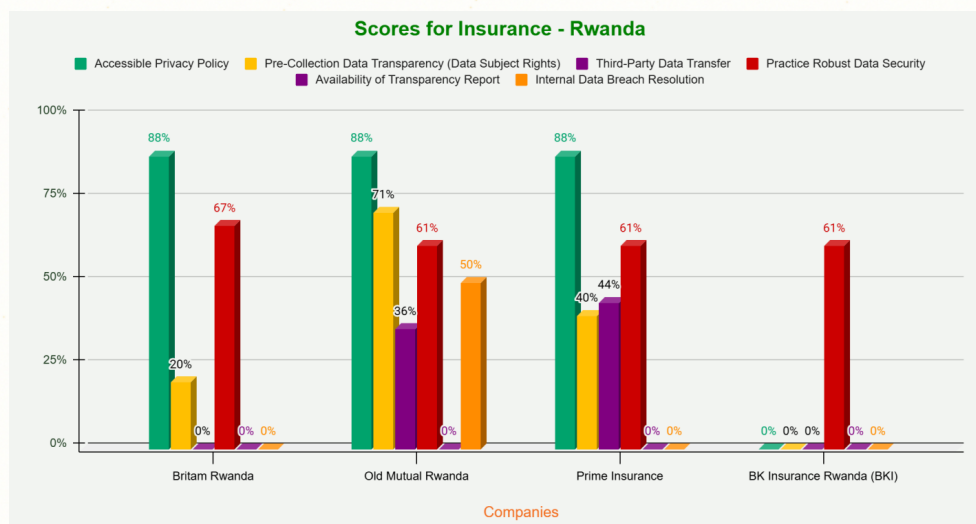
In sum, Botswana Life Insurance shows comparatively better practices, though still lacking in customer control and breach management mechanisms. Botswana Insurance Company and Hollard Botswana demonstrate only partial compliance, while Metropolitan Life Insurance trails significantly, offering minimal customer protections. Overall, the insurance sector in Botswana reveals an urgent need for reform, particularly in improving policy accessibility, establishing robust and transparent breach response frameworks, and ensuring enforceable data subject rights in line with data protection laws.

d. Britam Rwanda, Old Mutual Rwanda, Prime Insurance and BK Insurance Rwanda in Rwanda

Overall, the Rwandan insurance sector continues to demonstrate uneven and largely partial compliance with data protection and privacy obligations. While some companies have maintained or modestly improved their performance in specific areas since last year, structural weaknesses persist particularly in transparency reporting, third-party data sharing, and internal data breach resolution mechanisms.

As in the previous assessment, Britam Rwanda, Old Mutual Rwanda, and Prime Insurance continue to lead in the accessibility of privacy policies, each maintaining a score of 88%. Their policies are publicly available, exceed the minimum length threshold of 200 words, and are fairly readable, though the relatively high readability grades (12–13) suggest that complexity remains a barrier for average users.

In contrast, BK Insurance Rwanda again scored 0%, as no publicly available privacy policy could be identified. This represents no improvement from last year and continues to signal a serious lack of transparency and accountability, exposing customers to heightened privacy risks and potential regulatory non-compliance.



Performance in pre-collection transparency and observance of data subject rights shows mixed progress compared to last year. Old Mutual Rwanda strengthened its lead, improving from 66% to 71%, reflecting clearer contact disclosures, more comprehensive categorization of personal data collected, broader recognition of data subject rights (including access, correction, deletion, restriction, withdrawal of consent, and complaint mechanisms), and marketing opt-out options. However, its policy still provides only general descriptions of retention periods and law enforcement access.

Prime Insurance declined from 45% to 40%, while Britam Rwanda dropped from 30% to 20%, indicating regression in the clarity and scope of rights disclosure, retention practices, and complaint mechanisms. Both companies continue to provide only basic explanations of data collection purposes and limited recognition of user rights. BK Insurance Rwanda again scored 0%, offering no transparency or safeguards due to the absence of a privacy policy. These trends suggest that while Old Mutual is consolidating its position as the sector leader, other insurers are failing to build on earlier progress, weakening overall sectoral compliance with data protection principles.

All assessed insurers were found to share personal data with third parties, but compliance levels remain low, albeit with some shifts compared to last year. Prime Insurance remains the highest performer, scoring 44%, though this represents a decline from 50% last year. Old Mutual Rwanda improved significantly, rising from 16% to 36%, reflecting clearer identification of third-party categories and reporting channels, though it still fails to specify the exact data types shared. Britam Rwanda and BK Insurance Rwanda both scored 0%, unchanged from last year, due to a lack of transparency around third-party recipients, data categories shared, law enforcement access conditions, and breach reporting mechanisms. Despite modest improvements by Old Mutual, the sector overall continues to fall short of legal expectations regarding lawful, transparent, and accountable data sharing.

Data security practices remain one of the relatively stronger areas across the sector, with performance largely stable compared to last year. Britam Rwanda maintained its leading position at 67%, supported by strong technical indicators (B SSL rating and A security headers), though its policy still lacks detailed explanations of safeguards. Old Mutual Rwanda, Prime Insurance, and BK Insurance Rwanda each scored 61%. Prime Insurance improved from 45% to 61%, reflecting more detailed disclosures on physical, electronic, and procedural safeguards, despite weak security headers. Old Mutual and BK Insurance maintained their previous scores. Notably, BK Insurance's relatively strong technical security scores contrast sharply with its complete lack of policy transparency, underscoring a disconnect between technical controls and governance disclosure.

As in the previous assessment, none of the assessed insurance companies have published transparency reports. Britam Rwanda, Old Mutual Rwanda, Prime Insurance, and BK Insurance Rwanda all scored 0% in this category. This continued absence of reporting reflects a persistent lack of proactive accountability and alignment with international best practices, particularly regarding disclosures on government access requests and systemic risks.

Internal data breach resolution remains a critical weakness, though there has been limited improvement. Old Mutual Rwanda showed notable progress, increasing its score from 17% to 50%, indicating clearer acknowledgment of breach handling and complaint processes, albeit still lacking detailed timelines, investigation standards, and guarantees of impartiality.

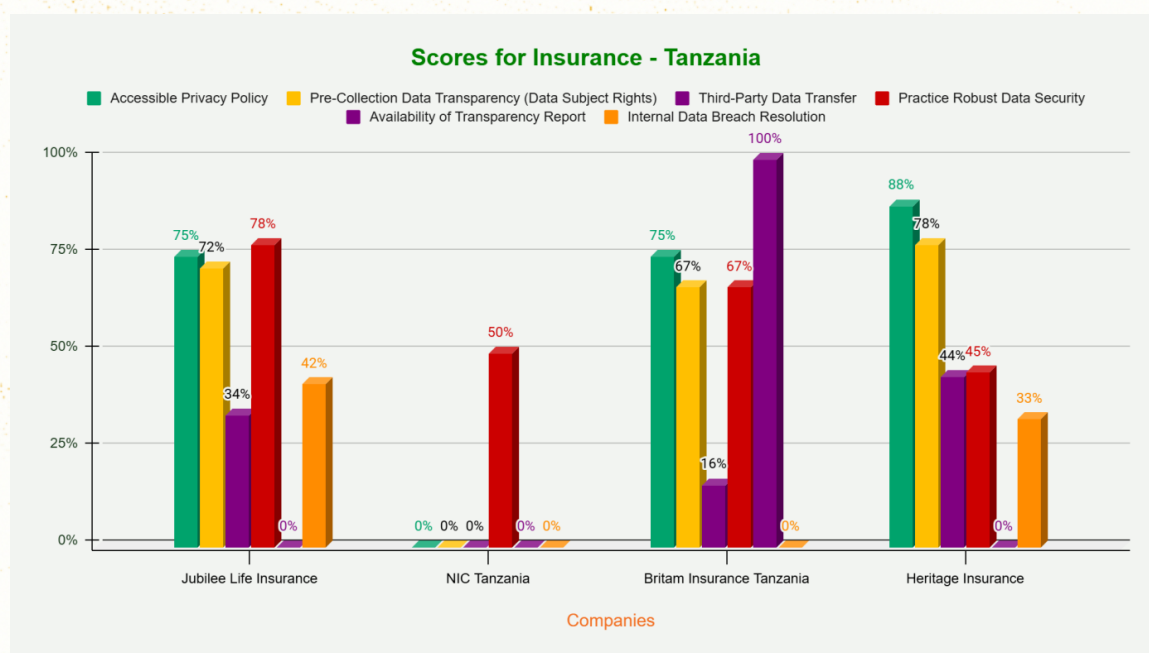
All other insurers (Britam Rwanda, Prime Insurance, and BK Insurance Rwanda maintained scores of 0%), unchanged from last year. Their policies either fail to address data breaches altogether or do not provide actionable guidance on notification, investigation, or remediation, leaving data subjects with little recourse in the event of a breach.

Compared to last year, the overall picture remains largely unchanged, with modest improvements by Old Mutual Rwanda offset by stagnation or decline among other insurers. Old Mutual continues to emerge as the strongest performer, particularly in data subject rights, third-party disclosures, and breach handling, though gaps remain in retention specificity and transparency reporting.

Prime Insurance and Britam Rwanda show weakening compliance, especially in user rights and third-party transparency, raising concerns about regression rather than continuous improvement. BK Insurance Rwanda remains the most problematic, with persistent zero scores across multiple indicators, representing a significant compliance risk under data protection laws.

In sum, while technical data security measures are relatively consistent across the sector, governance, transparency, and accountability mechanisms remain underdeveloped. The lack of transparency reports, weak third-party data transfer disclosures, and inadequate internal breach response frameworks highlight the urgent need for regulatory enforcement, clearer guidance, and stronger institutional commitment to data protection compliance in Rwanda's insurance sector.

e. *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 with 1478 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.

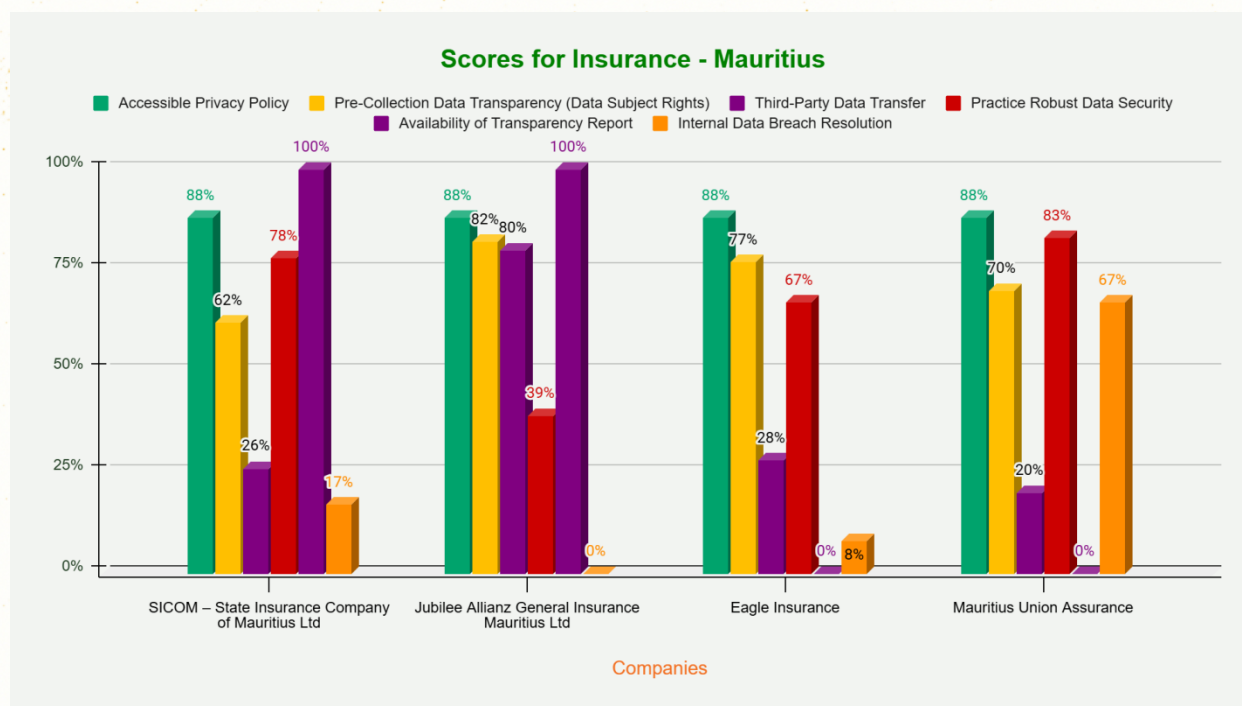
The level of transparency in informing users about data collection varied with Heritage observed as the most transparent at 69% while moderate transparency was exhibited by Jubilee (61%), NIC (56%) and Britam (53%). The lower scores indicate that some companies may not clearly communicate what data is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

f. Sicom – State Insurance Company of Mauritius Ltd, Jubilee Allianz General Insurance Mauritius Ltd, Eagle Insurance and Mauritius Union Assurance in Mauritius



The Mauritian insurance sector continues to demonstrate moderate to strong awareness of data protection obligations, with notable improvements in some areas since last year, alongside regression in others.

Overall, the sector reflects growing maturity in privacy governance, though inconsistencies persist across companies and compliance indicators.

All assessed insurance companies (SICOM-State Insurance Company of Mauritius Limited, Jubilee Allianz General Insurance Mauritius Ltd, Eagle Insurance, and Mauritius Union Assurance) continue to maintain accessible privacy policies, each scoring 88% in the current assessment. This represents a decline for Mauritius Union Assurance, which dropped from a perfect score of 100% last year, while SICOM, Jubilee Allianz, and Eagle Insurance maintained their previous scores. These results indicate that while policy availability and visibility remain strong across the sector, some firms have lost ground in terms of clarity or accessibility, underscoring the need for regular review and updating of privacy documentation to ensure continued compliance.

All companies demonstrated efforts to recognise and facilitate data subject rights, though performance levels vary and some scores declined compared to last year. Jubilee Allianz General Insurance Mauritius Ltd leads with a score of 82%, down from 88%, reflecting continued strong disclosure of data practices, lawful bases for processing, and user rights, albeit with less clarity in certain areas. Eagle Insurance and Mauritius Union Assurance both improved, scoring 77%, up from 70% and 68% respectively, reflecting stronger articulation of data subject rights, lawful processing bases, and complaint mechanisms. SICOM maintained its score of 62%, indicating stable but limited progress in this area. Overall, the sector demonstrates growing recognition of data subject rights, though declining scores for some insurers highlight the need for consistent and continuous improvement to meet evolving regulatory expectations.

All assessed companies share personal data with third parties, but compliance in this area remains uneven. Jubilee Allianz General Insurance Mauritius Ltd shows a marked improvement, scoring 80%, up from 44% last year, and clearly leading the sector. This improvement reflects better disclosure of third-party recipients, consent requirements, and safeguards for cross-border transfers. By contrast, Eagle Insurance declined to 28% from 36%, SICOM improved slightly to 26% from 20%, and Mauritius Union Assurance dropped to 20% from 34%. These lower scores point to continued deficiencies in

identifying third-party recipients, specifying the categories of data shared, and clarifying law enforcement access, which may undermine compliance with data protection principles of transparency and accountability.

Visible and significant improvements were recorded in data security practices across most companies. Mauritius Union Assurance now leads with 83%, up from 61% last year, reflecting strengthened organisational and technical safeguards and clearer governance frameworks. SICOM improved to 78% from 67%, and Eagle Insurance rose to 67% from 50%, indicating increased investment in data security controls. In contrast, Jubilee Allianz General Insurance Mauritius Ltd declined to 39% from 56%, suggesting potential gaps between policy commitments and technical or operational implementation. These trends indicate that while data security is increasingly prioritised, progress remains uneven and should be reinforced through detailed disclosures and consistent implementation.

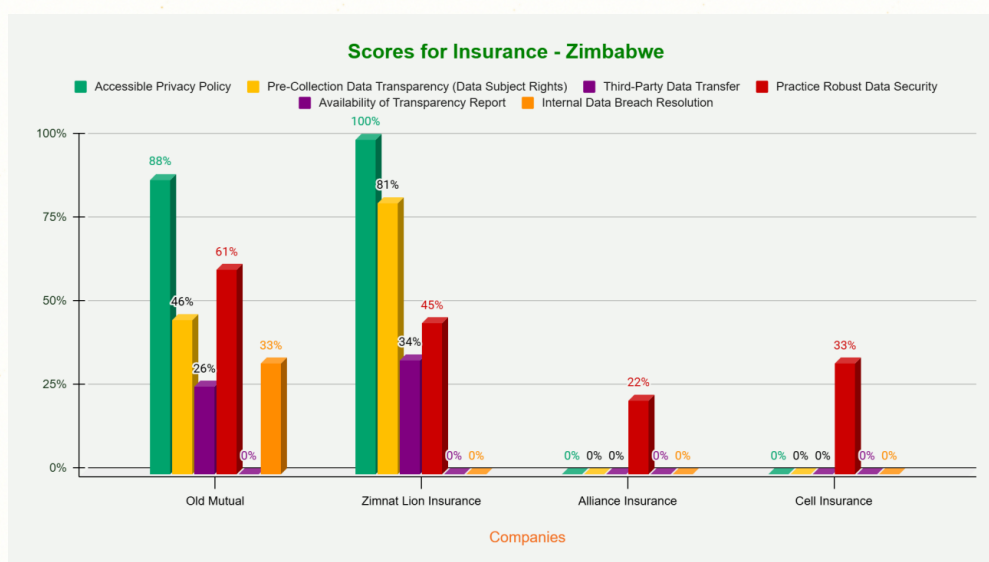
Transparency reporting presents a mixed picture. Jubilee Allianz General Insurance Mauritius Ltd maintained its perfect score of 100%, continuing its leadership in public accountability. SICOM recorded a significant improvement, increasing from 0% last year to 100%, demonstrating enhanced commitment to openness and regulatory best practices. In contrast, Mauritius Union Assurance experienced a sharp decline, falling from 100% last year to 0%, while Eagle Insurance continues to lack transparency reports. These fluctuations highlight inconsistencies in sector-wide accountability and underscore the importance of sustained transparency efforts.

All companies continue to demonstrate efforts to establish internal data breach resolution mechanisms, though overall compliance remains limited. Mauritius Union Assurance leads with a score of 67%, maintaining its performance from last year and reflecting clearly defined breach notification obligations and regulatory reporting timelines. SICOM maintained a low score of 17%, indicating limited procedural clarity. Eagle Insurance improved slightly to 8% from 0%, suggesting early steps toward formalisation. In contrast, Jubilee Allianz General Insurance Mauritius Ltd declined from 8% to 0%, reflecting the absence of clear internal breach response procedures in publicly available policies. These findings suggest that while awareness of breach obligations exists, most insurers still lack comprehensive, transparent, and user-facing breach response frameworks, posing compliance and trust risks.

Compared to last year, the Mauritian insurance sector shows both progress and regression, resulting in a more complex and uneven compliance landscape. Jubilee Allianz General Insurance Mauritius Ltd and Mauritius Union Assurance remain sector leaders, though both exhibit notable weaknesses in certain areas. SICOM demonstrates steady improvement, particularly in transparency and security, while Eagle Insurance shows incremental gains but continues to lag in accountability mechanisms. Overall, the sector performs well in terms of policy accessibility and recognition of data subject rights, reflecting alignment with the Data Protection Act 2017. However, persistent gaps in third-party data sharing transparency, breach response mechanisms, and consistency in transparency reporting indicate a need for stronger regulatory enforcement, clearer guidance, and ongoing internal governance improvements to ensure full and sustained compliance with data protection laws.

g. Old Mutual Zimbabwe, Zimnat Lion Insurance, Alliance Insurance and Cell Insurance in Zimbabwe

Compared to last year, the insurance sector in Zimbabwe shows measured but uneven progress in privacy practices and data protection compliance. While some companies have made notable improvements particularly in policy accessibility and recognition of data subject rights systemic weaknesses remain, especially in transparency reporting and internal data breach resolution.



Unlike last year, when only one insurer had an accessible privacy policy, two companies now demonstrate policy accessibility. Zimnat Lion Insurance leads with a score of 100%, representing a significant improvement from 0% last year, while Old Mutual Zimbabwe maintains its score of 88%, reflecting consistent performance. In contrast, Alliance Insurance and Cell Insurance continue to have no accessible privacy policies, maintaining scores of 0%, which indicates ongoing non-compliance with basic transparency and accountability requirements.

Only Old Mutual Zimbabwe and Zimnat Lion Insurance demonstrated efforts to observe data subject rights. Old Mutual Zimbabwe improved to 46% from 35% last year, while Zimnat Lion Insurance recorded a substantial increase to 81% from 0%, now leading the sector in this category. The remaining companies (Alliance Insurance and Cell Insurance) again recorded 0%, reflecting the absence of publicly available information on how personal data is collected, used, or how individuals may exercise their rights. This continued lack of transparency raises compliance risks and undermines consumer trust.

Although all assessed companies share personal data with third parties, only Zimnat Lion Insurance (34%, up from 0%) and Old Mutual Zimbabwe (26%, up from 10%) demonstrated partial compliance by disclosing some aspects of third-party data sharing. Alliance Insurance and Cell Insurance maintained scores of 0%, suggesting that data may be shared without any publicly disclosed safeguards or explanations. This presents a significant concern, as third-party data transfers are a high-risk area under data protection laws and require clear justification and transparency.

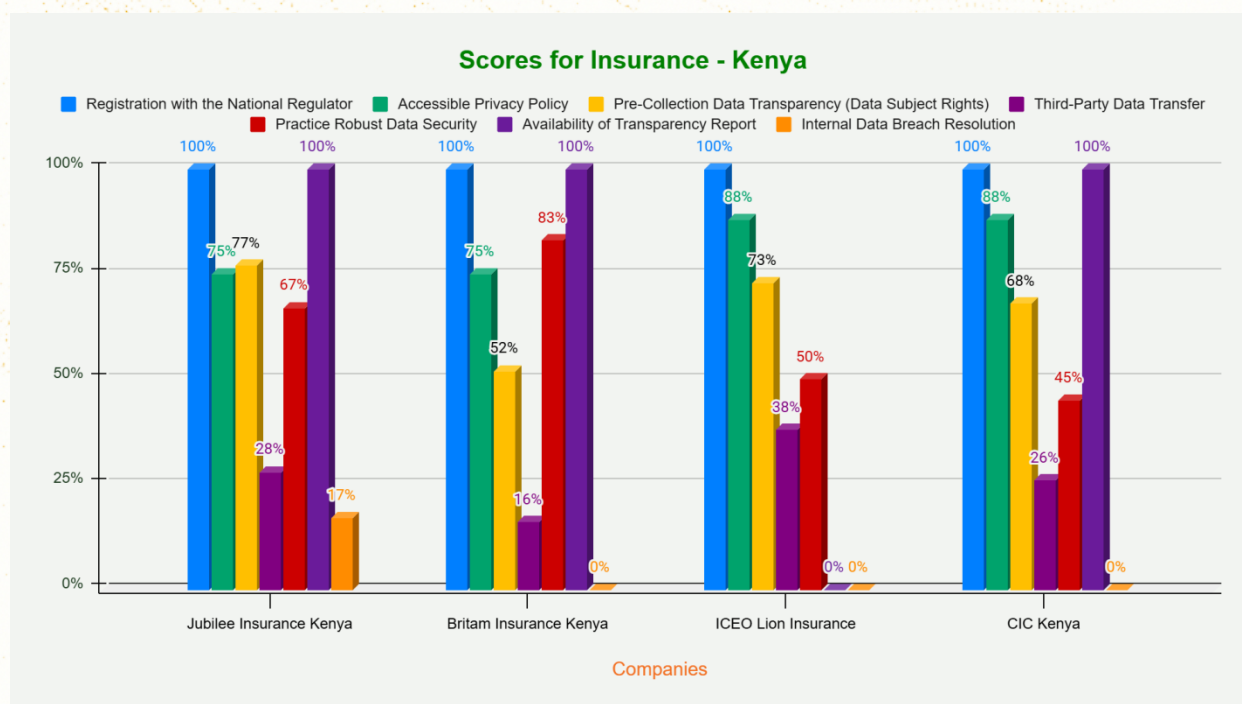
All companies showed some effort to secure personal data, with Old Mutual Zimbabwe maintaining its sector-leading score of 61%, unchanged from last year. Zimnat Lion Insurance improved to 45% from 28%, and Cell Insurance increased to 33% from 22%, indicating incremental progress. Alliance Insurance maintained its score of 22%, reflecting minimal improvement. While these results suggest a baseline level of technical protection across the sector, security measures are not consistently supported by comprehensive policy disclosures or governance frameworks.

Transparency reporting remains a major weakness. Old Mutual Zimbabwe is the only company that previously published a transparency report, but its score declined from a perfect 100% last year to 0%, indicating the absence of a current or updated report. All other companies maintained scores of 0%, continuing the sector-wide lack of public accountability. The absence of transparency reports significantly weakens oversight, limits public trust, and signals misalignment with international best practices.

As in the previous assessment, all companies recorded very low compliance in relation to internal data breach resolution mechanisms. Old Mutual Zimbabwe made limited efforts, scoring 33%, while Zimnat Lion Insurance, Alliance Insurance, and Cell Insurance each maintained scores of 0%. This persistent gap suggests that most insurers lack clear internal procedures for investigating, resolving, and communicating data breaches, posing serious risks to both consumers and regulatory compliance.

Taken together, the current assessment shows incremental improvements over last year, particularly among larger insurers such as Zimnat Lion Insurance and Old Mutual Zimbabwe, which have expanded policy accessibility and improved recognition of data subject rights. However, these gains are undermined by the continued absence of transparency reporting and robust breach-handling frameworks, which remain systemic weaknesses across the sector. Smaller insurers, notably Alliance Insurance and Cell Insurance, continue to operate with minimal or no visible data protection frameworks, despite handling sensitive financial and health-related information. This highlights a significant regulatory and governance gap within the industry. Overall, while progress is evident, Zimbabwe's insurance sector remains partially compliant at best. Without sustained improvements in transparency, third-party data governance, and internal breach resolution, current practices fall short of fully meeting data protection law requirements and international standards, leaving consumers exposed and confidence in the sector weakened.

h. Jubilee Insurance Kenya, Britam Insurance Kenya, ICEA Lion Insurance and CIC Kenya in Kenya



As in the previous assessment period, all insurance companies reviewed in Kenya fully complied with registration requirements under the national data protection framework, each maintaining a perfect score of 100%. This sustained performance reflects a strong and institutionalised commitment to regulatory compliance at the entry level and indicates that registration with the national regulator is now well embedded across the sector.

Insurance companies also continued to demonstrate efforts to maintain accessible privacy policies. ICEA Lion Insurance Kenya and CIC Insurance Kenya lead the sector with scores of 88%. ICEA Lion showed notable improvement, increasing from 75% last year to 88%, suggesting enhancements in the visibility, clarity, or completeness of its privacy policy. CIC Kenya, by contrast, maintained its 88% score, indicating consistency but no further improvement. Jubilee Insurance Kenya and Britam Insurance Kenya followed closely, each maintaining scores of 75%, unchanged from last year. While these scores indicate basic compliance, the lack of progress suggests that accessibility and user-friendliness of privacy policies have largely plateaued for these insurers.

All assessed companies demonstrated observable efforts to respect data subject rights, although performance levels varied. Jubilee Insurance Kenya remains the strongest performer, maintaining a score of 77%, consistent with last year. This reflects a relatively mature framework for informing users about data collection practices and recognising rights such as access and correction. ICEA Lion Insurance Kenya improved its performance, rising from 68% to 73%, indicating progress in pre-collection transparency and user rights recognition. In contrast, CIC Kenya experienced a significant decline, dropping from 76% last year to 52%, suggesting reduced clarity or completeness in disclosures related to data subject rights. This regression raises concerns about sustained compliance and consistency in privacy governance.

All companies were found to share personal data with third parties, but compliance levels in this area remain low across the sector, mirroring last year's findings. ICEA Lion Insurance leads with 38%, improving from 26%, which indicates some progress in disclosing third-party sharing practices. Jubilee Insurance Kenya scored 28%, slightly declining from 30%, while CIC Kenya maintained a low score of 26%. Britam Insurance Kenya recorded the lowest score at 16%, dropping from 26%. These results underscore a persistent weakness in transparency around third-party data transfers, including limited disclosure of recipient categories, data types shared, and safeguards in place, an area of heightened regulatory risk under data protection law.

All companies demonstrated efforts to secure personal data, with performance remaining relatively strong overall. Britam Insurance Kenya continues to lead, maintaining a high score of 83%, unchanged from last year. Jubilee Insurance Kenya improved to 67%, up from 61%, reflecting strengthened technical or organisational safeguards. By contrast, ICEA Lion Insurance's score declined sharply, falling from 78% to 50%, while CIC Kenya also dropped from 61% to 45%.

These declines suggest potential gaps in the consistency or documentation of security measures and highlight the need for ongoing investment in data protection infrastructure and practices.

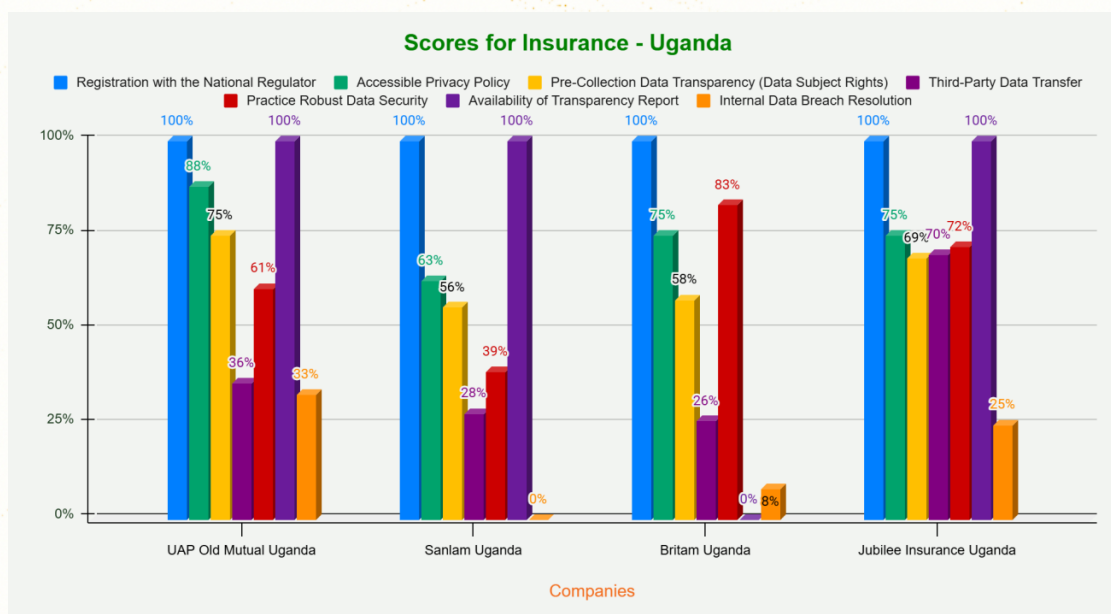
A notable improvement compared to last year is the availability of transparency reports. Jubilee Insurance Kenya, Britam Insurance Kenya, and CIC Kenya each published transparency reports, scoring 100%, a substantial improvement from 0% across the sector last year. This marks a positive step toward greater accountability and public disclosure. However, internal data breach resolution mechanisms remain weak, with little progress since last year. Jubilee Insurance Kenya scored only 17%, declining from 25%, while ICEA Lion Insurance and CIC Kenya both dropped from 8% to 0%. These persistently low scores indicate that most insurers lack clear, fair, and time-bound procedures for managing data breaches and notifying affected individuals, which remains a critical compliance gap.

Overall, the Kenyan insurance sector demonstrates strong commitment to foundational compliance, particularly in registration, privacy policy availability, and data security. Compared to last year, there are notable improvements in transparency reporting and selective gains in data subject rights and third-party disclosure. However, these gains are uneven and offset by regressions in key areas, including third-party data sharing clarity, data security consistency for some firms, and internal breach response mechanisms.

The sector's privacy frameworks reflect the heightened sensitivity of insurance data, including health information for medical underwriting, location data for motor insurance, and detailed risk profiling for actuarial analysis. While insurers show a sophisticated understanding of consent management and data use for pricing and risk assessment, persistent weaknesses in breach handling and third-party transparency continue to undermine full compliance with data protection laws. In sum, compared to last year, Kenya's insurance sector shows incremental but uneven progress. While transparency reporting has improved significantly, internal accountability mechanisms and comprehensive third-party data governance remain underdeveloped, posing ongoing risks to consumer trust and regulatory compliance.

i. UAP Old Mutual Uganda, Sanlam, Britam Uganda and Jubilee Insurance Uganda in Uganda

All assessed insurance companies in Uganda (UAP Old Mutual Uganda, Jubilee Insurance Uganda, Britam Uganda, and Sanlam Uganda) continued to fully comply with registration requirements with the national data protection regulator, each maintaining a perfect score of 100%, unchanged from last year. This sustained performance confirms that regulatory registration is now a baseline compliance requirement within the sector.



Bottom of Form

All companies also demonstrated continued efforts to maintain accessible privacy policies, although performance trends were mixed. UAP Old Mutual Uganda remains the sector leader, maintaining a strong score of 88%, consistent with last year. Britam Uganda and Jubilee Insurance Uganda each scored 75%; while Jubilee maintained its previous score, Britam experienced a decline from 88%, suggesting reduced visibility, clarity, or accessibility of its policy. Sanlam Uganda recorded the lowest score at 63%, representing a notable drop from 88% last year, and indicating a regression in policy accessibility.

Efforts to observe data subject rights improved overall compared to last year. UAP Old Mutual Uganda continued to lead, maintaining a score of 75%, reflecting a relatively mature approach to transparency and rights recognition. Jubilee Insurance Uganda showed notable improvement, increasing from 61% to 69%, while Britam Uganda also improved, rising from 52% to 58%. Sanlam Uganda maintained a score of 56%, showing no progress but also no decline.

These results indicate gradual strengthening of pre-collection transparency and user rights across the sector, though gaps remain in consistency and depth of implementation.

All companies were found to share personal data with third parties, but compliance in this area improved significantly compared to last year. Jubilee Insurance Uganda emerged as the strongest performer, increasing sharply from 24% to 70%, reflecting clearer disclosure and stronger safeguards around third-party access. UAP Old Mutual Uganda improved from 16% to 36%, Sanlam Uganda from 26% to 28%, and Britam Uganda from 16% to 26%.

Despite these gains, third-party data sharing remains a moderate-risk area, as disclosures are still often general and lack specificity regarding data types shared, safeguards applied, and law enforcement access conditions.

All companies demonstrated continued efforts to secure personal data, though performance shifted compared to last year. Britam Uganda remains the strongest performer, maintaining a high score of 83%. Jubilee Insurance Uganda declined to 72%, down from 83%, while UAP Old Mutual Uganda dropped to 61%, from 78%. Sanlam Uganda remained the weakest performer, maintaining a low score of 39%. These changes suggest that while baseline security measures remain in place, some insurers may not be consistently updating or documenting their technical and organisational safeguards.

A major improvement over last year is the availability of transparency reports. UAP Old Mutual Uganda, Jubilee Insurance Uganda, and Sanlam Uganda each published transparency reports, scoring 100%, compared to 0% across the sector last year. Britam Uganda remains the only insurer without a transparency report, maintaining a score of 0%. However, internal data breach resolution mechanisms remain weak, despite slight improvements. UAP Old Mutual Uganda leads with 33%, up from 17%, followed by Jubilee Insurance Uganda at 25%, also up from 17%. Britam Uganda improved marginally to 8%, from 0%, while Sanlam Uganda remained at 0%. These low scores indicate persistent deficiencies in clear reporting channels, investigation timelines, user notification, and impartial resolution procedures.

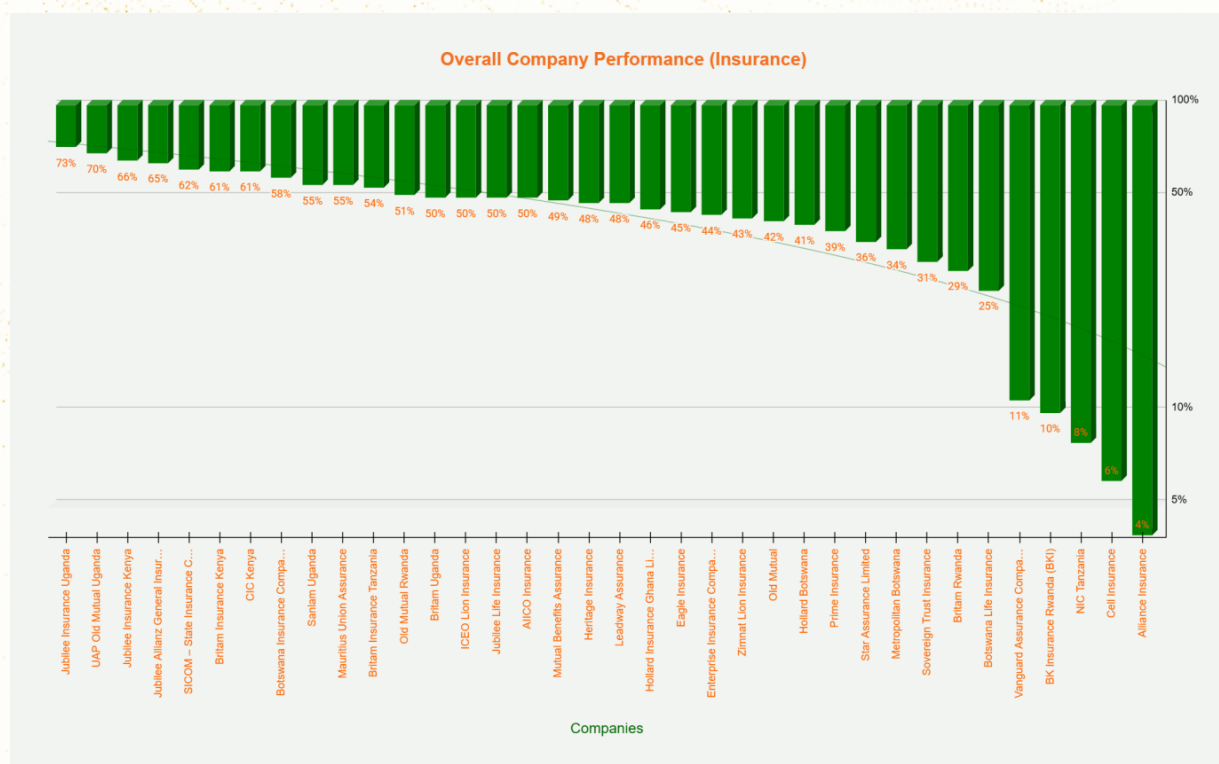
The insurance sector in Uganda demonstrates a relatively higher level of compliance compared to many other sectors, particularly in registration, policy availability, and gradual improvements in transparency reporting and third-party disclosure. UAP Old Mutual Uganda and Jubilee Insurance Uganda emerge as stronger performers, combining accessible privacy policies with moderate security, improved transparency, and clearer third-party data practices. UAP's privacy policy is highly visible, readable, and user-friendly, with a Hemingway readability score of 10, and is supported by an available transparency report. The policy clearly outlines data collection purposes, categories of data collected, lawful retention periods, behavioural marketing with opt-out options, and core data subject rights including access, correction, deletion, and complaint lodging. However, its approach to data breach management remains largely reactive, relying on statutory requirements rather than defined internal standards, with no clear timelines or investigative procedures.

Jubilee Insurance Uganda recorded the highest score on third-party data transfer, largely due to strict consent-based sharing practices and its refusal to share data with advertisers. Nonetheless, its limited reporting channels and lack of detailed breach-handling procedures constrain full compliance.

Britam Uganda, while strong on data security, continues to underperform on transparency and breach resolution. Its absence of a transparency report and lack of clear internal breach-handling procedures pose ongoing compliance risks. Sanlam Uganda, despite having a transparency report, remains weak in data security and internal breach resolution, reflecting uneven implementation of privacy safeguards.

Compared to last year, Uganda's insurance sector shows measurable progress, particularly in third-party data transfer disclosures and transparency reporting. However, internal data breach resolution remains a systemic weakness, and recent declines in policy accessibility and data security for some firms suggest the need for renewed focus on sustaining compliance. In sum, while foundational compliance is strong and several indicators have improved, effective breach management, consistent security practices, and clearer accountability mechanisms remain critical gaps that must be addressed to ensure full alignment with data protection laws and to strengthen consumer trust.

3.4.5.3 Comparison of companies/entities within the sector



High-Performing Jurisdictions: Emerging Compliance Leaders and Trajectories

Uganda, Kenya, and Mauritius now emerge as the strongest-performing jurisdictions in the insurance sector, with several companies recording clear year-on-year improvements and moving closer to meaningful compliance with data protection laws.

Uganda shows the most pronounced upward trajectory. Jubilee Insurance Uganda (73%) and UAP Old Mutual Uganda (70%) now lead the sector, representing a significant improvement from last year, when leading scores ranged between 51% and 53%. This progress suggests stronger internalisation of privacy governance, improved data security controls, and better recognition of data subject rights. Sanlam Uganda (55%) and Britam Uganda (50%) also show modest improvement, indicating that compliance efforts are becoming more evenly distributed across the market.

Kenya maintains its position as a relatively strong performer, with Jubilee Insurance Kenya (66%), Britam Insurance Kenya (61%), and CIC Kenya (61%) all improving from last year's narrow band around 51–52%. These gains indicate more mature privacy practices, particularly in policy accessibility and security safeguards. However, while Kenya's insurers are progressing, their scores still reflect partial rather than comprehensive compliance.

Mauritius continues to demonstrate relatively advanced performance compared to many peers. Jubilee Allianz General Insurance Mauritius Ltd (65%) and SICOM (62%) have improved from last year's low-60% and low-40% ranges, respectively. Mauritius Union Assurance (55%) remains stable, while Eagle Insurance (45%) shows incremental progress. These results suggest that Mauritian insurers are strengthening baseline compliance but continue to face gaps in accountability-driven obligations.

Despite these positive trends, it is notable that only two companies exceed 70%, indicating that even in high-performing jurisdictions, full compliance with data protection laws has not yet been achieved.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

Several jurisdictions continue to experience systemic compliance challenges, with some companies showing stagnation or regression compared to last year.

Zimbabwe remains the most concerning case. While Zimnat Lion Insurance (43%) and Old Mutual Zimbabwe (42%) show marginal improvement from last year's lows, Cell Insurance (6%) and Alliance Insurance (4%) remain effectively non-compliant. These persistently low scores indicate an absence of basic privacy governance, exposing companies to significant legal and reputational risks.

Rwanda also presents ongoing challenges at the lower end. Britam Rwanda (29%) and BK Insurance Rwanda (10%) remain among the weakest performers, showing little improvement from last year. This suggests limited institutional capacity or prioritisation of data protection compliance.

Ghana shows a widening performance gap. While Hollard Insurance Ghana Limited (46%) and Enterprise Insurance Company Limited (44%) perform moderately, Vanguard Assurance Company Limited (11%) remains extremely weak, reflecting systemic deficiencies in privacy practices.

In Tanzania, NIC Tanzania (8%) continues to score very poorly, indicating regression or stagnation despite broader improvements in the sector.

These low-performing jurisdictions demonstrate entrenched compliance failures, where privacy obligations are either poorly understood or inadequately enforced.

Key Cross-Cutting Implications

Several cross-cutting insights emerge across the insurance sector. First, overall performance has improved year-on-year, with more companies now scoring above 50% than in the previous assessment. This suggests growing awareness of data protection obligations, particularly in jurisdictions with more active regulatory environments.

Second, improvements remain uneven and largely concentrated in baseline measures such as privacy policy availability and data security. High-risk accountability mechanisms, particularly transparency reporting, third-party data governance, and internal data breach resolution remain weak across all performance tiers.

Third, jurisdictional context matters, but corporate governance and institutional commitment are decisive. Significant performance variation within the same country indicates that compliance outcomes depend as much on internal leadership and risk culture as on national legal frameworks.

In conclusion, while the insurance sector shows clearer signs of maturation compared to last year, compliance with data protection laws remains partial and fragile. Without deeper investment in accountability, breach preparedness, and third-party oversight, current gains risk plateauing, leaving consumers exposed to privacy and data protection risks despite measurable progress.

3.4.6 e – Government Sector Analysis

3.4.6.1 Overview of the sector and data collectors evaluated

The e-government sector across East, Southern, and parts of West Africa continues to expand rapidly, driven by the increasing use of digital technologies to improve public service delivery, operational efficiency, and administrative transparency. Governments are deploying digital platforms to deliver essential services such as tax administration, civil registration, public health systems, social protection, immigration services, and land management, with the aim of improving accessibility and responsiveness to citizens.

This digital transformation, however, has significantly increased the volume and sensitivity of personal data collected by public institutions, raising critical concerns around privacy, data protection, and accountability. The latest scorecard assessment reveals that while e-government adoption is accelerating, privacy practices and compliance with data protection laws remain uneven across countries and platforms.

The assessment highlights inconsistent implementation of data protection safeguards, with wide disparities in transparency, data security, third-party data sharing, and breach response mechanisms. In Uganda, e-government platforms continue to face significant transparency challenges. Many services provide limited information about the categories of data collected, the purposes of processing, retention periods, and third-party access. While Uganda has made progress in digitising public services, insufficient public-facing disclosures undermine compliance with data protection standards and weaken public trust. Kenya remains one of the more advanced jurisdictions in terms of digital government infrastructure and legal frameworks. However, the assessment identifies persistent risks associated with extensive reliance on third-party service providers. Inadequate disclosure of vendor relationships and weak oversight mechanisms heighten the risk of data misuse. Strengthening contractual safeguards, public disclosure, and accountability of third-party processors remains a priority.

In Mauritius, relatively mature e-government systems coexist with ongoing data security concerns. Despite a well-established data protection law, gaps remain in the implementation of technical safeguards, including secure storage, transmission controls, and routine security audits. These weaknesses expose government systems to potential breaches and unauthorised access. Zimbabwe continues to face structural challenges in both the development and protection of

e-government services. Many platforms remain underdeveloped, and existing data protection legislation is outdated, limiting effective enforcement. The lack of modern security infrastructure and regulatory clarity poses heightened risks to citizens' personal data.

Rwanda has made notable strides in digital governance and service integration. However, the assessment finds ongoing gaps in data transparency and user awareness, particularly around how personal data is collected, shared, and retained. While policies exist, clearer communication and stronger technical security measures are needed to ensure full compliance and public confidence. In Tanzania, the e-government sector remains in a developmental phase, with limited infrastructure and evolving regulatory frameworks. Weak data protection safeguards, unclear compliance obligations, and insufficient security controls present significant privacy risks, particularly as digital service uptake increases.

The inclusion of Nigeria, Ghana, and Botswana in the current assessment expands the regional perspective and underscores similar systemic challenges. In Nigeria, e-government platforms operate within a rapidly evolving regulatory environment following the enactment of the Nigeria Data Protection Act. While some platforms demonstrate improved policy availability and registration compliance, implementation gaps persist, particularly in transparency reporting, breach response mechanisms, and control over third-party data processors. Ghana shows moderate progress, supported by an established data protection authority and registration regime. However, the assessment reveals weak enforcement and limited transparency across many e-government platforms, with insufficient disclosure of data practices and underdeveloped internal breach-handling mechanisms. In Botswana, digital government initiatives are expanding, but privacy compliance remains uneven. While some platforms demonstrate strong transparency and policy accessibility, others lack clear privacy notices, defined data subject rights, and structured breach response frameworks, limiting effective protection of citizen data.

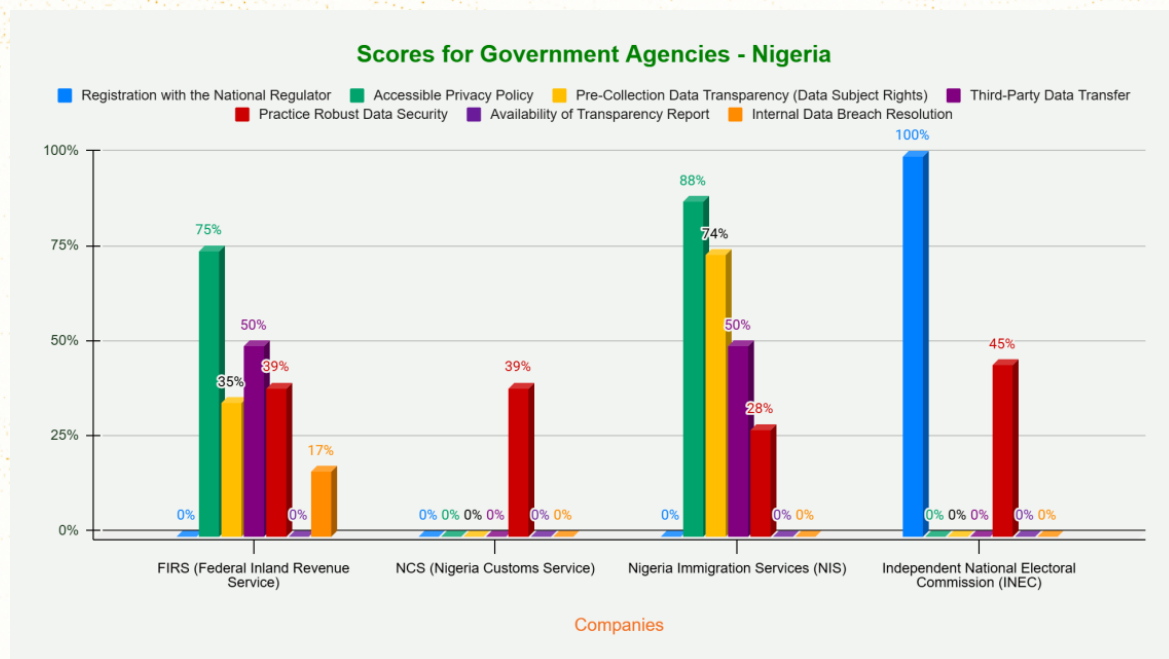
Across all assessed countries, a common pattern emerges: the expansion of e-government services has outpaced the consistent implementation of robust data protection safeguards. While countries such as Kenya, Mauritius, Nigeria, and Ghana have enacted data protection laws, enforcement remains inconsistent, and institutional capacity varies widely. In contrast, countries like Zimbabwe and Tanzania continue to face foundational legal and infrastructural gaps. E-government initiatives across the region hold substantial promise for improving public service delivery and citizen engagement. However, the assessment makes clear that privacy and data protection must be treated as core governance priorities, not secondary considerations.

3.4.6.2 Analysis of compliance with each criterion

This assessment is based on a total of 36 entities, with four (4) entities selected for evaluation from each participating country, namely: Federal Inland Revenue Service, Nigeria Customs Service, Nigeria Immigration Service and Independent National Electoral Commission from Nigeria; Ghana Revenue Authority, Passport Office, SSNIT Self Service Portal (Social Security and National Insurance Trust) and Ghana Immigration Services from Ghana; Botswana Unified Revenue Service, Botswana Communications Regulatory Authority, 1Gov e-Services Portal and Independent Electoral Commission of Botswana from Botswana; IremboGov, RSSB(Rwanda Social Security Board), Rwanda Revenue Authority(RRA) and Rwanda Information Society Authority from Rwanda; e-Immigration Tanzania, TCAA (Tanzania Civil Aviation Authority), TCRA (Tanzania Communications Regulatory Authority) and Tanzania Work Permit Application Portal from Tanzania; Mauritius Revenue Authority (MRA), MauPass(Mauritius Personal Access), ICTA (Information and Communication Technology Authority) and Passport & Immigration Office Mauritius from Mauritius; e-Visa Zimbabwe, NSSA (National Social Security Authority) self service portal, Zimbabwe Revenue Authority(ZRA) and eGP System Zimbabwe (Electronic Government procurement System) from Zimbabwe; e-Citizen, Huduma, Kenya Revenue Authority (KRA) and ETA Kenya (Electronic Travel Authorisation – Kenya); and Immigration Uganda, NIRA, Electoral Commission Uganda and UBOS (Uganda Bureau of Statistics).

a. Federal Inland Revenue Service, Nigeria Customs Service, Nigeria Immigration Service and Independent National Electoral Commission in Nigeria

The assessment reveals significant disparities in data protection compliance among the four agencies. Only the Independent National Electoral Commission (INEC) achieved full compliance (100%) with registration requirements with the national data protection regulator. All other entities scored 0% in this category, indicating a fundamental compliance gap that exposes them to regulatory risk and weakens institutional accountability.



In terms of accessibility of privacy policies, only the Nigeria Immigration Service (NIS) (88%) and the Federal Inland Revenue Service (FIRS) (75%) demonstrated meaningful effort. The absence of accessible privacy policies within the remaining entities reflects a lack of transparency and limits public understanding of how personal data is processed, contrary to core data protection principles.

Similarly, compliance with data subject rights was limited to NIS (74%) and FIRS (35%). The other agencies showed no measurable effort in this area. Given that data subject rights are central to modern data protection frameworks, the low scores indicate systemic weaknesses in empowering individuals to access, correct, or challenge the use of their personal data.

All four entities engage in third-party data sharing. However, compliance levels in this area remain critically low. NIS and FIRS led with only 50% each, while the Nigeria Customs Service (NCS) and INEC scored 0%. This is particularly concerning because third-party transfers especially involving sensitive categories such as immigration, tax, customs, and electoral data require clear legal bases, safeguards, and transparency mechanisms under data protection laws. Regarding data security safeguards, all entities demonstrated some effort. INEC scored highest at 45%, followed by FIRS and NCS (39% each), while NIS scored 28%. Although these efforts suggest awareness of security obligations, the relatively low percentages indicate that technical and organizational measures remain underdeveloped and may not meet the threshold of “appropriate security” required under data protection legislation.

Notably, none of the entities publishes transparency reports or maintains a clear internal data breach resolution mechanism. The absence of documented breach response frameworks and public accountability reporting significantly undermines compliance with statutory obligations relating to breach notification, risk mitigation, and institutional transparency. Overall, while pockets of progress exist, the findings point to fragmented compliance efforts and limited institutionalization of data protection governance across the agencies.

Nigeria Immigration Service (NIS) demonstrates the strongest overall privacy compliance profile among the assessed agencies. Its privacy framework reflects a structured and detailed approach tailored to the complex nature of immigration data processing. The Service provides comprehensive contact information, including passport offices, visa centers, and dedicated communication channels. It clearly catalogs the extensive categories of personal data collected identity documents, biometric data, travel history, employment information, visa records, and security screening data and links these categories to defined processing purposes such as immigration control, visa processing, border management, and international cooperation. NIS also provides comparatively strong transparency on data retention, aligning retention periods with legal and operational requirements. It discloses third-party sharing arrangements, including transfers to international immigration authorities, security agencies, airlines, and diplomatic missions, while referencing the legal bases and safeguards for such disclosures. Furthermore, NIS operationalizes data subject rights through defined procedures for access, correction, and complaint escalation. It also clarifies circumstances under which law enforcement and security agencies may access immigration data, referencing applicable legal frameworks and oversight mechanisms. However, despite these strengths, the absence of full regulatory registration compliance and formalized breach response transparency indicates that its governance structure still requires strengthening to achieve comprehensive legal alignment.

Independent National Electoral Commission (INEC) demonstrates strong regulatory alignment in registration compliance (100%), positioning it as the most compliant agency in this specific legal obligation. Its privacy policies reflect an understanding of the unique sensitivities associated with electoral data. The Commission clearly outlines categories of voter data collected and explains processing purposes, including voter registration, election administration, constituency delimitation, and candidate verification. INEC provides transparency regarding retention periods in line with electoral law and explains data-sharing arrangements, particularly the provision of voter registration data to political parties for legitimate electoral purposes. It also implements electoral-context data subject rights, such as record access, correction, and voter transfer between constituencies. However, despite strong performance in regulatory registration, INEC scored 0% in third-party data-sharing compliance and demonstrated limited security safeguards (45%). These gaps create potential vulnerabilities in the handling of highly sensitive voter data and may expose the Commission to legal and reputational risk if not addressed through clearer safeguards and documented transfer controls.

Federal Inland Revenue Service (FIRS) demonstrates moderate compliance. It provides accessible privacy information and basic contact channels and outlines general categories of taxpayer data collected for tax assessment, enforcement, and compliance purposes. The Service acknowledges data sharing with other government agencies and implements standard taxpayer rights, including access and correction procedures. However, its lower score in data subject rights (35%) indicates partial rather than comprehensive implementation. Although FIRS scored relatively higher in third-party sharing (50%) and security safeguards (39%) compared to some agencies, these figures remain below optimal compliance standards. Given the sensitivity of financial and taxpayer data, stronger governance, clearer legal bases for transfers, and more robust technical safeguards are necessary to ensure full alignment with data protection requirements.

Nigeria Customs Service (NCS) faces significant compliance challenges. Despite processing large volumes of personal and commercial data through import/export operations, border control, and trade facilitation, accessible privacy disclosures remain limited. Its 0% score in both regulatory registration and third-party sharing compliance highlights serious governance deficiencies. The limited transparency creates a gap between the scale of data processing activities and the safeguards publicly articulated to protect such data. This disconnect increases legal exposure, reduces stakeholder trust, and heightens the risk of non-compliance with statutory transparency, accountability, and lawful processing obligations.

The assessment indicates that data protection compliance across the agencies remains uneven and largely procedural rather than systemic. While NIS and INEC demonstrate comparatively stronger frameworks in specific areas, all entities exhibit structural weaknesses particularly in third-party data governance, breach response mechanisms, transparency reporting, and comprehensive regulatory alignment.

To achieve full compliance with data protection laws, agencies must move beyond policy publication toward institutionalized data governance structures, including:

- Formal registration with the regulator
- Documented data-sharing agreements with safeguards
- Comprehensive data subject rights implementation
- Structured breach detection and notification frameworks
- Regular transparency reporting
- Stronger technical and organizational security measures

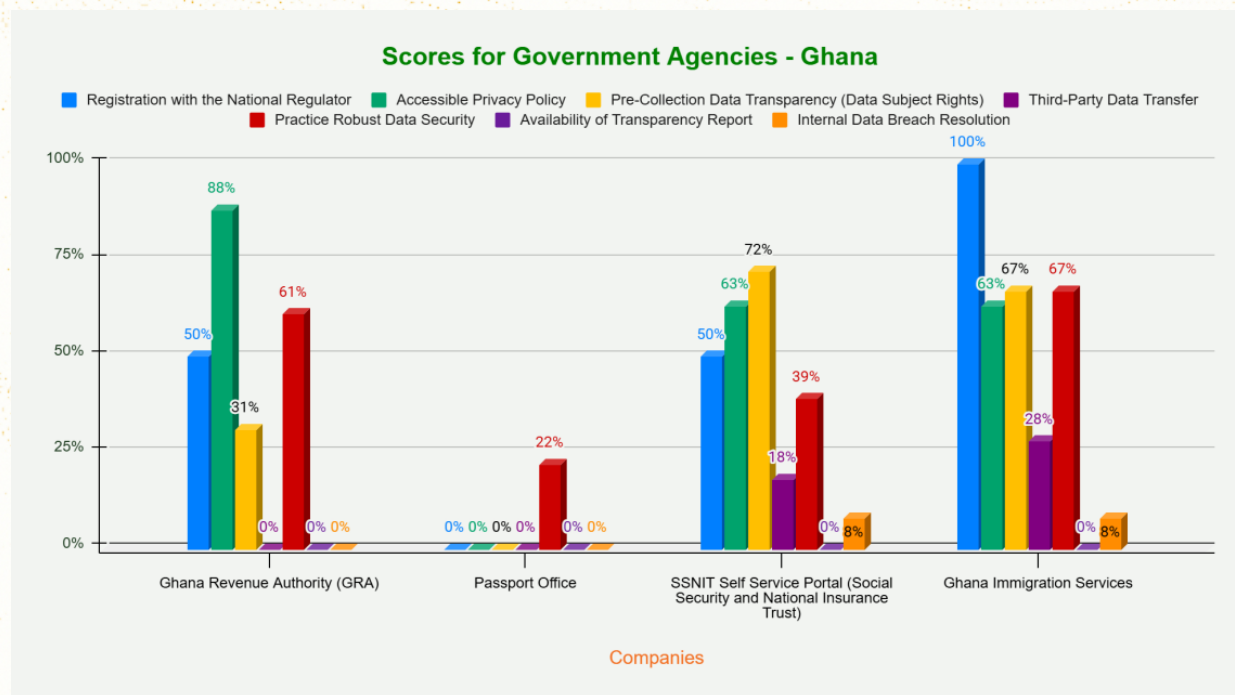
Without these measures, privacy practices will remain fragmented, exposing institutions to regulatory sanctions, operational vulnerabilities, and diminished public trust.

b. Ghana Revenue Authority, Passport Office, SSNIT Self Service Portal (Social Security and National Insurance Trust) and Ghana Immigration Services in

Ghana

The assessment of Ghana's key e-government institutions reveals uneven and largely partial compliance with data protection obligations. While some agencies demonstrate structured efforts in specific areas, systemic weaknesses persist particularly in third-party data governance, breach response mechanisms, and transparency reporting.

Compliance with registration requirements shows a mixed picture. Ghana Immigration Services (GIS) leads with full compliance (100%) and maintains an active registration valid until November 26, 2025. By contrast, the Ghana Revenue Authority (GRA) and SSNIT Self Service Portal each scored 50%, reflecting expired certifications (August 13, 2025, and September 20, 2024, respectively). The Passport Office scored 0%, having never registered.



From a compliance perspective, expired or absent registration undermines institutional accountability and may constitute a direct breach of statutory obligations under Ghana's data protection framework. Registration is a foundational requirement; failure to maintain active certification weakens regulatory oversight and exposes agencies to legal and reputational risks.

Efforts to provide accessible privacy policies also vary significantly. GRA leads (88%) with the most structured and visible policy. SSNIT and GIS follow (63% each), while the Passport Office has no publicly available privacy policy (0%). Although Immigration's policy exceeds 1,900 words suggesting detail and substantive content readability scores (Hemingway grades 11–12) indicate bureaucratic and difficult-to-read language across agencies. The absence of any policy at the Passport Office represents a serious transparency failure, effectively denying citizens notice of how their data is processed. In practical terms, limited accessibility or absence of policies undermines the principle of transparency and informed consent, core pillars of data protection law.

Compliance with data subject rights demonstrates relative strength in some institutions but remains incomplete overall. SSNIT leads (72%), followed by GIS (67%), GRA (31%), and the Passport Office (0%).

- SSNIT clearly outlines data categories, processing purposes, and limited third-party sharing (NIA and GHIPSS), and recognizes core user rights. However, vague retention timelines, absence of complaint mechanisms, and silence on law enforcement access weaken its compliance posture.
- GIS provides comprehensive contact details, extensive data categories, and acknowledges rights such as access, rectification, and erasure. Nonetheless, vague retention standards, absence of structured complaint channels, and provisions for targeted marketing introduce compliance gaps.
- GRA offers only basic information on purposes and contact details, without clarity on retention, third-party sharing safeguards, complaint processes, or law enforcement access.
- Passport Office provides no privacy framework at all.

The variation reflects inconsistent institutionalization of data subject rights. Where complaint mechanisms, retention clarity, and lawful access safeguards are absent, agencies risk failing statutory obligations concerning fairness, purpose limitation, and accountability.

All entities share personal data with third parties, yet compliance in this area is critically low. GIS leads with only 28%, followed by SSNIT (18%), while GRA and the Passport Office scored 0%.

- GRA's policy omits essential disclosures on third-party sharing, law enforcement access, data categories transferred, and breach reporting procedures indicating non-compliance with basic transparency requirements.

- SSNIT specifies sharing with NIA and GHIPSS for identity verification and payment processing, excluding advertisers and analytics platforms. However, it fails to clarify data categories transferred, safeguards, or breach procedures.
- GIS discloses sharing with MDAs, SOEs, MMDAs, and payment processors, and allows law enforcement access when reasonably requested. Yet, procedural safeguards and breach notification processes remain undefined.
- Passport Office provides no disclosure at all.

Given that data transfers pose heightened risks especially in immigration, taxation, and social security contexts the low compliance levels indicate significant exposure to unlawful or inadequately safeguarded processing. Under data protection law, third-party transfers require clear legal bases, defined safeguards, and accountability mechanisms, which are presently insufficient.

All institutions demonstrate some technical security measures, though implementation quality varies.

- GIS leads (67%) with an A SSL rating, partial security header implementation (28%), and policy references to protective measures.
- GRA follows (61%) with an A SSL rating but failing security headers (F).
- SSNIT scored 39% (B SSL rating, failing security headers).
- Passport Office scored lowest (22%) with a B SSL rating and no policy reference to personal data security.

While SSL ratings indicate encrypted connections, failing security headers and limited policy specificity suggest incomplete technical and organizational safeguards. This gap may fall short of the legal requirement for “appropriate security measures,” particularly given the sensitivity of financial, immigration, and identity data processed.

None of the assessed agencies (GRA, Passport Office, SSNIT, or GIS) has published a transparency report since 2024, resulting in 0% scores across the board. The absence of transparency reporting weakens public accountability and obscures how frequently data is shared, accessed by law enforcement, or subjected to breaches. This limits oversight and undermines public trust.

Internal breach resolution mechanisms are largely absent.

- SSNIT and GIS scored 8% each, referencing general security measures but lacking defined procedures, reporting timelines, user notification protocols, or independent review safeguards.
- GRA and Passport Office scored 0%, providing no guidance at all.

Without structured breach detection, investigation, and notification procedures, agencies risk non-compliance with statutory breach notification requirements. This also increases the likelihood of delayed or inadequate responses to incidents, potentially exacerbating harm to data subjects.

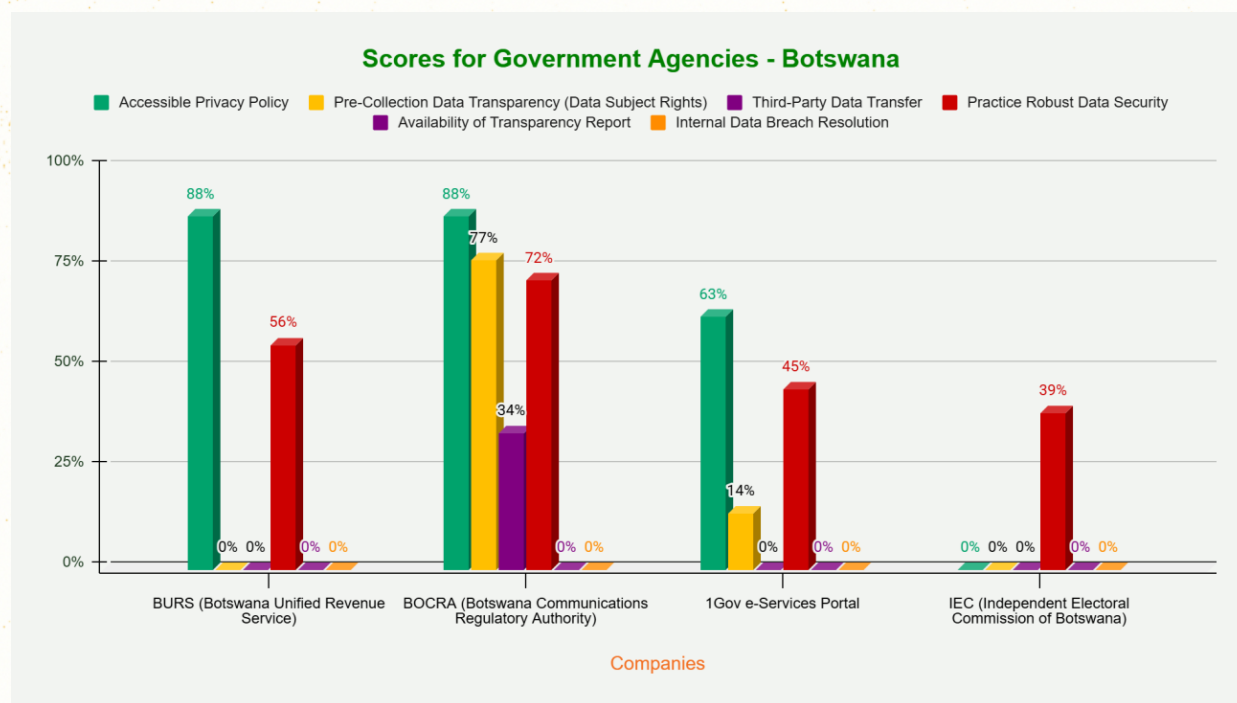
The assessment demonstrates that Ghana’s public sector agencies are at different stages of privacy maturity, but none achieves comprehensive compliance across all indicators. Key systemic weaknesses include:

- Expired or absent regulatory registration
- Limited clarity in third-party data transfer safeguards
- Vague retention policies
- Absence of structured complaint and redress mechanisms
- Lack of transparency reporting
- Weak or undocumented breach response frameworks

Although Ghana Immigration Services shows comparatively stronger overall performance, and SSNIT demonstrates notable effort in data subject rights, compliance remains fragmented rather than institutionalized. To achieve full alignment with data protection laws, agencies must move beyond partial policy disclosures and adopt integrated privacy governance frameworks that embed accountability, transparency, and risk management into operational practice. Without these reforms, current privacy practices remain legally vulnerable and insufficient to fully protect citizens’ personal data.

C. *Botswana Unified Revenue Service, Botswana Communications Regulatory Authority, 1Gov e-Services Portal and Independent Electoral Commission of Botswana in Botswana*

The assessment reveals uneven and generally low levels of compliance with core data protection principles among Botswana's key public institutions: Botswana Unified Revenue Service (BURS), Botswana Communications Regulatory Authority (BOCRA), 1Gov e-Services Portal, and Independent Electoral Commission of Botswana (IEC). While some progress is observable, particularly in policy publication and stated security commitments, significant structural deficiencies remain in transparency, data subject rights, third-party accountability, and breach response mechanisms.



Demonstrable efforts to provide accessible privacy policies were strongest at BOCRA and BURS (both scoring 88%), followed by the 1Gov e-Services Portal (63%), while the IEC scored 0%. However, accessibility alone does not equate to compliance. Under the Botswana Data Protection Act, transparency requires that data controllers clearly inform data subjects about: Categories of personal data collected, lawful basis and purposes of processing, retention periods, data subject rights, third-party recipients and complaint and redress mechanisms.

Although BURS has an accessible privacy policy, the content is vague. It does not clearly define categories of data collected, specific purposes, retention timelines, or breach reporting procedures. This undermines the principle of informed consent and transparency. The absence of specificity limits accountability and may place the institution in partial non-compliance with statutory disclosure requirements.

BOCRA Demonstrates stronger alignment with transparency obligations. Its policy specifies data categories, purposes, contact details, and acknowledges data subject rights. It explicitly references compliance with the Data Protection Act. However, the absence of clearly defined retention periods and breach notification timelines suggests incomplete compliance.

While a policy exists for 1Gov e-Services Portal, it is broadly framed and lacks substantive detail. It permits marketing uses and third-party sharing without specifying recipients, creating risks of function creep and opaque processing practices.

The absence of a privacy policy for the IEC represents a fundamental transparency failure. For an institution handling highly sensitive voter data, this gap raises serious concerns about lawfulness, fairness, and accountability.

BOCRA scored highest (77%) in recognizing data subject rights, followed distantly by 1Gov (14%), while BURS and IEC scored 0%. The Data Protection Act grants individuals rights including access, rectification, erasure, restriction of processing, and the right to lodge complaints. By explicitly referencing these rights and complaint procedures, BOCRA demonstrates partial alignment with statutory requirements. This enhances accountability and empowers citizens to exercise control over their personal information. The failure by BURS and 1Gov to clearly articulate these rights significantly weakens legal compliance. Without procedural clarity, data subjects may be unaware of how to request access, correction, or deletion. This creates a compliance gap and increases institutional liability. The absence of any documented

rights framework in respect of IEC suggests a complete lack of procedural safeguards for voters, which may be incompatible with statutory obligations.

All entities share personal data with third parties, yet compliance levels were critically low. BOCRA led with 34%, while all others scored 0%.

Third-party sharing represents one of the highest-risk areas under data protection law. Compliance requires: Identification of recipients or categories of recipients, clear lawful basis for sharing, safeguards through contractual controls and restrictions on onward transfer. BOCRA limits sharing to government bodies, service providers, and legal proceedings, reflecting some degree of necessity and proportionality. However, the absence of detailed safeguards or contractual transparency remains a weakness. Both BURS and 1Gov permit sharing with advertisers without identifying recipients. This creates heightened risk of misuse, profiling, or unauthorized secondary use. The lack of disclosure undermines transparency and could constitute non-compliance with accountability principles. IEC that has no policy disclosure, citizens have no visibility into whether or how voter data is shared. Collectively, these findings suggest systemic weaknesses in third-party governance frameworks across institutions.

Demonstrable efforts to ensure data security were observed across all institutions, with BOCRA scoring highest (72%), followed by BURS (56%), 1Gov (45%), and IEC (39%). BOCRA specifies encryption, audits, and access controls, indicating relatively mature security governance. BURS and 1Gov reference “security measures” but lack specificity, making it difficult to assess adequacy or compliance with technical and organizational safeguard requirements.

IEC with no publicly articulated safeguards, voter data security remains opaque and potentially vulnerable. Security transparency is a core accountability requirement. Generic statements without demonstrable controls weaken institutional credibility and public trust.

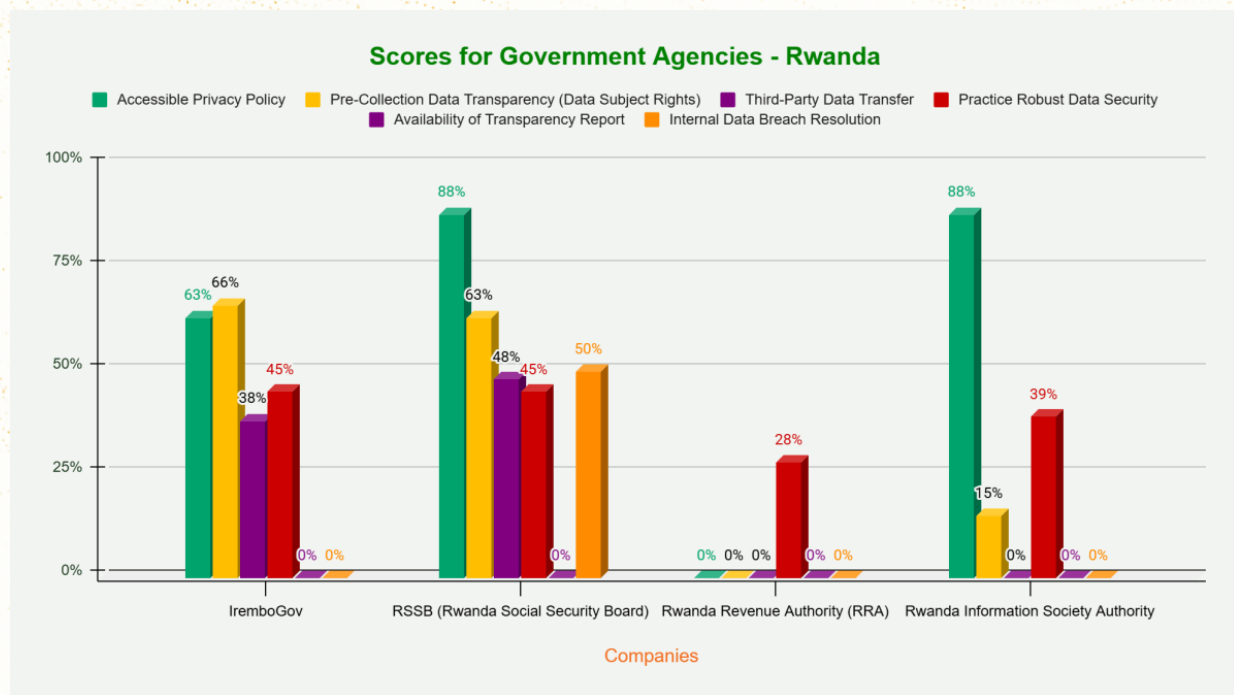
All entities lack publicly available transparency reports and fail to demonstrate internal data breach resolution mechanisms. This represents a critical compliance gap. The Data Protection Act requires timely notification of breaches to the regulator and, where applicable, affected individuals. The absence of defined reporting procedures, timelines, or internal escalation protocols increases: Legal exposure, reputational risk and citizen vulnerability in the event of unauthorized access. Without breach response frameworks, even institutions with stronger security controls remain operationally non-compliant.

BOCRA emerges as the strongest performer, demonstrating meaningful alignment with transparency, rights recognition, and security safeguards. Nonetheless, its compliance remains incomplete due to undefined retention periods and breach notification procedures. BURS and 1Gov e-Services Portal exhibit partial compliance through policy publication but fail to meet core accountability and rights-based standards. IEC demonstrates a systemic compliance failure, lacking even foundational transparency measures despite managing highly sensitive voter data. The findings indicate that Botswana’s public sector institutions are at varying stages of data protection maturity, with most lacking fully operational compliance frameworks. The weaknesses observed suggest: Inadequate internal governance structures for data protection, weak enforcement or oversight mechanisms, limited integration of privacy-by-design principles and potential exposure to legal, reputational, and cybersecurity risks.

Given the volume and sensitivity of citizen data processed, tax records, communications data, identity information, and voter registration data the current compliance gaps may undermine public trust and institutional legitimacy. While incremental progress is evident, particularly at BOCRA systemic improvements are urgently required. To achieve substantive compliance with the Botswana Data Protection Act, these institutions must: Enhance transparency and specificity in privacy notices, operationalize data subject rights procedures, strengthen third-party governance and contractual safeguards, establish formal breach detection and notification frameworks and publish transparency and accountability reports. Without these reforms, government data controllers remain exposed to compliance risks, and citizens remain inadequately protected in the digital governance environment.

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

In 2025, accessibility of privacy policies remains strongest at RSSB and RISA, both maintaining scores of 88% unchanged from 2024. Their policies are publicly available, relatively readable, and sufficiently detailed to meet baseline transparency standards. By contrast, IremboGov’s score declined from 88% in 2024 to 63% in 2025. This decline is not due to lack of substantive content but rather reduced visibility and accessibility of the policy to users, which undermines practical transparency. RRA continues to score 0%, as it does not provide a publicly accessible privacy policy. From a compliance perspective, the absence of a privacy policy constitutes a fundamental breach of transparency obligations under data protection law. Even where policies exist, reduced accessibility weakens informed consent and fair processing standards.



With respect to pre-collection transparency and data subject rights, the 2025 assessment reveals moderate improvement for some entities but significant regression for others. IremboGov leads with a score of 66%, up from 54% in 2024, reflecting clearer articulation of data categories, purposes of processing, and recognition of certain user rights. RSSB follows closely at 63%, a slight improvement from 60% last year, demonstrating continued effort to describe data types and processing purposes. However, both entities still lack fully developed complaint mechanisms, detailed deletion procedures, and explicit regulatory recourse pathways, which limits the enforceability of user rights in practice. RISA's performance declined sharply from 40% in 2024 to 15% in 2025, indicating a substantial reduction in transparency concerning user rights and retention practices. RRA remains at 0 percent, providing no visible pre-collection disclosures.

The uneven performance in this domain suggests that while awareness of data subject rights is growing in certain institutions, rights realization mechanisms remain underdeveloped and inconsistent across the sector.

Third-party data sharing remains an area of high risk and uneven compliance. In 2025, RSSB significantly improved its score from 10% to 48% by identifying categories of third-party recipients, such as government bodies and financial institutions, and clarifying that processing occurs under its instructions. IremboGov also improved from 10% to 38%, disclosing categories of service providers and affiliates. However, both entities fail to specify the exact types of personal data shared or provide sufficiently detailed safeguards governing these transfers. RISA experienced the most dramatic regression, dropping from 60% in 2024 to 0% in 2025, indicating either removal or dilution of previously disclosed third-party safeguards. RRA again scores 0% due to the absence of a policy framework addressing transfers. These findings are particularly significant because third-party transfers often trigger heightened accountability and lawful processing requirements. Limited disclosure in this area increases legal exposure and reduces public confidence in data governance practices.

Regarding technical and organizational security measures, all four entities maintain strong SSL encryption ratings, demonstrating effective protection of personal data in transit. However, website security header implementation remains uniformly weak, with predominantly failing scores, indicating insufficient deployment of additional HTTP security protections. In terms of overall security disclosure and implementation, IremboGov and RSSB each scored 45%, unchanged from 2024. RISA declined from 56% to 39%, while RRA improved marginally from 22% to 28% but continues to lag significantly behind.

Although encryption standards are commendable, vague policy statements and weak supplementary technical safeguards suggest limited progress toward comprehensive privacy-by-design implementation. Strong encryption alone is insufficient to demonstrate full compliance with risk-based security obligations.

Accountability mechanisms remain the weakest area across all entities. As in 2024, none of the assessed institutions has published a transparency report. Structured internal data breach resolution procedures are not publicly documented. RSSB references breach notification but does not specify timelines or procedural steps, while the remaining entities provide little to no information regarding breach handling. The absence of defined breach governance frameworks con-

stitutes a significant compliance vulnerability, as timely notification, documentation, and remediation processes are core requirements under modern data protection regimes. The continued failure to institutionalize transparency reporting and breach management indicates that accountability mechanisms have not matured alongside policy development.

Overall, the 2025 assessment demonstrates incremental but uneven progress. RSSB and IremboGov show measurable improvement in areas such as data subject rights and third-party disclosure, suggesting gradual strengthening of internal compliance awareness. However, this progress is offset by RISA's marked regression and RRA's continued structural non-compliance. Encryption standards remain consistently strong, yet broader web security practices and accountability frameworks show little advancement. The sector's overall trajectory can therefore be characterized as selectively progressive rather than systematically reformative.

From a compliance standpoint, the most urgent priorities include the publication of a comprehensive privacy policy by RRA, restoration and strengthening of third-party disclosure practices by RISA, development of clearly articulated breach notification procedures across all entities, publication of transparency reports, and improved implementation of website security headers. Without these structural reforms, improvements in policy language and selective transparency will not be sufficient to achieve full alignment with data protection law or to sustain public trust in digital government services.

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

The 2025 findings reveal a persistent pattern from 2024: government agencies continue to score zero in nearly all transparency and accountability-related metrics. As was the case last year, none of the assessed entities demonstrates measurable effort to publish accessible privacy policies, articulate data subject rights, establish internal data breach resolution mechanisms, issue transparency reports, or comply with third-party data transfer disclosure requirements.

The only area where performance is recorded is technical data security. This indicates that, structurally, compliance remains narrowly focused on cybersecurity safeguards while neglecting the broader legal obligations under Tanzania's Personal Data Protection Act. Notably, the Act does not exempt government agencies from compliance, except under narrowly defined exceptions provided under Sections 23(3) and 25(2). The continued absence of transparency and accountability measures therefore raises serious compliance concerns.

In both 2024 and 2025, all assessed agencies scored 0% in accessible privacy policies and pre-collection transparency. No publicly available, comprehensive privacy policy frameworks were identified, nor were there adequate disclosures regarding categories of personal data collected, lawful bases for processing, retention periods, or complaint mechanisms.

Compared to last year, there has been no improvement in this domain. The absence of visible privacy policies directly undermines the principles of transparency, fairness, and lawful processing. Without clear disclosures, data subjects cannot meaningfully understand how their personal data is handled, nor can they exercise their rights effectively. This persistent zero performance signals systemic non-compliance rather than isolated gaps.

As in 2024, none of the agencies demonstrates compliance with requirements relating to data subject rights or third-party data transfers. There is no clear articulation of rights such as access, correction, deletion, objection, or restriction of processing. Similarly, there is no disclosure of categories of third-party recipients, safeguards governing transfers, or legal bases for sharing personal data.

The lack of improvement from 2024 to 2025 suggests that data governance frameworks within these institutions have not evolved to incorporate rights-based compliance mechanisms. This is particularly concerning because third-party transfers represent high-risk processing activities that demand enhanced accountability and safeguards under data protection law. The continued absence of transparency in these areas exposes agencies to legal risk and undermines citizens' ability to challenge misuse of their personal data.

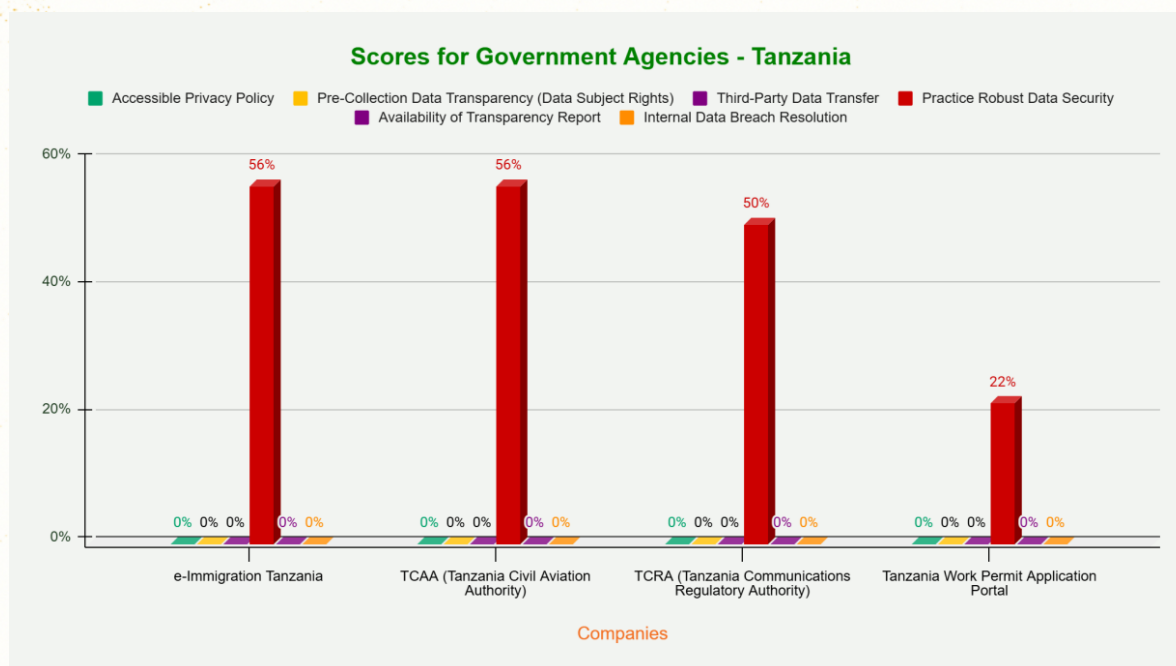
The 2025 assessment confirms that, as in 2024, none of the agencies has published transparency reports or established visible internal data breach resolution mechanisms. There is no evidence of structured breach notification timelines, escalation protocols, or publicly accessible incident reporting procedures. The failure to implement breach governance frameworks constitutes a significant accountability gap. Data protection law requires not only the prevention of breaches but also documented procedures for responding to and reporting them. Without such mechanisms, compliance cannot be demonstrated, even if security controls exist. The absence of transparency reporting further weakens public oversight and trust.

Data security remains the only measurable area of effort. In 2025, e-Immigration Tanzania and Tanzania Civil Aviation Authority each scored 56%, unchanged from 2024. Tanzania Communications Regulatory Authority declined from 61% in 2024 to 50% in 2025, indicating regression. Tanzania Work Permit Application Portal maintained a low score of 22%, unchanged from last year.

While it is positive that agencies continue to invest in technical safeguards, the stagnation and regression in some cases indicate that security maturity is not advancing.

Moreover, even the highest score of 56% remains below what would be considered robust compliance under a risk-based data protection framework.

Importantly, security safeguards alone do not equate to compliance. Data protection law requires a holistic approach incorporating transparency, accountability, lawful processing, and enforceable rights. A narrow focus on cybersecurity, without parallel governance reforms, results in partial and insufficient compliance.



A comparison between the two years shows near-total stagnation in transparency and accountability measures. In 2024, all agencies scored zero in privacy policy accessibility, third-party disclosure, transparency reporting, and breach management. In 2025, this remains unchanged. The only notable shift is the decline of TCRA's security score from 61% to 50%. e-Immigration Tanzania and TCAA maintained their 56% scores, while the Tanzania Work Permit Application Portal remained at 22%. Thus, there is no evidence of systemic reform, only maintenance of existing technical safeguards with minor fluctuations.

The 2025 findings confirm a troubling compliance imbalance. Government agencies expected to lead by example in implementing the Personal Data Protection Act remain largely non-compliant in areas fundamental to data protection governance. The absence of accessible privacy policies, rights frameworks, third-party disclosure mechanisms, breach resolution systems, and transparency reports reflects a failure to operationalize core principles of accountability and transparency. Given that the law does not provide blanket exemptions for public authorities, continued non-compliance may expose agencies to regulatory enforcement risks and reputational harm.

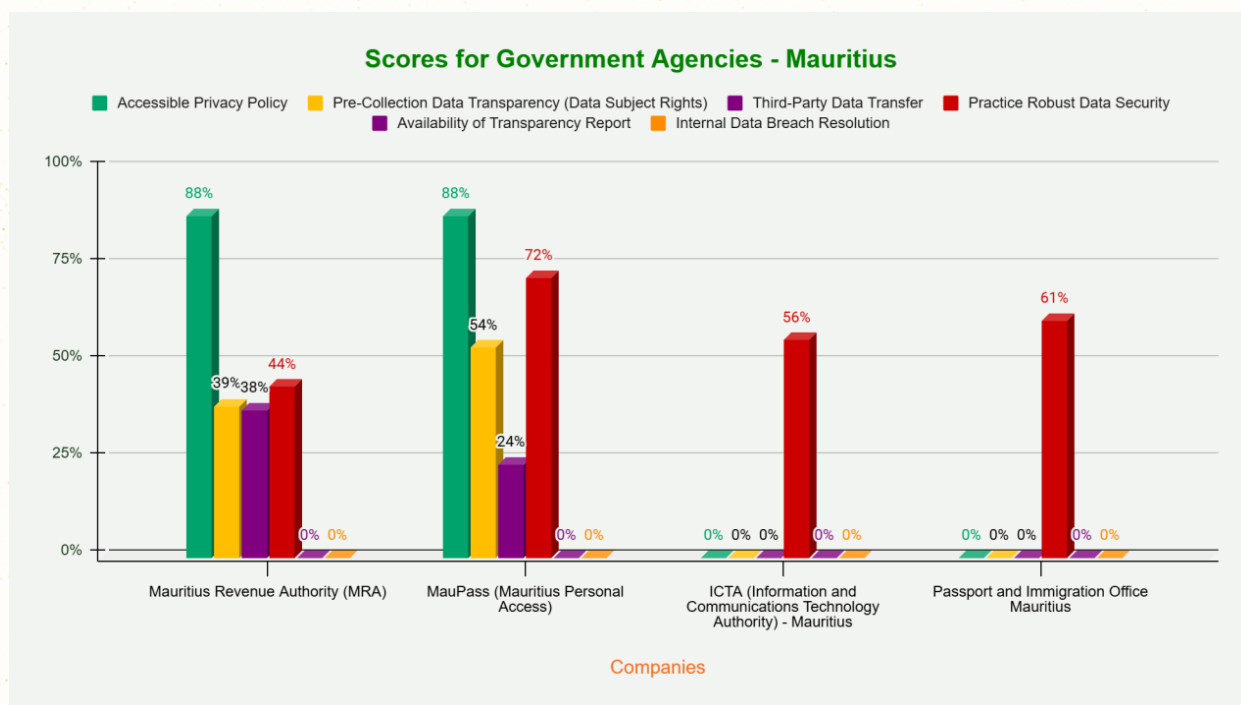
Most critically, the current approach emphasizes technical security while neglecting legal and procedural safeguards. This creates an incomplete compliance model that protects data in transit or storage but fails to guarantee lawful, fair, and transparent processing.

The 2025 assessment demonstrates that, compared to 2024, there has been no meaningful progress in aligning Tanzania's government digital platforms with comprehensive data protection standards. While some agencies maintain moderate data security practices, structural gaps in transparency, accountability, and rights protection persist unchanged.

Unless deliberate institutional reforms are undertaken particularly in publishing privacy policies, formalizing data subject rights procedures, regulating third-party transfers, and establishing breach governance frameworks, government agencies will continue to fall short of full compliance with Tanzania's data protection laws and principles.

f. Mauritius Revenue Authority (MRA), MauPass(Mauritius Personal Access), ICTA (Information and Communication Technology Authority) and Passport & Immigration Office Mauritius in Mauritius

The comparative assessment of government agencies this year reveals incremental yet uneven progress in privacy governance and compliance with the Data Protection Act 2017. While certain institutions have demonstrated measurable improvements, systemic weaknesses persist across key transparency and accountability indicators.



The Mauritius Revenue Authority (MRA) and MauPass emerged as the strongest performers under the accessible privacy policy indicator, each scoring 88% MRA maintained its performance from last year, when it was the only agency credited with having an accessible privacy policy. MauPass, by contrast, recorded the most significant improvement, rising from 0% last year to 88% this year. This shift reflects a substantial advancement in transparency practices. Both institutions now provide publicly available privacy policies that outline how personal data is collected, used, stored, and shared.

MRA's privacy policy remains concise and structured around compliance with Mauritian laws and regulations. It identifies the categories of data processed, including personal identifiers, contact details, financial information, and survey-related data. It clarifies that information may be collected directly from individuals or indirectly from third parties such as government entities or public sources. The policy also explains that data may be shared with statutory, regulatory, and law enforcement authorities where legally required, and that retention periods are governed by applicable legislation. However, while the policy demonstrates a baseline level of legal compliance, it provides limited detail regarding specific security safeguards or internal data breach procedures, which constrains full accountability under the Data Protection Act.

MauPass's privacy policy is comparatively more comprehensive. It specifies the collection of personal identifiers, contact details, derivative data such as IP addresses and access logs, and mobile device information. It explains that information is obtained directly through the National Authentication Framework or indirectly through usage logs and third-party integrations.

The policy outlines purposes including secure authentication, fraud prevention, service improvement, statistical analysis, and lawful disclosure. It also affirms users' rights to review, update, or delete their account information and describes secure storage at the Government Online Centre. This marked improvement from last year strengthens MauPass's compliance posture, particularly in relation to transparency and user rights.

In contrast, the Information and Communications Technology Authority (ICTA) and the Passport and Immigration Office Mauritius again scored 0 percent for accessible privacy policies, reflecting no progress from the previous year. The continued absence of publicly accessible privacy notices presents a significant compliance gap. Transparency is a foundational obligation under the Data Protection Act, and failure to provide clear notice regarding data processing activities undermines lawful processing and exposes these institutions to regulatory and reputational risks.

Progress is also visible in the area of data subject rights, though unevenly distributed. MRA improved from 21% last year to 39%, while MauPass advanced from 0% to 54%. These improvements suggest a growing recognition of statutory rights such as access, rectification, and erasure. MauPass, in particular, has embedded clearer mechanisms for users to manage their data. However, partial scores indicate that operational clarity and comprehensiveness remain limited. ICTA and the Passport and Immigration Office maintained 0% in this category, signaling continued deficiencies in recognizing and facilitating data subject rights. This stagnation raises concerns regarding compliance with core rights guaranteed under the Data Protection Act and risks eroding public confidence.

Transparency regarding third-party data sharing has improved modestly. MRA increased from 14% last year to 38%, and MauPass rose from 0% to 24%. Both institutions now provide clearer acknowledgment that data may be shared with other government entities or law enforcement authorities where required by law. Nevertheless, scores remain below half of the total possible, indicating limited disclosure regarding safeguards, oversight mechanisms, or the terms governing such transfers. ICTA and the Passport and Immigration Office again recorded 0 percent, reflecting continued opacity in this critical area. Given the sensitivity of regulatory and immigration-related data, the absence of visible safeguards heightens compliance risks.

All four agencies demonstrated efforts to ensure data security. MauPass now leads with 72%, up from 45% last year, indicating strengthened technical and organizational measures.

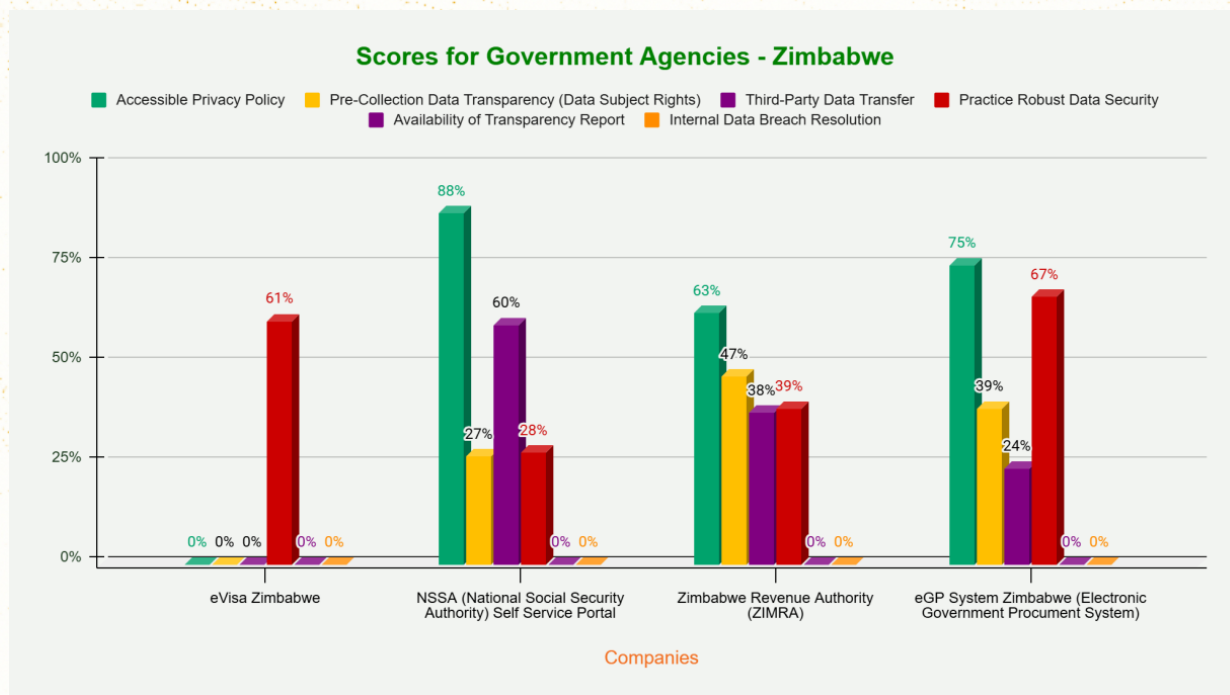
The Passport and Immigration Office maintained its previous score of 61%, remaining relatively strong in security safeguards. ICTA also maintained its score of 56%, while MRA improved modestly from 39% to 44%. These results suggest that preventive security controls are comparatively more developed than transparency and accountability mechanisms. However, none of the agencies provide evidence of internal data breach resolution frameworks or publish transparency reports. As in the previous year, all scored 0% in these categories. The absence of documented breach response mechanisms and public reporting reflects a persistent accountability gap and limits demonstrable compliance with the Act's requirements for responsible data governance.

In comparison to last year's findings, the most notable change is MauPass's substantial advancement across multiple indicators, particularly in privacy policy accessibility, data subject rights, and third-party transparency. MRA has shown steady, incremental improvement while maintaining its leadership in policy accessibility. However, ICTA and the Passport and Immigration Office have remained largely stagnant, with no measurable progress in core transparency indicators. Additionally, sector-wide weaknesses in transparency reporting and internal breach management remain unchanged.

Overall, while this year's assessment indicates gradual movement toward stronger data governance practices, compliance remains partial rather than comprehensive. Improvements in policy accessibility and security safeguards are encouraging, yet persistent deficiencies in transparency reporting, breach response mechanisms, and full operationalization of data subject rights suggest that accountability structures are still underdeveloped. Without sustained institutional reform particularly within ICTA and the Passport and Immigration Office, regulatory exposure and public trust risks will continue to shape the privacy landscape within Mauritius' public sector.

g. 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

The current assessment of Zimbabwean government digital platforms reveals modest progress in selected areas of privacy governance, but continued structural weaknesses that raise concerns regarding sustained compliance with data protection laws. While certain entities have strengthened transparency and security controls compared to last year, overall performance across the sector remains inconsistent and, in critical areas, stagnant.



In relation to accessible privacy policies, visible effort was made this year. The National Social Security Authority (NSSA) recorded the strongest improvement, rising from 50% last year to 88%. This marks a substantial enhancement in policy accessibility and suggests a deliberate effort to improve transparency around data processing practices.

The e-Government Procurement (eGP) System Zimbabwe maintained its prior-year performance at 75%, indicating stability but no further advancement. In contrast, the Zimbabwe Revenue Authority (ZIMRA) experienced a notable decline, dropping from 88% last year to 63%. This reduction may reflect either diminished visibility of its privacy framework or reduced comprehensiveness in its disclosures.

Compared to last year, when ZIMRA led the sector in policy accessibility, this year's results show a shift in leadership to NSSA. While three agencies previously demonstrated accessible privacy policies, the redistribution of scores indicates both improvement and regression within the sector. From a compliance perspective, accessible privacy notices are central to the transparency principle embedded in data protection legislation. Improvements by NSSA and the maintained performance of eGP strengthen their legal footing; however, ZIMRA's decline signals potential backsliding in maintaining clear, user-facing data protection commitments.

With respect to data subject rights, performance improved across most entities, although scores remain moderate. ZIMRA led in this category at 47%, improving from 32% last year. The eGP System Zimbabwe rose slightly from 37% to 39%, while NSSA increased from 19% to 27%.

eVisa Zimbabwe, however, maintained a score of 0%, indicating no visible mechanisms to facilitate access, rectification, or erasure rights.

These incremental improvements suggest a growing institutional awareness of the need to operationalize user rights. Nevertheless, partial scores below 50% indicate that rights frameworks are not yet fully embedded or clearly actionable. The continued absence of any measurable effort by eVisa Zimbabwe is particularly concerning, as the platform processes highly sensitive travel and identity information. Failure to provide accessible mechanisms for data subject rights may expose the institution to regulatory risk and undermine the fairness and lawfulness principles required under data protection laws.

All entities share personal data with third parties and demonstrated some level of disclosure regarding such transfers. NSSA remained the strongest performer in this category, maintaining a high score of 80% from last year. ZIMRA's score declined marginally from 39% to 38%, while eGP maintained 24%. Although these figures show that third-party transfers are acknowledged, they also reveal limited progress in strengthening safeguards or expanding transparency. Compared to last year, when ZIMRA led this category at 70% and NSSA followed at 60%, this year reflects a reordering of compliance performance but no systemic strengthening across the board.

The implications for privacy practice are significant. Third-party transfers present heightened risks of misuse, especially where contractual safeguards, oversight mechanisms, and cross-border protections are unclear. While NSSA appears to have institutionalized stronger disclosure practices, the moderate to low scores for ZIMRA and eGP suggest that citizens may not be fully informed about how and under what safeguards their information is shared.

Data security measures present a mixed but somewhat encouraging trend. The eGP System Zimbabwe recorded the most substantial improvement, increasing from 39% last year to 67% this year, thereby emerging as the sector leader in security safeguards. eVisa Zimbabwe demonstrated marked improvement, rising from 11% to 61%, indicating enhanced technical protections despite its broader governance deficiencies. ZIMRA maintained its previous score of 39%, while NSSA declined from 39% to 28%.

These shifts indicate that while some platforms are investing in technical safeguards, others may be deprioritizing or insufficiently documenting their security controls. The decline in NSSA's security score, despite its strong transparency performance, suggests an imbalance between policy visibility and technical implementation.

Effective compliance requires both transparent governance frameworks and robust technical safeguards; improvements in one area cannot compensate for weaknesses in another.

As in the previous year, all entities scored 0% for transparency reporting and internal data breach resolution mechanisms. This persistent absence of accountability structures is one of the most significant compliance gaps across the sector. Transparency reports and clearly articulated breach response procedures are essential components of modern data protection regimes. Their continued absence signals limited institutional maturity in incident management and oversight. Without documented breach handling processes, citizens remain uncertain about how incidents would be addressed, notified, or remedied.

Overall, although measurable improvements have been recorded in privacy policy accessibility, data subject rights, and security safeguards for certain agencies, the sector's performance remains fragmented. NSSA has made notable gains in transparency, eGP has strengthened its security posture, and ZIMRA has moderately improved its recognition of data subject rights despite a decline in policy accessibility. However, eVisa Zimbabwe continues to perform poorly overall, with no visible registration safeguards, no accessible privacy policy, no pre-collection transparency, and no mechanisms for data subject rights, despite improvements in security controls.

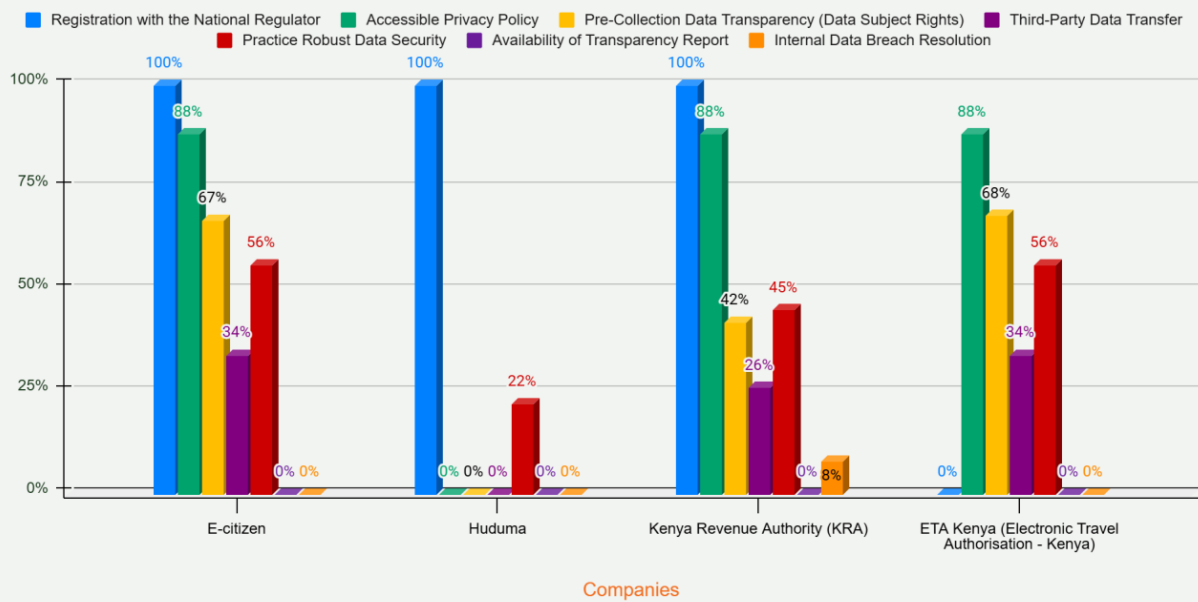
Compared to last year's findings, progress is evident but not transformative. Leadership positions have shifted, some scores have improved, and security investment appears more pronounced in certain platforms. However, the systemic weaknesses identified previously particularly the absence of transparency reporting, inadequate breach management frameworks, and weak pre-collection transparency remain largely unchanged.

These ongoing deficiencies raise concerns about sustained compliance with data protection laws and the ability of public institutions to demonstrate accountability. While incremental progress is commendable, comprehensive reform is necessary to align operational practices with legal requirements. Without stronger oversight mechanisms, clearer articulation of user rights, and institutionalized breach response frameworks, Zimbabwe's government digital platforms risk continued regulatory exposure and erosion of public trust in their handling of personal data.

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

The current assessment of Kenya's key government digital service platforms demonstrates measurable progress in certain compliance areas, yet continued structural weaknesses in transparency and accountability. Although some institutions have strengthened alignment with data protection requirements compared to last year, overall performance remains uneven, revealing significant disparities in privacy governance despite uniform legal obligations under Kenya's Data Protection Act.

Scores for Government Agencies - Kenya



With respect to registration with the national regulator, there was demonstrable improvement. e-Citizen, Huduma, and the Kenya Revenue Authority (KRA) each scored 100%. KRA maintained its perfect score from last year, confirming sustained compliance and institutional maturity in meeting formal regulatory requirements. In contrast, e-Citizen and Huduma improved from 0% last year to full compliance this year, representing a notable strengthening of their legal posture. Registration with the regulator is a foundational obligation under the Data Protection Act, and these improvements reflect enhanced recognition of statutory accountability requirements. However, the Electronic Travel Authorization (ETA) system maintained a score of 0 percent, unchanged from last year, signaling continued non-compliance with one of the most basic regulatory obligations.

In relation to accessible privacy policies, visible effort was again demonstrated. e-Citizen, KRA, and ETA Kenya each maintained a score of 88%, consistent with last year's results. This stability indicates that these entities have preserved their public-facing transparency frameworks. Huduma, however, continues to lag behind, with no accessible privacy policy documentation. The presence of privacy policies for e-Citizen, KRA, and ETA suggests formal acknowledgment of transparency requirements, yet the maintenance of identical scores year-on-year implies limited enhancement in policy depth or clarity. Accessibility alone does not guarantee comprehensive compliance; policies must evolve to reflect changing operational practices, emerging risks, and enhanced regulatory expectations.

Performance in facilitating data subject rights reveals a more dynamic picture. ETA Kenya led this category with 68%, improving from 56% last year, indicating strengthened mechanisms for access, correction, or other statutory rights. e-Citizen recorded a slight decline, dropping from 72% to 67%, while KRA experienced a more pronounced reduction from 58% to 42%. Huduma again maintained 0%, demonstrating no visible effort to operationalize data subject rights. These mixed results suggest that while some entities are enhancing procedural pathways for individuals to exercise their rights, others may be experiencing implementation gaps or reduced transparency. Given that data subject rights are central to lawful and fair processing, declining scores in this area raise concerns about sustained compliance, particularly for KRA, which otherwise demonstrates strong institutional governance.

Third-party data sharing remains an area of weakness across all entities. Although all platforms share personal data with other government bodies or service providers, compliance levels are low. e-Citizen improved from 20% to 34%, indicating incremental progress in disclosing inter-agency or service provider data transfers. ETA Kenya, however, declined from 44% to 34%, while KRA dropped from 40% to 26%. Huduma once again scored 0%. Compared to last year, the general trend reflects either stagnation or regression rather than systemic improvement. Given the complexity of inter-agency collaboration within government digital ecosystems, insufficient disclosure about third-party transfers poses risks related to accountability, data minimization, and cross-border safeguards. Weak performance in this area undermines citizens' ability to understand how their information circulates across state systems and external partners.

Data security safeguards present a relatively stable but modest compliance landscape. e-Citizen and ETA Kenya both scored 56%, with e-Citizen maintaining last year's performance and ETA declining slightly from 61%. KRA maintained 45%, and Huduma remained at 22%. Compared to last year, when ETA led with 44% and KRA followed at 40%, this year reflects incremental strengthening for some entities but no transformative enhancement of security maturity. While the presence of technical and organizational safeguards is evident, scores below full compliance suggest that documentation, risk assessments, encryption protocols, or independent audits may not be sufficiently robust or publicly articulated.

As in the previous year, all entities scored 0% for transparency reporting and internal data breach resolution mechanisms. This persistent gap is one of the most concerning findings. Transparency reports, breach notification procedures, and documented internal resolution frameworks are essential to demonstrating accountability and preparedness. Their absence indicates that although certain preventive measures may exist, reactive and oversight mechanisms remain underdeveloped. This exposes agencies to regulatory risk and limits public confidence in the event of security incidents.

Taken together, the findings reveal highly variable privacy protection standards across Kenya's government digital services. KRA continues to demonstrate relatively strong overall compliance, supported by comprehensive governance structures such as Data Protection Officer designation, detailed retention policies, and complaint escalation pathways. Its consistent regulatory registration and sustained policy accessibility reflect institutional commitment, though recent declines in data subject rights facilitation and third-party transparency suggest areas requiring renewed attention.

e-Citizen's performance reflects meaningful progress, particularly in achieving full regulatory registration and modest improvements in third-party disclosure. However, the slight decline in data subject rights and stagnant security performance indicate that operational consistency remains a challenge. ETA Kenya demonstrates moderate compliance, with improvements in data subject rights but regression in third-party transparency and slight decline in security safeguards. Given the sensitive nature of immigration and travel-related data, enhanced specificity in retention practices and cross-border data sharing arrangements is essential to mitigate legal and reputational risk.

Huduma's continued weak performance remains particularly concerning. Although it achieved full regulatory registration this year, it still lacks an accessible privacy policy, data subject rights mechanisms, third-party transparency, and robust security safeguards.

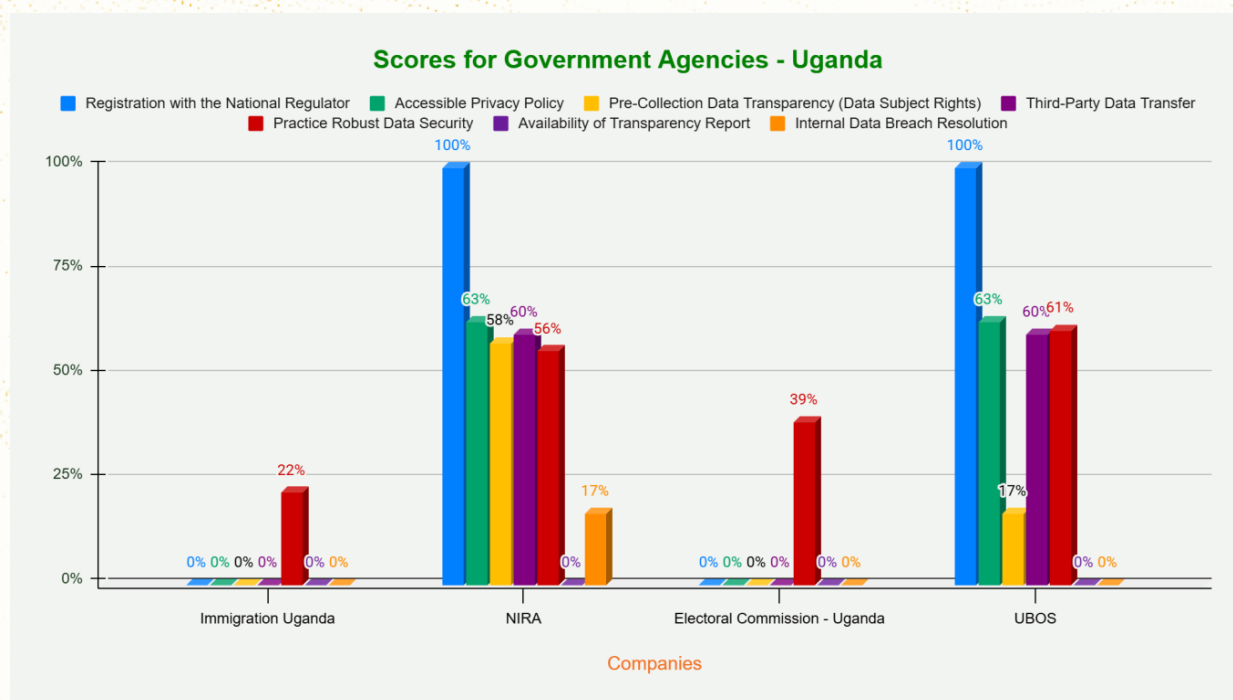
For a platform handling sensitive services such as identity documentation and civil registration, these deficiencies represent significant compliance and trust risks.

Compared to last year, the most notable improvements are the expansion of regulatory registration compliance and incremental gains in certain rights-based frameworks. However, declines in third-party transparency and stagnation in accountability mechanisms indicate that progress is neither uniform nor comprehensive. The continued absence of transparency reporting and breach resolution processes across all entities highlights a systemic governance weakness that remains unaddressed.

In conclusion, while Kenya's government digital platforms demonstrate growing awareness of data protection obligations, compliance remains partial and uneven. Stronger institutionalization of accountability mechanisms, clearer third-party transfer disclosures, consistent facilitation of data subject rights, and development of formal breach response frameworks are necessary to ensure sustained alignment with the Data Protection Act and to preserve citizen trust in digital public services.

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

The current assessment of key Ugandan government agencies reveals modest progress in formal compliance measures but continued systemic weaknesses in transparency, accountability, and operational safeguards. Although certain institutions have improved their alignment with statutory requirements compared to last year, overall performance across the sector remains low. This is particularly concerning given the volume and sensitivity of personal data processed by these agencies, including biometric, electoral, immigration, and national identification records.



With respect to registration with the national regulator, demonstrable compliance was recorded for the National Identification and Registration Authority (NIRA) and the Uganda Bureau of Statistics (UBOS), both of which maintained a perfect score of 100% from last year. This sustained performance reflects continued adherence to one of the foundational requirements under Uganda’s Data Protection and Privacy Act. In contrast to last year when Immigration Uganda, the Electoral Commission, and UBOS had scored 0% in registration this year’s findings confirm that NIRA and UBOS remain the only agencies fully compliant in this respect, while Immigration Uganda and the Electoral Commission continue to lag behind. Regulatory registration represents the baseline of accountability; failure to comply signals fundamental gaps in legal adherence.

A notable development this year is the improvement in accessible privacy policies. NIRA and UBOS are now the only government entities within the study with published privacy policies, each scoring 63%. NIRA improved significantly from 0 percent last year, marking an important step toward transparency. UBOS maintained its previous score of 63%, remaining stable but without further enhancement. Immigration Uganda and the Electoral Commission again scored 0%, reflecting the continued absence of publicly available privacy documentation. Compared to last year, when UBOS was the only agency with an accessible policy, NIRA’s introduction of a policy constitutes meaningful progress. However, the overall picture remains troubling, as half of the assessed institutions still operate without any publicly articulated privacy framework.

An examination of NIRA’s privacy policy reveals both strengths and notable gaps. The policy details specific technical safeguards, including encryption at the point of data capture, transmission, processing, sharing, and disposal, particularly in relation to national identification data. It also indicates that data subjects will be notified of data breaches and recognizes rights such as access, correction, erasure, and the right to lodge a complaint. However, important ambiguities remain. The policy does not define what constitutes “undue delay” in breach notification, does not outline clear investigative procedures or timelines for handling complaints, and fails to specify how breaches may be reported or which contact channels should be used. Additionally, while the policy defines personal data and provides contact details for NIRA, it does not clearly articulate the purposes of data collection, retention periods, or the identities of third parties with whom data may be shared. The absence of provisions regarding the right to restrict processing further limits its completeness.

UBOS’s policy, while accessible, demonstrates more substantial limitations. It does not clearly define the categories of data collected, the purposes of processing, or the contact details of the data controller. It lacks explicit recognition of core data subject rights, including access, rectification, erasure, restriction, or withdrawal of consent. The policy does not articulate complaint procedures, nor does it specify whether law enforcement may access personal data. Although UBOS does not permit third-party access to personal data within its policy framework, the lack of clarity regarding rights and procedural safeguards weakens its compliance posture. Compared to last year, UBOS’s policy remains largely unchanged, suggesting stagnation rather than improvement.

In terms of data subject rights, NIRA recorded significant progress, improving from 0% last year to 58% this year. This indicates growing institutional recognition of statutory rights and mechanisms for their exercise. UBOS maintained a

modest score of 17%, reflecting limited facilitation of rights despite having a policy in place. Immigration Uganda and the Electoral Commission again scored 0%, demonstrating no visible effort to operationalize data subject rights. These findings highlight a concerning inconsistency: while certain agencies have begun to formalize rights-based protections, others remain entirely opaque, undermining citizens' ability to exercise control over their personal data.

All entities share data with third parties, yet compliance in this area remains uneven. NIRA improved from 0% last year to 60%, reflecting greater disclosure of data-sharing practices. UBOS maintained its score of 60%, continuing to demonstrate relative strength in this area compared to its peers. Immigration Uganda and the Electoral Commission maintained 0%, indicating no transparency regarding third-party data transfers. Compared to last year, when UBOS led this category and other agencies scored 0%, the inclusion of NIRA as a leading performer marks improvement. However, the absence of disclosure by Immigration and the Electoral Commission remains a significant compliance risk, particularly given the cross-border and inter-agency nature of immigration and electoral data processing.

Data security safeguards show measurable progress overall. UBOS led with 61%, improving from 39% last year. NIRA increased significantly from 22% to 56%, reflecting enhanced technical and organizational measures. The Electoral Commission maintained 39%, while Immigration Uganda remained at 22%. Compared to last year, improvements in NIRA and UBOS suggest growing investment in technical security infrastructure. However, stable or stagnant scores for Immigration and the Electoral Commission indicate limited advancement in safeguarding sensitive citizen data.

As in the previous assessment, all entities scored 0% for transparency reporting and internal data breach resolution mechanisms. The continued absence of published transparency reports and documented breach-handling procedures represents a persistent accountability gap. While certain policies reference breach notification, there is no evidence of comprehensive internal frameworks detailing investigation procedures, escalation pathways, or independent oversight mechanisms. This omission undermines demonstrable compliance with accountability and responsiveness obligations under data protection law.

Government agencies remain the weakest-performing sector in the study. Immigration Uganda and the Electoral Commission continue to operate without published privacy policies and scored zero on most indicators, exposing the absence of even basic transparency safeguards. NIRA and UBOS performed comparatively better, particularly in registration compliance, security safeguards, and limited policy accessibility. However, even these agencies exhibit significant gaps in retention disclosure, clarity of purpose limitation, detailed breach procedures, and comprehensive articulation of data subject rights.

Compared to last year, the most notable changes are NIRA's introduction of a privacy policy, improvements in data subject rights recognition, and strengthened security safeguards by both NIRA and UBOS. Nevertheless, the structural weaknesses identified in the previous assessment particularly the absence of transparency reporting, inadequate breach resolution mechanisms, and incomplete policy frameworks remain largely unchanged.

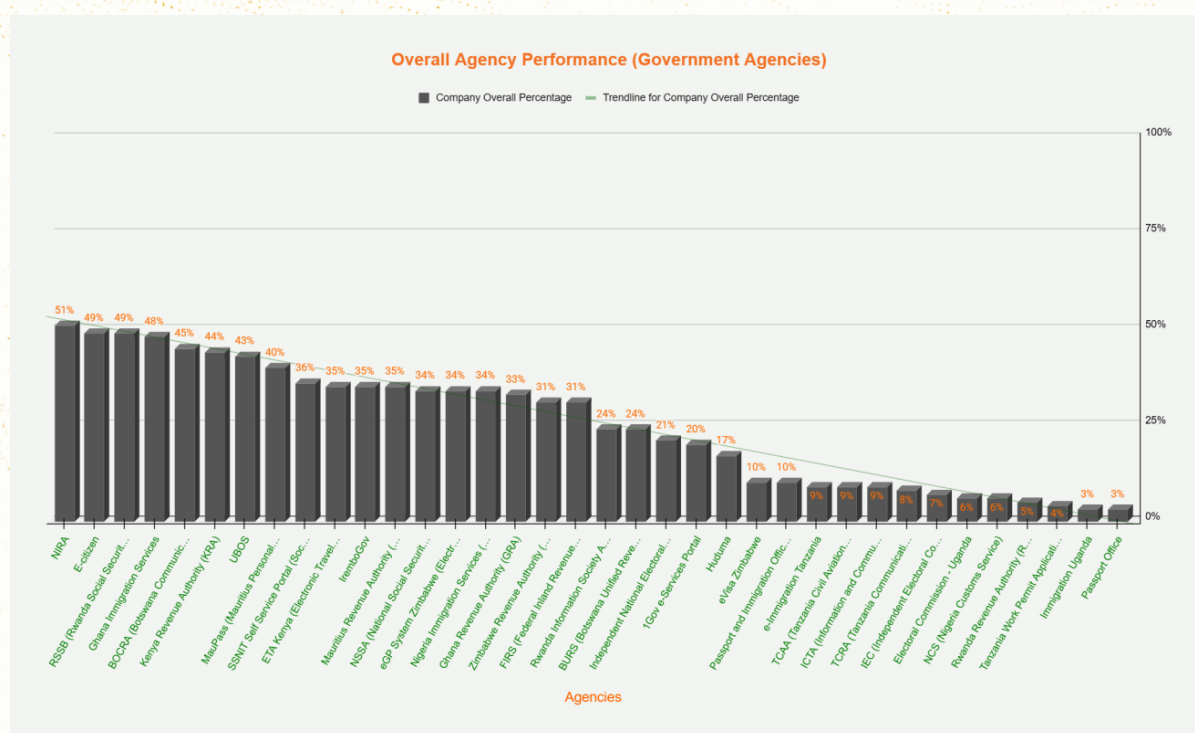
In conclusion, while incremental improvements are evident, Uganda's government institutions continue to demonstrate fragmented and partial compliance with data protection requirements. The limited transparency and accountability mechanisms, especially within Immigration Uganda and the Electoral Commission, present ongoing risks to citizen privacy and institutional trust. Comprehensive reform, including clear articulation of data processing purposes, retention limits, enforceable rights mechanisms, and documented breach management procedures, is essential to ensure meaningful compliance and to safeguard the sensitive personal data entrusted to public authorities.

3.4.6.3 Comparison of companies/entities within the sector

High-Performing Jurisdictions: Emerging Compliance Leaders and Trajectories

Even at the upper end of performance, government agencies show only modest compliance with data protection requirements, with no institution exceeding 51%. Uganda, Kenya, Rwanda, and Ghana feature the strongest individual performers, though progress remains incremental rather than transformative.

Uganda's National Identification and Registration Authority (NIRA) now leads the sector at 51%, representing a significant improvement from last year's 17%. This upward shift suggests stronger governance around privacy policies, improved transparency, and more consistent security practices particularly notable given the sensitivity and scale of biometric and identity data processed by NIRA. UBOS (43%) has also improved slightly from last year's 40%, indicating gradual maturation in data handling practices.



Kenya's eCitizen (49%) and Kenya Revenue Authority (44%) show moderate improvement compared to last year, when eCitizen scored as low as 3% and KRA stood at 47%. While KRA's score reflects relative stability, eCitizen's sharp rise signals meaningful reforms in privacy disclosures and system governance. Rwanda's RSSB (49%) also represents an improvement from the low-40% range, suggesting increasing attention to data protection within core social service platforms. Ghana Immigration Services (48%) similarly demonstrates modest gains, indicating improving compliance in immigration-related digital systems. Despite these positive trajectories, the fact that the highest score barely crosses 50% underscores that even emerging leaders remain only partially compliant, with unresolved gaps in accountability, breach preparedness, and third-party data governance.

Mid-Range Performers: Partial Compliance and Structural Gaps (Change Over Time)

A large proportion of agencies cluster between 35% and 45%, reflecting partial compliance and slow, uneven progress over time. These agencies typically demonstrate baseline privacy measures such as published policies or basic security controls but lack deeper operational safeguards.

Botswana's BOCRA (45%) and Uganda's UBOS (43%) sit at the upper end of this tier, showing incremental improvement from last year. Mauritius' MauPass (40%) and Kenya's ETA system (35%) also demonstrate modest gains, suggesting gradual alignment with digital governance standards. Rwanda's IremboGov (35%) reflects continued but limited progress in e-government service delivery.

However, these agencies remain constrained by structural gaps. Transparency around data use, clarity on third-party data sharing, and internal breach response mechanisms are often absent or poorly documented. Compared to last year, improvements are visible but not systemic, indicating that compliance efforts may be reactive or project-based rather than embedded institutionally.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

A significant number of government agencies continue to exhibit systemic compliance failures, with scores below 30% and, in some cases, below 10%. These agencies present the highest risk to citizens' personal data.

Tanzania remains the most concerning jurisdiction. Core platforms such as e-Immigration Tanzania (9%), TCAA (9%), TCRA (8%), and the Tanzania Work Permit Application Portal (4%) remain extremely weak, showing little improvement from last year. These persistently low scores suggest entrenched deficiencies in privacy governance, security safeguards, and transparency.

Similarly, several agencies in Zimbabwe (eVisa Zimbabwe at 10%), Mauritius (Passport and Immigration Office at 10%; ICTA at 9%), Botswana (IEC at 7%; 1Gov e-Services at 20%), Nigeria (NCS at 6%; INEC at 21%), Uganda (Immigration

Uganda at 3%; Electoral Commission at 6%), and Ghana (Passport Office at 3%) continue to demonstrate minimal compliance. In many cases, scores have stagnated or declined, indicating regression or lack of sustained reform. These agencies typically lack accessible privacy policies, provide little or no transparency on data processing, and show no evidence of internal data breach preparedness, placing them at high risk of violating data protection laws.

Key Cross-Cutting Implications

Several cross-cutting insights emerge from the updated assessment. First, overall performance across government agencies remains low relative to the sensitivity of the data they process. Even the strongest performers demonstrate only partial compliance with data protection laws.

Second, while some agencies have made notable year-on-year improvements particularly in Uganda and Kenya progress remains uneven and heavily dependent on individual institutional reforms rather than sector-wide transformation. Agencies handling identity, immigration, taxation, and electoral data remain among the weakest performers, despite the heightened risks associated with these functions.

Third, accountability mechanisms are consistently absent across all performance tiers. Transparency reports, clear third-party data-sharing frameworks, and internal data breach response procedures remain rare, severely undermining lawful and trustworthy data governance.

In sum, the digital government services across the assessed countries remain structurally underprepared to meet data protection obligations. Without coordinated regulatory enforcement, sustained institutional investment, and a shift toward privacy-by-design in public sector digital systems, citizens' personal data will continue to face elevated risks of misuse, exposure, and rights violations undermining both legal compliance and public trust.

3.4.7 Health Sector Analysis

3.4.7.1 Overview of the sector and data collectors evaluated

The health sector across East, West, and Southern Africa with a particular focus on Rwanda, Kenya, Uganda, Tanzania, Zimbabwe, Mauritius, Nigeria, Ghana, and Botswana is undergoing rapid digital transformation. Countries are expanding the use of electronic health records, mobile health platforms, and national health information systems to improve service delivery and health outcomes. While digitization is advancing, privacy and data protection practices remain uneven.

Most of these countries now have comprehensive data protection laws that classify health data as sensitive personal information. Rwanda, Kenya, Mauritius, Nigeria, Ghana, and Botswana have relatively structured regulatory frameworks with designated data protection authorities. Uganda, Tanzania, and Zimbabwe also have legal regimes in place, though enforcement capacity and sector-specific implementation remain limited.

Despite legislative progress, several challenges persist across the region: weak enforcement capacity, inconsistent compliance among healthcare providers, limited cybersecurity safeguards, unclear cross-border data transfer mechanisms, and low public awareness of data protection rights. Many health data collectors still lack comprehensive privacy policies, clear consent procedures, and breach response systems.

Overall, while legal frameworks have improved significantly, practical implementation within healthcare systems continues to lag. Strengthening regulatory enforcement, institutional compliance, and technical safeguards will be essential to ensuring that digital health expansion in these countries protects patient confidentiality and builds public trust.

3.4.7.2 Analysis of compliance with each criterion

This evaluation covers a total of 36 entities, comprising four (4) health facilities selected from each participating country. From Nigeria, the facilities assessed were Avon Medical, Lagos Hospital, St. Catherine's Specialist Hospital Abuja, and St. Nicholas Hospital. In Ghana, the selected institutions were Korle-Bu Teaching Hospital, Komfo Anokye Teaching Hospital, Nyaho Medical Centre, and The Trust Hospital. Botswana was represented by Gaborone Private Hospital, Sidilega Private Hospital, Diagnofirm Medical Laboratories, and Sir Ketumile Masire Teaching Hospital.

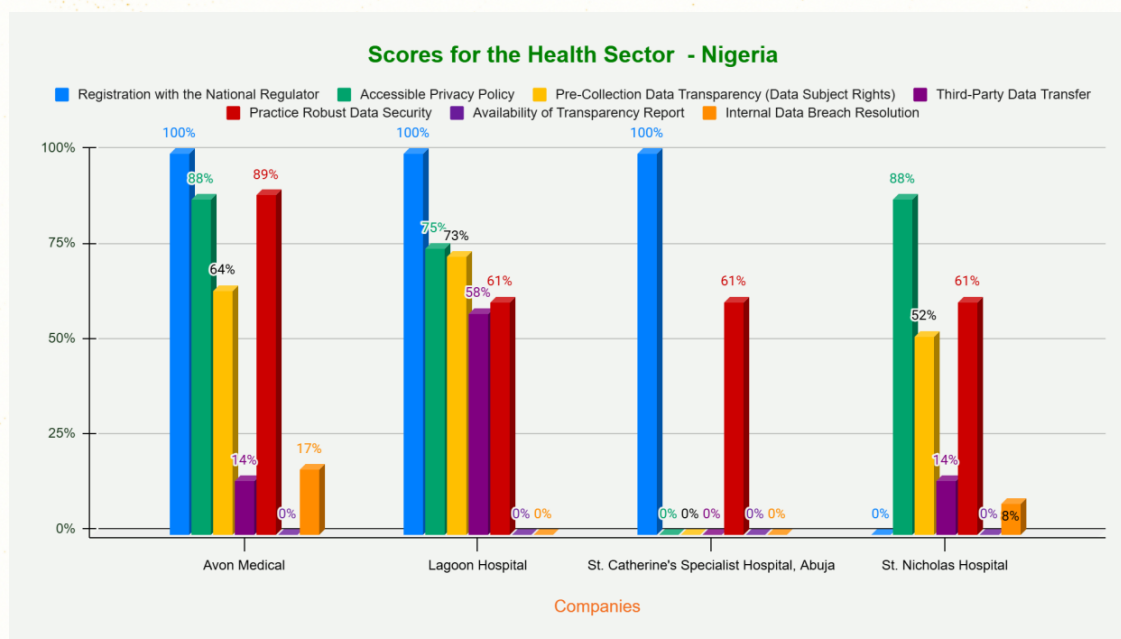
In Rwanda, the facilities included CHUK (University Teaching Hospital of Kigali), King Faisal Hospital, Ruhengeri Referral Hospital, and Rwanda Military Hospital. Tanzania's assessed institutions were Muhimbili National Hospital, Regency Medical Center, CRBT Tanzania, and LyfPlus Tanzania. From Mauritius, Wellkin Hospital, Clinique Darne, Aegle Clinic, and Dr. Agarwal's Eye Hospital Mauritius were evaluated. The facilities reviewed in Zimbabwe were Karanda Mission Hospital, Mpilo Central Hospital, Baines Avenue Clinic, and Parirenyatwa General Hospital (PGH).

In Kenya, the assessment covered Aga Khan University Hospital, Nairobi Hospital, Nairobi Women's Hospital (Karen), and Karen Hospital. Finally, in Uganda, Case Hospital, IHK Hospital, Lubaga Hospital, and Nakasero Hospital were included in the evaluation.

a. Avon Medical, Lagos Hospital, St. Catherine's Specialist Hospital Abuja and St. Nicholas Hospital in Nigeria

The assessment reveals uneven levels of compliance with data protection requirements across the four evaluated facilities with performance varying significantly across key privacy indicators. Demonstrable efforts to comply with mandatory registration requirements with the national data protection regulator were strongest at Avon Medical, Lagoon Hospital, and St. Catherine's Specialist Hospital, Abuja, each scoring 100%. In contrast, St. Nicholas Hospital recorded no evidence of registration compliance (0%). This gap exposes St. Nicholas Hospital to potential regulatory sanctions and reflects weaknesses in foundational compliance governance structures.

Accessibility and quality of privacy policies also varied. Avon Medical and St. Nicholas Hospital led in this category (88%), followed by Lagoon Hospital (75%), while St. Catherine's Specialist Hospital, Abuja scored 0%, indicating the absence of an accessible privacy notice. The lack of publicly available privacy information significantly limits patient awareness of data processing practices and undermines transparency obligations under data protection law.



Lagoon Hospital's privacy framework stands out as the most comprehensive. Its policies reflect a mature understanding of healthcare data protection requirements, clearly outlining categories of personal data collected (including medical, insurance, diagnostic, and digital platform data), lawful purposes for processing, data retention periods aligned with medical record standards, and detailed third-party sharing arrangements. The hospital also provides structured mechanisms for patients to exercise their rights and escalate complaints, demonstrating alignment with statutory accountability and transparency principles.

Avon Medical demonstrates solid baseline compliance, with policies covering key privacy elements such as categories of data collected, processing purposes, patient rights, and general third-party disclosures. However, certain areas particularly detailed retention timelines and granular disclosure of third-party arrangements could be strengthened to meet best-practice standards. St. Nicholas Hospital shows moderate compliance, providing basic disclosures and recognition of patient rights, though transparency around data sharing and retention practices remains limited. St. Catherine's Specialist Hospital, Abuja presents the most significant transparency gaps. The absence of accessible privacy documentation suggests weak implementation of statutory notice requirements, creating heightened compliance and reputational risk.

In operationalizing data subject rights, Lagoon Hospital again performed strongest (73%), followed by Avon Medical (64%) and St. Nicholas Hospital (52%). St. Catherine's Specialist Hospital, Abuja scored 0%, indicating no visible mechanisms for facilitating rights such as access, correction, or complaint resolution. Weak rights-management frameworks directly affect compliance with core legal obligations and may expose facilities to disputes and enforcement action.

All assessed facilities engage in third-party data sharing, a standard practice in healthcare delivery. However, compliance levels differ substantially. Lagoon Hospital demonstrated comparatively stronger safeguards and disclosure practices

(58%), while Avon Medical and St. Nicholas Hospital each scored 14%, and St. Catherine's Specialist Hospital, Abuja scored 0%. Limited transparency and weak contractual safeguards around third-party processors increase risks of unauthorized disclosure, cross-border transfer violations, and accountability failures.

All facilities showed measurable effort in implementing security safeguards. Avon Medical led in this category (89%), while Lagoon Hospital, St. Catherine's Specialist Hospital, Abuja, and St. Nicholas Hospital each scored 61%. This indicates general recognition of cybersecurity obligations. However, security strength alone does not compensate for weaknesses in transparency, rights facilitation, and governance structures.

A significant compliance gap across all facilities relates to internal data breach management and transparency reporting. None of the hospitals publish transparency reports, and compliance with structured internal breach resolution mechanisms is low. Avon Medical recorded the highest score in this area (17%), followed by St. Nicholas Hospital (8%), while the remaining facilities scored 0%. This deficiency signals limited preparedness for incident response and regulatory notification obligations, increasing exposure to legal and operational risk in the event of a data breach.

The findings indicate that while some facilities particularly Lagoon Hospital and Avon Medical are progressing toward structured privacy governance, compliance remains uneven and, in some cases, superficial. Registration compliance and technical safeguards appear more developed than transparency, accountability, and breach management frameworks. Facilities with limited privacy disclosures and weak rights-management systems face elevated risks of regulatory enforcement, reputational damage, and erosion of patient trust. The absence of structured breach response mechanisms further compounds institutional vulnerability.

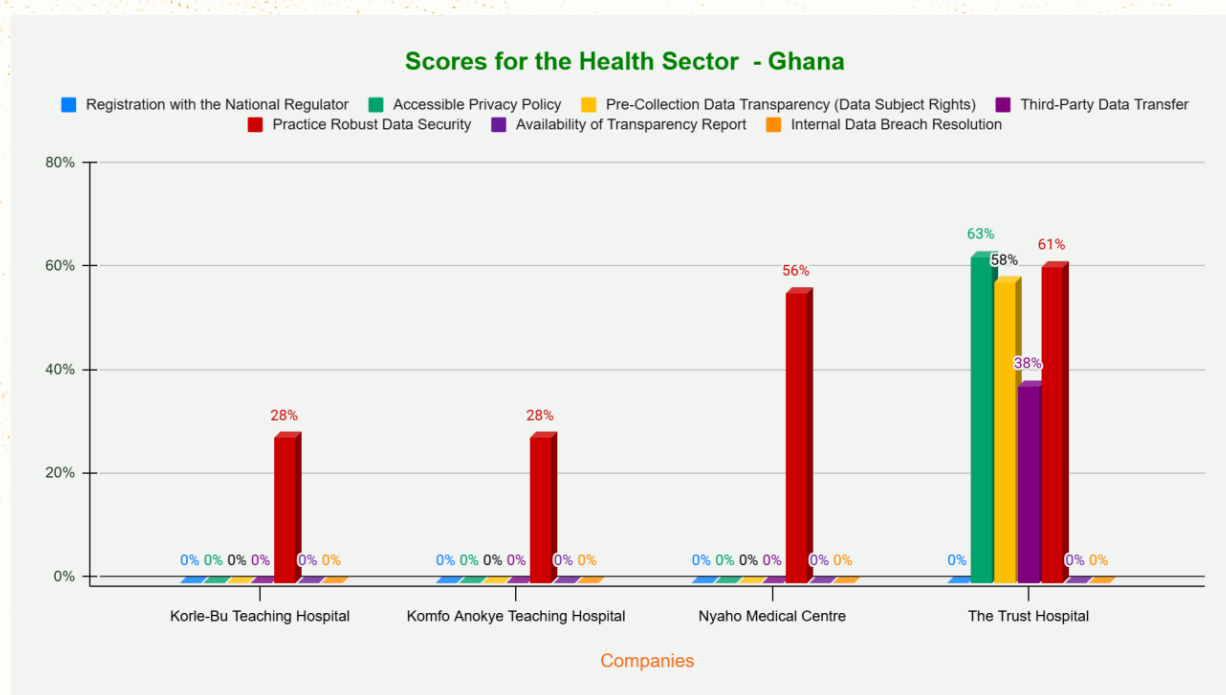
To strengthen compliance, facilities should prioritize:

- Publication of clear, accessible, and comprehensive privacy notices
- Formalization of third-party data processing agreements
- Development of documented breach response and notification procedures
- Strengthening of data subject rights management systems
- Periodic internal audits and privacy impact assessments

Overall, while there is evidence of growing awareness of data protection obligations within the healthcare sector, deeper institutionalization of privacy governance frameworks is necessary to ensure sustained compliance and alignment with national data protection laws.

b. *Korie-Bu Teaching Hospital, Komfo Anokye Teaching Hospital, Nyaho Medical Centre and The Trust Hospital in Ghana*

The assessment reveals systemic weaknesses in privacy governance and compliance with national data protection requirements across the sector. All four institutions failed to comply with mandatory registration requirements with the national data protection regulator. As a result, they remain inactive in the regulator's records. This foundational gap signals weak institutional accountability and exposes the facilities to potential regulatory sanctions.



Registration is a basic compliance obligation; failure at this level reflects broader governance deficiencies.

The sector demonstrates particularly weak transparency practices. Of the four institutions assessed, only The Trust Hospital has a publicly available privacy policy, scoring 63% for accessibility and 58% for content quality. However, the policy is not prominently displayed, limiting patient awareness and practical transparency.

Korle-Bu Teaching Hospital, Komfo Anokye Teaching Hospital, and Nyaho Medical Centre have no publicly available privacy policies, resulting in a complete absence of clarity regarding how patient data is collected, processed, stored, or shared. This creates significant compliance risks, particularly given the sensitive nature of health data.

The Trust Hospital's policy outlines categories of personal data collected (including health, payment, usage, and location data), identifies general processing purposes (healthcare management, payments, service improvement), and permits third-party sharing with healthcare providers, service partners, and where legally required. It affirms that data is not shared with advertisers and provides users with rights to access, correct, and request deletion of their data.

However, notable weaknesses remain:

- Retention timelines are vague.
- User rights are limited, particularly regarding objection and complaint escalation.
- Regulator complaint mechanisms are not clearly defined.
- Third-party entities are described by category but not specifically identified.

The absence of policies in the other three institutions leaves patients without notice of their legal rights or institutional safeguards, undermining transparency obligations under data protection law.

Only The Trust Hospital demonstrates measurable effort in operationalizing data subject rights (58%). The remaining three institutions scored 0%, as no visible mechanisms exist for access, correction, deletion, objection, or complaint handling. This lack of structured rights-management frameworks significantly impairs compliance with statutory requirements and increases exposure to disputes and regulatory enforcement.

All four institutions engage in third-party data sharing, which is expected in healthcare service delivery.

However, compliance safeguards are weak across the board. The Trust Hospital scored 38%, reflecting partial transparency and limited safeguards. Korle-Bu Teaching Hospital, Komfo Anokye Teaching Hospital, and Nyaho Medical Centre each scored 0% due to the absence of disclosed data-sharing frameworks. The absence of detailed processor agreements, data-sharing disclosures, or cross-border safeguards raises risks of unauthorized disclosure and accountability failures.

All institutions demonstrate some level of technical security implementation, though practices vary:

- The Trust Hospital leads with 61%, supported by an SSL rating of A and policy references to encryption, access controls, and secure storage practices.
- Nyaho Medical Centre follows with 56%, supported by a strong SSL rating (A+) and relatively stronger security headers (B), though without policy disclosure explaining these measures.
- Korle-Bu Teaching Hospital and Komfo Anokye Teaching Hospital both scored 28%, with acceptable SSL ratings (A) but failing security headers (F) and no policy disclosure addressing personal data security.

While technical safeguards exist, the absence of publicly documented security commitments limits accountability and weakens demonstrable compliance.

Performance in accountability and incident response is uniformly weak. None of the four institutions has published a transparency report since 2024. Additionally, no facility demonstrates visible internal data breach resolution mechanisms.

Korle-Bu, Komfo Anokye, and Nyaho Medical Centre lack privacy policies entirely, and therefore provide no information on breach notification procedures, investigation timelines, reporting channels, or escalation mechanisms. Although The Trust Hospital has a privacy policy, it does not provide specific guidance on breach detection, user notification timeframes, reporting channels, or regulator notification procedures. Consequently, all four institutions scored 0% in this category.

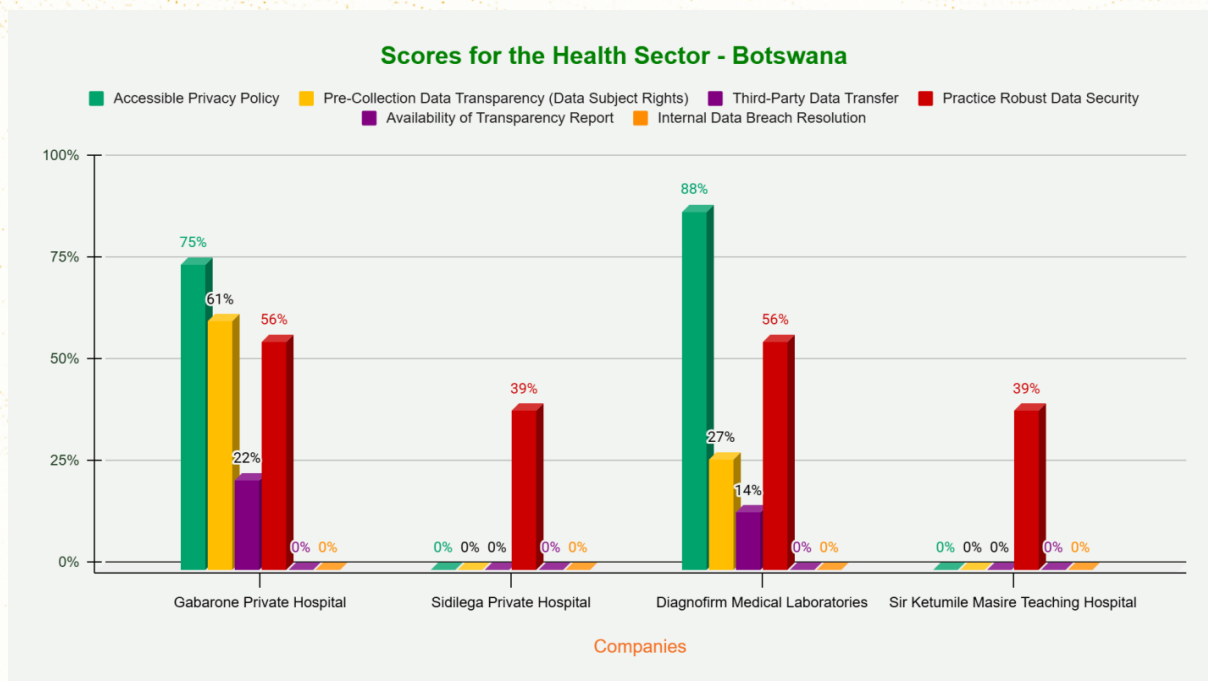
This gap represents a serious compliance vulnerability. In the event of a data breach, these institutions may lack structured procedures for lawful notification, mitigation, and remediation exposing them to regulatory penalties and reputational damage.

The findings indicate that privacy governance in the Ghanaian health sector remains underdeveloped. Non-registration with the regulator, absence of privacy policies in three of four institutions, weak rights-management systems, limited third-party transparency, and nonexistent breach response frameworks collectively point to systemic compliance deficiencies.

c. *Gaborone Private Hospital, Sidilega Private Hospital, Diagnofirm Medical Laboratories and Sir Ketumile Masire Teaching Hospital in Botswana*

The assessment of Gaborone Private Hospital, Diagnofirm Medical Laboratories, Sidilega Private Hospital, and Sir Ketumile Masire Teaching Hospital indicates moderate progress in certain areas of privacy governance, but persistent structural weaknesses that undermine full compliance with data protection laws.

Performance across the facilities varies significantly with respect to transparency and public-facing privacy documentation. Diagnofirm Medical Laboratories demonstrates the strongest commitment to accessibility, scoring 88%, followed by Gaborone Private Hospital at 75%. In contrast, Sidilega Private Hospital and Sir Ketumile Masire Teaching Hospital have no accessible privacy policies, each scoring 0%. The absence of publicly available privacy notices in two of the four institutions creates substantial compliance gaps. Privacy policies serve as the primary mechanism for informing patients of their rights, data processing purposes, and institutional safeguards.



Without them, transparency obligations under data protection law are not met, and patients lack visibility into how their sensitive health information is handled.

Gaborone Private Hospital shows moderate effort in operationalizing data subject rights, scoring 61%. This suggests some level of procedural recognition of access, correction, or related rights. However, the remaining facilities; Diagnofirm Medical Laboratories, Sidilega Private Hospital, and Sir Ketumile Masire Teaching Hospital scored 0%, indicating no visible mechanisms for facilitating statutory rights. The limited implementation of rights-management frameworks represents a critical compliance weakness. Data protection laws typically require institutions processing health data to establish clear procedures for responding to access requests, corrections, and complaints. The absence of such systems exposes facilities to legal risk and undermines patient trust.

All four facilities engage in third-party data sharing, which is standard practice in healthcare delivery (e.g., laboratories, insurers, technology providers). However, compliance safeguards in this area are notably weak. Gaborone Private Hospital recorded the highest score at 22%, followed by Diagnofirm Medical Laboratories at 14%, while Sidilega Private Hospital and Sir Ketumile Masire Teaching Hospital scored 0%. These low scores reflect limited transparency around categories of third-party recipients, absence of clearly articulated safeguards, and weak disclosure of cross-border transfer protections where applicable. Inadequate governance of third-party processing increases the risk of unauthorized disclosure, contractual non-compliance, and accountability failures, particularly given the sensitivity of medical data.

All facilities demonstrate some measurable effort to implement technical security controls. Gaborone Private Hospital and Diagnofirm Medical Laboratories lead in this category, each scoring 56%, suggesting moderate investment in cybersecurity protections. Sidilega Private Hospital and Sir Ketumile Masire Teaching Hospital scored 39%, indicating more limited but still observable safeguards. While these results suggest awareness of data security obligations, technical safeguards alone are insufficient to ensure full legal compliance. Effective privacy governance requires integration of security measures within broader accountability and transparency frameworks.

A significant cross-cutting weakness is the complete absence of transparency reporting and documented internal data breach response mechanisms. None of the four facilities has published a transparency report, nor is there visible evidence of structured breach notification procedures, internal investigation protocols, or patient notification frameworks. This represents a serious compliance vulnerability.

Data protection laws typically mandate timely breach notification to regulators and affected individuals. Without documented procedures, facilities risk delayed responses, regulatory penalties, and reputational damage in the event of a security incident.

The findings suggest that privacy governance among the assessed Botswana health facilities remains uneven and underdeveloped. While Diagnofirm Medical Laboratories and Gaborone Private Hospital demonstrate comparatively stronger performance in policy accessibility and technical security, sector-wide weaknesses persist in data subject rights implementation, third-party accountability, transparency reporting, and breach management.

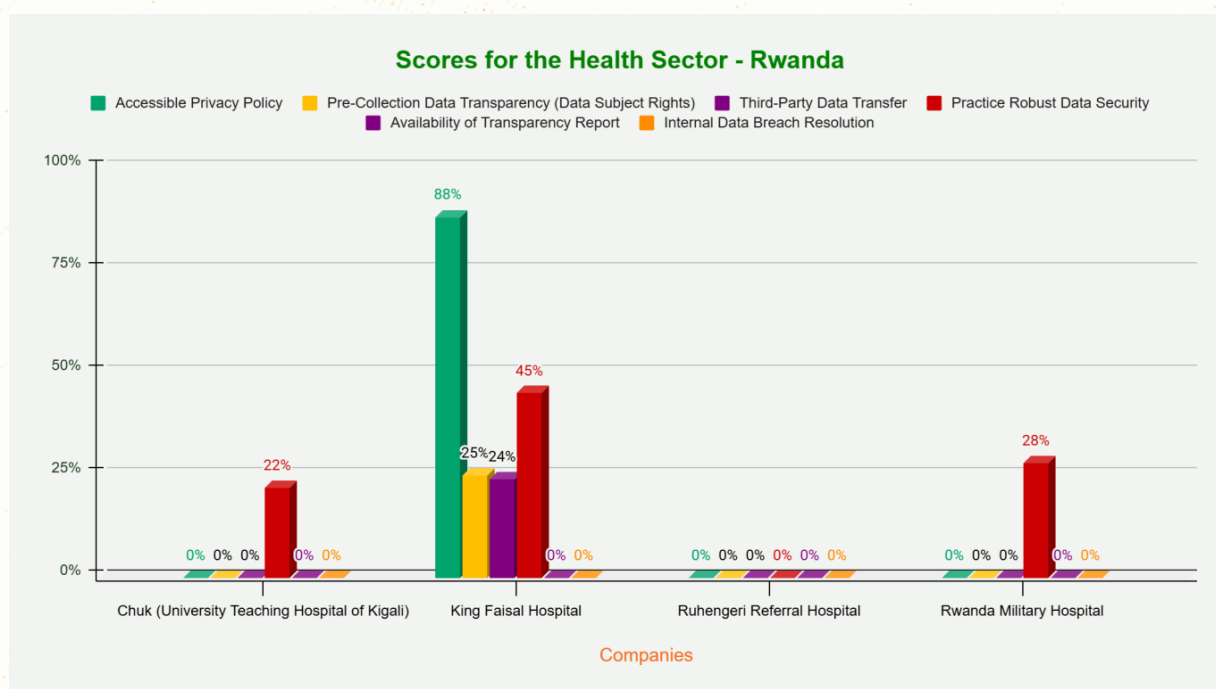
The lack of accessible privacy policies in half of the facilities and uniformly weak breach response mechanisms highlight systemic compliance risks. To align with data protection law and strengthen patient trust, facilities should prioritize:

- Publishing comprehensive and accessible privacy notices
- Establishing formal procedures for managing data subject rights
- Strengthening contractual and transparency safeguards for third-party processors
- Implementing documented breach detection and notification frameworks
- Introducing periodic transparency reporting mechanisms

Without these improvements, healthcare institutions remain exposed to regulatory enforcement risks and potential erosion of public confidence in their handling of sensitive health information.

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

The reassessment of CHUK (University Teaching Hospital of Kigali), King Faisal Hospital, Ruhengeri Referral Hospital, and Rwanda Military Hospital shows that there has been little measurable progress in strengthening privacy governance across Rwanda's public health sector since last year. While one institution continues to demonstrate partial compliance with data protection requirements, sector-wide performance remains weak, with some areas showing stagnation and others clear regression. King Faisal Hospital remains the only facility with a publicly accessible privacy policy, maintaining its score of 88% from the previous assessment.



The policy is visible and reasonably readable, meeting minimum length and accessibility standards. However, no substantive improvements have been observed in its content. Key compliance gaps identified last year persist, including incomplete contact information, limited clarity on retention periods, insufficient detail regarding third-party recipients, and the absence of a clearly defined complaint escalation process to the regulator. In contrast, CHUK, Ruhengeri Referral Hospital, and Rwanda Military Hospital continue to have no publicly available privacy policies, each maintaining a score of 0%. This sustained lack of transparency represents a significant compliance deficiency, as patients remain uninformed about how their personal and sensitive health data are collected, processed, retained, or shared.

With respect to data subject rights, King Faisal Hospital remains the only institution demonstrating effort in this area. However, its score declined markedly from 61% last year to 25% in the current assessment. Although the policy references rights such as access, correction, and deletion, it does not provide adequate procedural clarity or structured mechanisms for exercising these rights. The absence of detailed complaint channels or timelines further weakens its compliance posture. The other three hospitals again recorded 0%, reflecting no visible systems for facilitating statutory rights.

This regression at King Faisal Hospital, combined with the continued inaction of the other facilities, suggests that the operationalization of patient rights in the sector has not strengthened and, in some respects, has deteriorated.

Third-party data sharing practices remain inadequately governed. King Faisal Hospital's score in this category dropped from 30% to 24%. While the hospital acknowledges that data may be shared with affiliates and service providers and excludes advertisers, it does not clearly identify categories of shared data, specify recipients, or outline safeguards for cross-border transfers. CHUK, Ruhengeri Referral Hospital, and Rwanda Military Hospital continue to score 0% due to the absence of any publicly disclosed information on third-party processing. The persistence of these gaps heightens the risk of unauthorized disclosures and weakens accountability mechanisms required under data protection law.

In the area of data security, results are mixed. King Faisal Hospital maintained its score of 45%, continuing to reference general technical, administrative, and physical safeguards without providing specific details. Its SSL rating improved from B to A, although security headers remain weak. Rwanda Military Hospital recorded a modest improvement, increasing from 22% to 28%, supported by a stronger SSL configuration, though it still lacks policy documentation addressing data security practices. CHUK maintained its prior score of 22%, reflecting no improvement in either technical safeguards or transparency. Ruhengeri Referral Hospital experienced a significant decline, dropping from 33% to 0%, indicating deterioration in its technical security posture. Although some institutions demonstrate baseline cybersecurity measures, the lack of detailed disclosure and consistent standards across facilities limits demonstrable compliance.

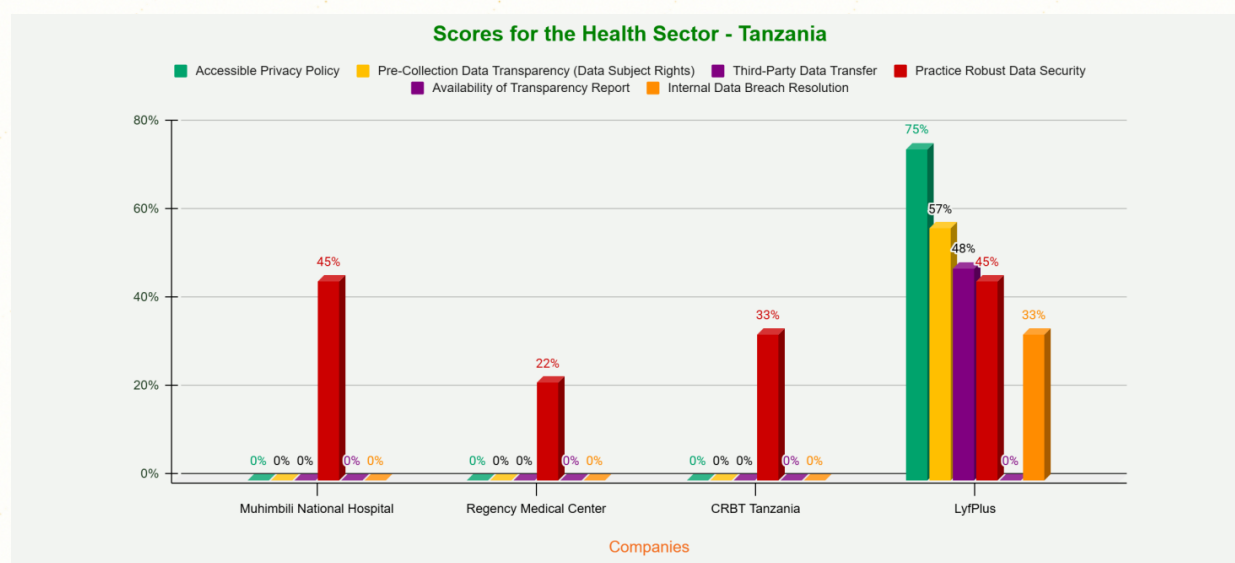
As in the previous year, none of the assessed hospitals has published a transparency report since 2024. Furthermore, there is no evidence of structured internal data breach resolution mechanisms across any of the four institutions. King Faisal Hospital provides limited complaint channels but does not articulate breach detection procedures, notification timelines, or regulator reporting obligations. The remaining hospitals provide no public guidance whatsoever on breach management. This continued absence of documented incident response frameworks represents a critical compliance vulnerability, particularly given the sensitive nature of health data.

Overall, the comparative analysis indicates that Rwanda's assessed health facilities have made no meaningful sector-wide progress in strengthening privacy practices since last year. King Faisal Hospital remains the relative leader but shows signs of stagnation and regression in certain areas, particularly in data subject rights and third-party transparency. The other institutions continue to demonstrate systemic non-compliance, especially in transparency and accountability.

These findings underscore persistent legal, operational, and reputational risks within the sector. Without deliberate institutional reforms focused on transparency, enforceable patient rights, structured third-party governance, strengthened cybersecurity documentation, and formal breach response mechanisms, the healthcare sector's compliance with data protection laws will remain limited and reactive rather than proactive and sustainable.

e. *Muhimbili National Hospital, Regency Medical Center, CRBT Tanzania and LyfPlus Tanzania in Tanzania*

The reassessment of Muhimbili National Hospital, Regency Medical Center, CRBT Tanzania, and LyfPlus Tanzania indicates that compliance with Tanzania's Personal Data Protection Act remains generally weak across the health sector, with limited progress recorded since last year. With the exception of LyfPlus, most institutions continue to demonstrate structural non-compliance in key privacy governance areas.



LyfPlus remains the only facility with a publicly accessible privacy policy. However, its score for policy accessibility declined from 88% last year to 75% in the current assessment. Although the policy is visible and available on its website, its readability has deteriorated, with a readability grade above level 14, making it difficult for the average data subject to understand. While the policy remains comprehensive in length and scope, reduced accessibility undermines the principle of transparency and the requirement that privacy notices be clear and intelligible.

In contrast, Muhimbili National Hospital, Regency Medical Center, and CRBT Tanzania continue to operate without publicly available privacy policies, each maintaining a score of 0% for the second consecutive year. This sustained absence of transparency significantly limits patient awareness of data processing practices and reflects non-compliance with statutory notice obligations.

In relation to data subject rights, LyfPlus recorded improvement, increasing from 43% last year to 57%. This suggests greater articulation of user rights within its privacy framework. Nonetheless, procedural clarity remains limited, particularly regarding complaint escalation and enforcement mechanisms. The other three hospitals again scored 0%, demonstrating no visible structures for enabling access, correction, objection, or other statutory rights. The absence of rights-management systems across most institutions indicates continued failure to operationalize one of the core pillars of data protection law.

Third-party data sharing practices show modest improvement only at LyfPlus, which increased from 32% to 48%. While this reflects enhanced disclosure regarding data transfers, the safeguards remain incomplete, particularly concerning identification of specific third parties and detailed transfer protections. Muhimbili National Hospital, Regency Medical Center, and CRBT Tanzania maintained scores of 0%, as no privacy documentation exists to explain whether and how personal data is shared. This lack of transparency heightens the risk of undisclosed or inadequately governed data transfers, particularly in a healthcare environment where sensitive data is routinely exchanged.

With respect to data security, performance across the facilities remains inconsistent and, in some cases, has declined. LyfPlus, which led the sector last year with 61%, dropped significantly to 45%. Muhimbili National Hospital recorded a marginal increase from 44% to 45%, thereby sharing the highest score in this category. CRBT Tanzania maintained its prior score of 33%, while Regency Medical Center continued to perform weakly. Although all facilities demonstrate some level of technical security effort, the overall scores remain low, raising concerns regarding compliance with Section 27 of the Personal Data Protection Act, which obliges data controllers to ensure appropriate security safeguards. The downward shift at LyfPlus is particularly notable, given that it previously demonstrated comparatively stronger digital governance practices.

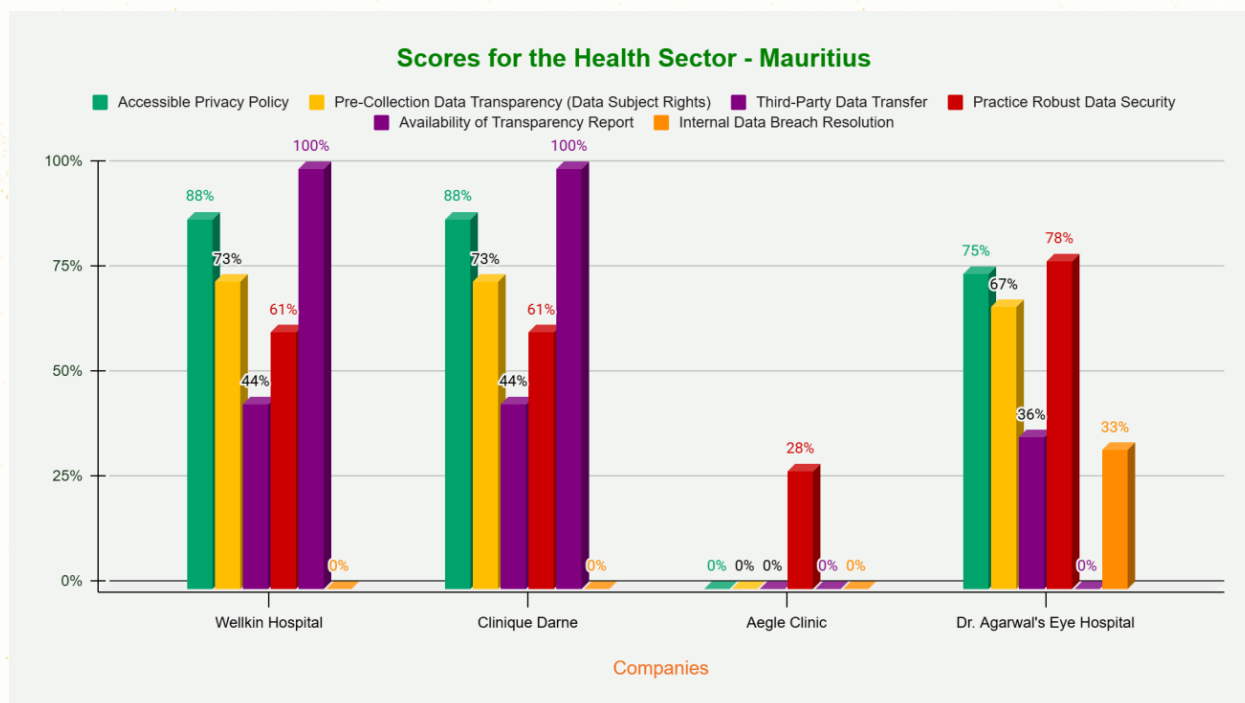
Transparency reporting remains entirely absent across the sector. None of the four facilities has published a transparency report, and all maintained a score of 0% in this category from last year. Similarly, internal data breach resolution mechanisms remain underdeveloped. LyfPlus showed improvement, rising from 17% to 33%, indicating some movement toward structured breach management. However, the framework remains incomplete, with no clearly defined notification timelines or investigation procedures. Muhimbili National Hospital, Regency Medical Center, and CRBT Tanzania maintained scores of 0%, reflecting no visible breach response protocols. This continued absence of documented breach management systems exposes facilities to significant regulatory and reputational risks in the event of a data incident.

Comparatively, last year's analysis positioned LyfPlus as the clear sector leader across nearly all privacy metrics, particularly in data security and policy transparency. While it remains the most compliant institution in the current assessment, its performance has declined in accessibility and data security, even as it improved in data subject rights, third-party transparency, and breach management. The other facilities show no measurable progress across most metrics, maintaining persistent non-compliance in transparency, rights facilitation, and accountability.

Overall, the findings indicate that Tanzania's assessed health facilities continue to exhibit widespread weaknesses in privacy governance. With the exception of LyfPlus, there is little evidence of structured compliance with data protection principles. Even LyfPlus, despite leading performance, demonstrates only partial compliance and faces challenges related to policy readability, detailed safeguards, and comprehensive breach response procedures. The stagnation across most institutions suggests that compliance efforts have not been institutionalized sector-wide. Without deliberate reforms aimed at establishing accessible privacy policies, enforceable data subject rights mechanisms, documented third-party safeguards, strengthened cybersecurity standards, and transparent breach response frameworks, the healthcare sector will remain exposed to regulatory enforcement risks and diminished patient trust.

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

The reassessment of Wellkin Hospital, Clinique Darné, Dr. Agarwal's Eye Hospital Mauritius, and Aegle Clinic indicates that Mauritius' private health sector continues to demonstrate relatively stronger transparency practices compared to peers in other jurisdictions assessed. However, despite pockets of progress, important compliance gaps remain, particularly in breach management and detailed security governance. A comparison with last year's findings shows a combination of stability, targeted improvements, and persistent structural weaknesses.



As in the previous assessment, Wellkin Hospital and Clinique Darné remain the sector leaders in privacy policy accessibility, each maintaining a score of 88%. Dr. Agarwal's Eye Hospital also maintained its prior score of 75%, while Aegle Clinic continues to have no accessible privacy policy, scoring 0% for the second consecutive year. The continued absence of a privacy notice at Aegle Clinic represents a fundamental transparency failure and places the institution at clear risk of non-compliance with data protection obligations requiring notice to data subjects.

The privacy policies of Wellkin Hospital and Clinique Darné remain prominently displayed and fairly comprehensive. Both outline the types of personal data collected, including medical and identifying information, explain the purposes of collection, and provide contact information for data protection queries. They recognize core patient rights, including access, rectification, erasure under certain conditions, objection to processing, and the right to lodge complaints with the institution or the national Data Protection Office. Both policies exclude sharing personal data with advertisers and allow disclosure to law enforcement where reasonably required. However, neither policy specifies detailed retention periods nor comprehensively lists all third-party recipients. In addition, while data security is referenced, specific technical and organizational measures are not described, and breach-handling procedures remain undefined.

Dr. Agarwal's Eye Hospital's privacy policy is similarly accessible and fairly detailed. It outlines categories of personal, medical, insurance, and financial data collected, explains processing purposes, and provides mechanisms for access, correction, deletion, and withdrawal of consent. The policy identifies categories of third-party recipients, including service providers and affiliates, and recognizes grievance procedures through a designated officer. Compared to last year, its performance improved notably in several operational areas, particularly third-party transparency and data security. However, retention periods remain broadly defined rather than specific, security measures lack technical detail, and the policy disclaims responsibility for certain third-party breaches, which may weaken accountability expectations.

In relation to data subject rights, Wellkin Hospital and Clinique Darné continue to lead the sector, although both experienced a slight decline from 79% last year to 73% this year. Dr. Agarwal's Eye Hospital improved significantly from 53% to 67%, narrowing the gap with the sector leaders. Aegle Clinic again recorded 0%, reflecting the absence of any publicly articulated rights framework. While the leading institutions demonstrate structured recognition of rights, the marginal decline at Wellkin and Clinique Darné suggests stagnation rather than advancement in strengthening procedural clarity.

Third-party data sharing practices remain an area of moderate but incomplete compliance. Wellkin Hospital and Clinique Darné maintained their prior scores of 44%, continuing to lead the sector but without improvement. Dr. Agarwal's Eye Hospital showed substantial progress, rising from 10% last year to 36%, reflecting enhanced disclosure of sharing arrangements. Nevertheless, across all facilities, third-party transparency remains limited by the absence of exhaustive recipient lists and insufficient clarity on safeguards governing transfers. Aegle Clinic's continued absence of a privacy policy results in a sustained 0% score in this category.

Data security practices show more encouraging developments. Dr. Agarwal's Eye Hospital improved markedly from 61% to 78%, emerging as the leader in this metric. Wellkin Hospital and Clinique Darné maintained their previous scores of 61%, demonstrating stable but not advancing security posture. Aegle Clinic remained at 28%, reflecting minimal improvement in technical safeguards. While the sector shows measurable effort in cybersecurity practices, privacy policies across institutions continue to provide only general references to security measures without detailing breach response frameworks, timelines, or user notification procedures.

A significant positive development this year is the publication of transparency reports by Wellkin Hospital and Clinique Darné, both scoring 100% in this category compared to 0% last year. This represents a substantial improvement in accountability and public reporting practices. Dr. Agarwal's Eye Hospital and Aegle Clinic, however, continue to score 0%, indicating no movement toward structured transparency reporting.

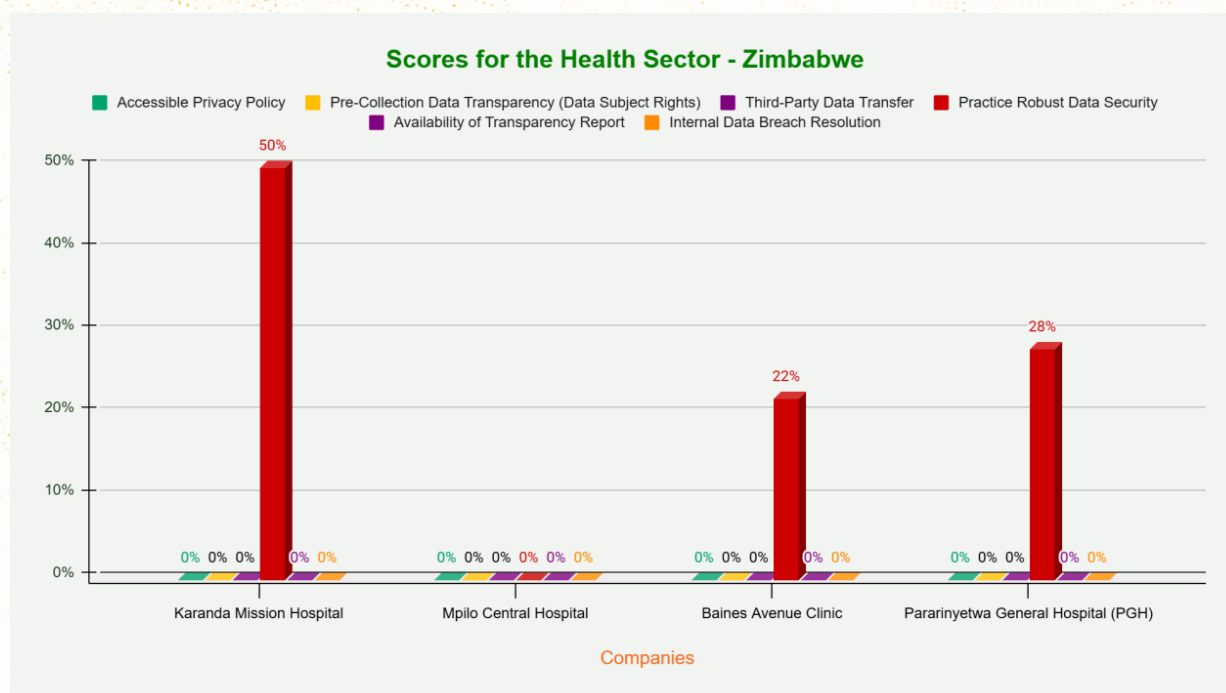
Internal data breach resolution mechanisms remain the weakest area of compliance across the sector. Dr. Agarwal's Eye Hospital improved from 0% to 33%, suggesting some development of internal grievance or response procedures. However, the framework remains incomplete and lacks detailed notification timelines and investigation protocols. Wellkin Hospital, Clinique Darné, and Aegle Clinic maintained scores of 0%, reflecting the absence of clearly articulated breach management systems. Despite general references to security, none of the policies provides comprehensive guidance on breach detection, user notification, or regulator reporting obligations.

Overall, the comparative analysis demonstrates that Mauritius' leading private hospitals continue to perform strongly in privacy policy accessibility and basic transparency, with incremental improvements in third-party disclosures and data security particularly at Dr. Agarwal's Eye Hospital. The introduction of transparency reporting by Wellkin Hospital and Clinique Darné marks meaningful progress since last year. However, persistent weaknesses in breach management, detailed security documentation, and retention specificity indicate that compliance remains partial rather than fully mature. Aegle Clinic's continued absence of a privacy policy highlights a clear outlier in sector performance and signals ongoing non-compliance.

While the sector shows comparatively stronger privacy governance than many peers, full alignment with data protection laws will require deeper institutionalization of breach response mechanisms, clearer documentation of retention and transfer safeguards, and consistent accountability reporting across all facilities. Without these reforms, even high-performing institutions remain exposed to regulatory scrutiny and reputational risk in the event of data protection failures.

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

The reassessment of Karanda Mission Hospital, Parirenyatwa General Hospital (PGH), Baines Avenue Clinic, and Mpilo Central Hospital indicates that Zimbabwe's health sector continues to exhibit systemic weaknesses in privacy governance, with no measurable progress since last year in core transparency and accountability indicators. The comparative analysis confirms that structural compliance gaps identified previously remain largely unaddressed.



For the second consecutive year, none of the assessed facilities has made visible effort to establish or publish accessible privacy policies. All four institutions maintained scores of 0% in this category. The absence of publicly available privacy notices means patients are not informed about how their personal and sensitive health data are collected, processed, stored, or shared. This sustained failure reflects non-compliance with fundamental data protection principles, particularly transparency and lawful processing obligations.

Similarly, performance in relation to data subject rights remains unchanged. All facilities again scored 0%, indicating that there are no visible mechanisms through which patients may exercise rights of access, correction, objection, or complaint. The absence of structured rights-management frameworks leaves data subjects without enforceable procedural protections and exposes institutions to potential legal and regulatory risk.

Third-party data sharing practices also show no meaningful improvement. All facilities maintained 0% in transparency and governance of third-party transfers. Although healthcare operations inherently require data sharing with laboratories, insurers, or service providers, none of the institutions provides public disclosure regarding such arrangements or associated safeguards. This continued opacity increases the risk of unauthorized disclosures and weakens accountability.

The only area where some measurable effort is observed is data security. Karanda Mission Hospital continues to lead the sector, maintaining its 50% score from last year. Parirenyatwa General Hospital retained its score of 28%, while Baines Avenue Clinic maintained 22%. Mpilo Central Hospital again scored 0%, reflecting no visible technical or organizational safeguards. Although these limited technical controls demonstrate some awareness of cybersecurity obligations, they remain isolated efforts unsupported by policy frameworks, documented procedures, or governance structures. As a result, even the highest-performing facility operates without a comprehensive privacy management system.

Transparency reporting and internal data breach resolution mechanisms remain entirely absent across the sector. As in the previous assessment, none of the facilities has published a transparency report, and none demonstrates documented breach detection, investigation, or notification procedures. This sustained absence of accountability mechanisms represents a critical compliance gap, particularly in light of statutory obligations to notify regulators and affected individuals in the event of a data breach.

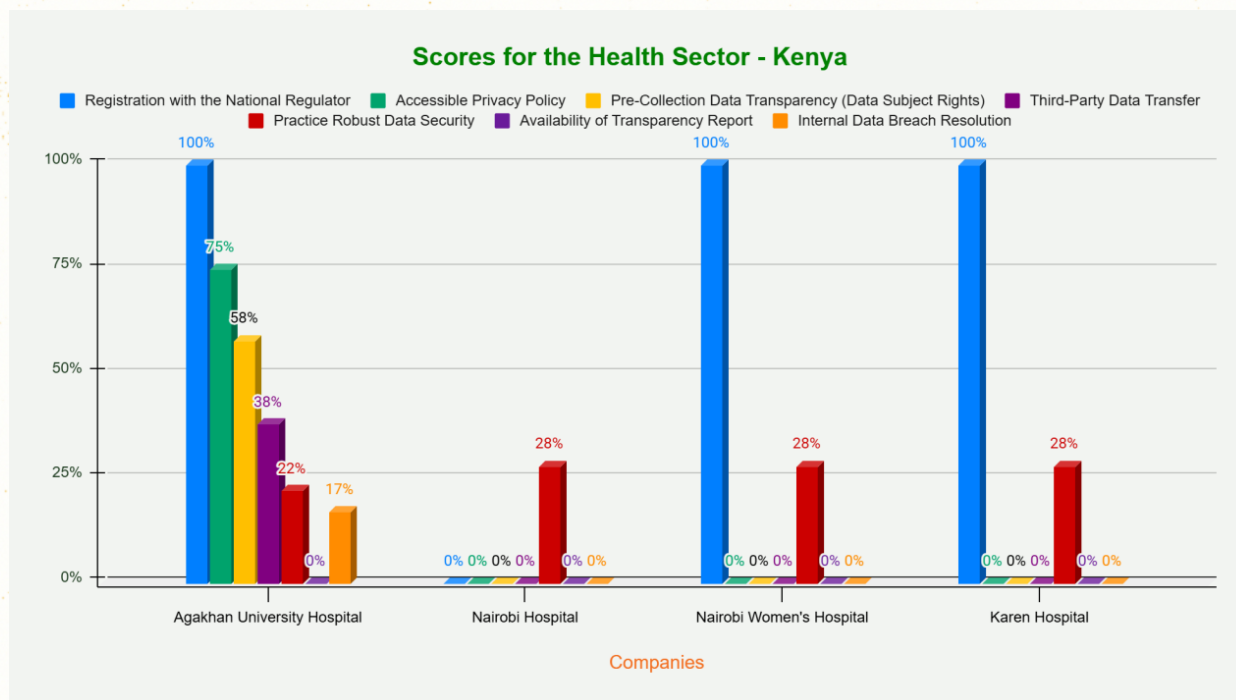
Compared to last year's findings, there has been no sector-wide improvement. Data security scores remain unchanged, and all other indicators including privacy policy accessibility, data subject rights, third-party governance, transparency reporting, and breach management continue to reflect total non-compliance. The stagnation suggests that privacy governance has not been institutionalized within the assessed facilities and that compliance efforts remain either minimal or nonexistent.

Overall, Zimbabwe's assessed healthcare institutions demonstrate a systemic absence of structured privacy and data protection management. Limited technical safeguards at a few facilities do not compensate for the lack of policy frameworks, accountability systems, or enforceable rights mechanisms. Without the introduction of accessible privacy notices, oper-

ational rights procedures, third-party governance controls, transparency reporting, and formal breach response systems, the sector remains highly vulnerable to regulatory enforcement, legal liability, and erosion of patient trust.

h. *Agakhan University Hospital, Nairobi Hospital, Nairobi Women's Hospital Karen Hospital in Kenya*

The reassessment of Aga Khan University Hospital, Nairobi Hospital, Nairobi Women's Hospital, and Karen Hospital indicates mixed progress within Kenya's healthcare sector, with improvements in regulatory registration but continued weaknesses in transparency, data governance, and breach accountability. When compared to last year's findings, the sector reflects incremental administrative compliance gains but regression in certain substantive privacy protections.



In relation to registration with the national regulator, there has been notable improvement. Aga Khan University Hospital and Karen Hospital maintained their perfect registration scores of 100%, consistent with last year's performance. Nairobi Women's Hospital demonstrated significant progress, improving from 0% to 100%, thereby aligning itself with statutory registration requirements. This marks a positive development in formal compliance with Kenya's Data Protection Act and oversight by the Office of the Data Protection Commissioner (ODPC). Nairobi Hospital's registration status, however, remains unchanged from last year. While improved registration strengthens regulatory visibility and accountability, registration alone does not equate to operational compliance.

Despite improvements in registration, transparency through accessible privacy policies remains limited. Aga Khan University Hospital continues to be the only facility with a publicly accessible privacy policy, maintaining its 75% score from last year. Nairobi Hospital, Nairobi Women's Hospital, and Karen Hospital again scored 0%, reflecting the absence of publicly available privacy notices. Given the sensitive nature of medical data processed including patient records, diagnostic results, and insurance information the absence of privacy policies at three major institutions represents a serious transparency failure and potential violation of statutory notice obligations.

Aga Khan University Hospital also remains the only institution demonstrating effort to operationalize data subject rights. However, its score declined slightly from 60% to 58%, suggesting stagnation rather than advancement in strengthening procedural clarity. While the hospital recognizes rights of access, correction, and other statutory protections, detailed guidance on timelines and complaint escalation remains limited. The other facilities maintained 0%, indicating no visible mechanisms for facilitating data subject rights. This sustained absence of rights-management systems exposes institutions to enforcement risk and undermines patient trust.

Third-party data sharing practices show marginal improvement only at Aga Khan University Hospital, which increased slightly from 36% to 38%. Although it provides some disclosure regarding third-party transfers, the safeguards remain incomplete and lack comprehensive identification of recipients or detailed transfer protections. Nairobi Hospital, Nairobi Women's Hospital, and Karen Hospital maintained 0%, offering no public transparency on third-party processing arrangements. In a healthcare ecosystem increasingly reliant on insurers, laboratories, digital health platforms, and cloud providers, the absence of clear third-party governance frameworks presents heightened compliance and security risks.

Data security performance reflects regression at previously stronger institutions. Aga Khan University Hospital's score dropped significantly from 56% to 22%, marking a concerning decline in demonstrable security posture. Karen Hospital also declined from 39% to 28%. Nairobi Hospital and Nairobi Women's Hospital maintained their prior scores of 28%. Although all institutions demonstrate some level of technical safeguards, overall performance remains modest, particularly in light of the statutory obligation to implement appropriate technical and organizational measures for sensitive health data. The decline at Aga Khan University Hospital is particularly notable given its prior leadership in this area.

Transparency reporting and internal data breach resolution mechanisms remain critically underdeveloped across the sector. As in the previous year, none of the facilities has published a transparency report. Internal breach management frameworks remain largely absent, with Aga Khan University Hospital's score declining from 25% to 17%, and all other institutions maintaining 0%. The absence of structured breach detection, notification timelines, and regulator reporting procedures represents a major compliance vulnerability under Kenya's data protection regime.

Comparatively, last year's analysis identified Aga Khan University Hospital as the clear sector leader across most metrics, with relatively stronger performance in privacy policy accessibility, third-party disclosures, breach management, and data security. In the current assessment, while the hospital maintains its leadership position in transparency and rights recognition, its decline in data security and breach management signals regression in operational safeguards. Nairobi Women's Hospital's improved registration status marks the most significant positive development this year, but it has not been accompanied by parallel improvements in transparency or rights facilitation.

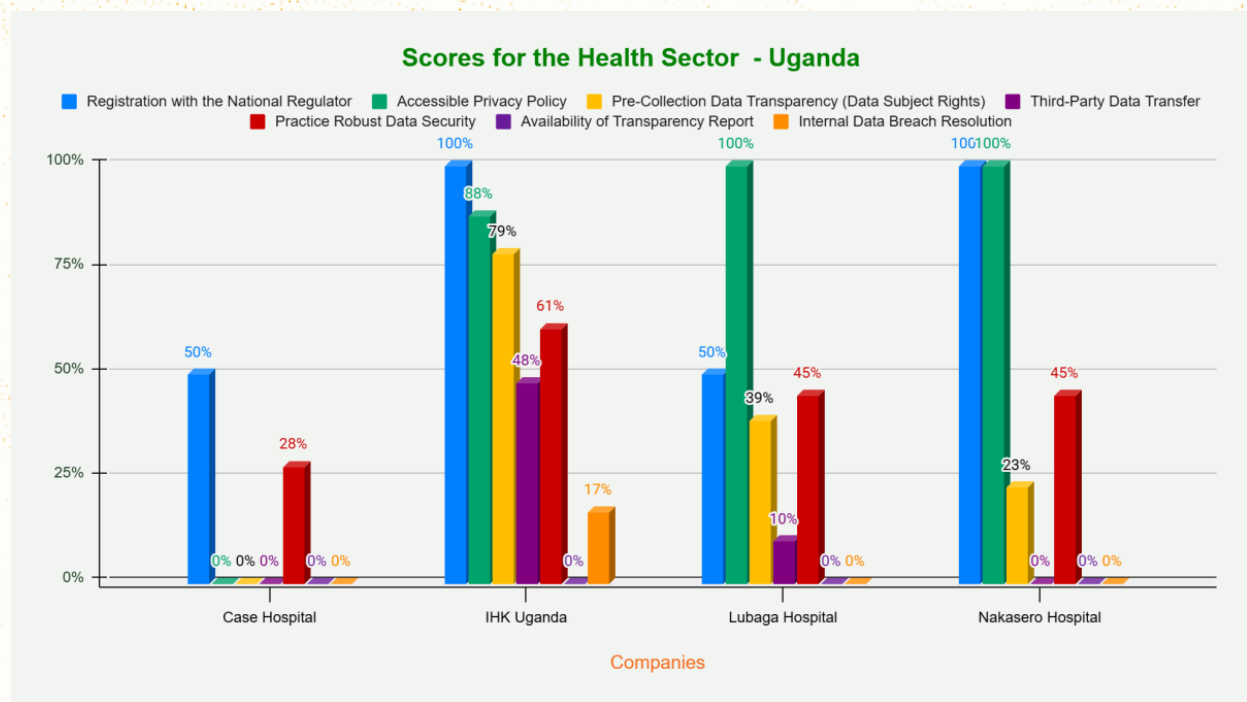
Overall, the healthcare sector's performance remains concerning. Although registration compliance has improved, substantive privacy governance particularly policy transparency, enforceable data subject rights, detailed third-party oversight, and structured breach response remains weak across most institutions. The processing of highly sensitive health data without accessible privacy notices or robust accountability frameworks exposes facilities to legal liability, regulatory sanctions, and reputational harm. As healthcare digitization accelerates through electronic medical records, telemedicine platforms, and integrated insurance systems, the need for comprehensive privacy governance becomes more urgent. Without sustained institutional commitment to strengthening operational compliance beyond basic registration, the sector risks falling short of both statutory requirements and patient trust expectations.

i. Case Hospital, IHK Hospital, Lubaga Hospital and Nakasero Hospital in Uganda

The reassessment of IHK Uganda, Nakasero Hospital, Lubaga Hospital, and Case Hospital indicates incremental progress in certain compliance areas, particularly registration and privacy policy publication, but continued weaknesses in accountability, third-party governance, and breach preparedness. Compared to last year's findings, the sector demonstrates modest structural improvements, although performance remains uneven and in several respects fragile.

With respect to registration with the national regulator (NPDPO), compliance levels have either been maintained or improved. IHK Uganda and Nakasero Hospital retained their perfect registration scores of 100%, reflecting continued adherence to formal regulatory requirements. Case Hospital maintained its 50% score, consistent with last year's inactive or partial registration status. Notably, Lubaga Hospital improved from 0% to 50%, marking progress toward regulatory formalization.

While these developments strengthen institutional legitimacy and regulatory oversight, registration alone does not ensure operational compliance with Uganda's data protection framework.



Significant movement was observed in the publication of accessible privacy policies. Lubaga Hospital recorded the most notable improvement, rising from 0% last year to 100%, while Nakasero Hospital improved from 88% to 100%. IHK Uganda, although still performing strongly at 88%, declined from last year's perfect score. Case Hospital continues to lack an accessible privacy policy, maintaining 0%. The improvement by Lubaga Hospital represents an important step toward transparency, given that the absence of a privacy notice last year was a critical compliance gap. However, the continued absence of a policy at Case Hospital remains a serious deficiency, particularly for an institution handling sensitive health data.

In the area of data subject rights, performance remains concentrated in a few institutions. IHK Uganda continues to lead, scoring 79%, though this reflects a slight decline from 81% last year. Its privacy framework recognizes rights of access, rectification, erasure, restriction, and complaint to the regulator, and provides multiple contact channels for its data protection office. Lubaga Hospital improved significantly from 0% to 39%, demonstrating growing recognition of statutory rights. Nakasero Hospital, however, declined from 36% to 23%, suggesting reduced clarity or visibility of its rights-management mechanisms. Case Hospital again recorded 0%, underscoring a continued absence of rights-based governance structures.

These disparities indicate that while some institutions are embedding rights-based compliance, sector-wide implementation remains inconsistent.

Third-party data sharing practices remain one of the weakest compliance areas. IHK Uganda improved modestly from 44% to 48%, maintaining its leadership in this category and disclosing that data may be shared with service providers and law enforcement upon lawful request, while excluding advertisers. Lubaga Hospital showed marginal progress from 0% to 10%. However, Nakasero Hospital's performance declined sharply from 60% last year to 0%, representing a significant regression in transparency regarding external data transfers. Case Hospital maintained 0%. Given the routine involvement of insurers, laboratories, and cross-border data hosting arrangements in healthcare delivery, the absence of clearly articulated third-party safeguards presents material legal and operational risk.

Data security remains the area of relatively strongest performance across the sector, though still at moderate levels. IHK Uganda maintained its leading position at 61%, consistent with last year. Lubaga Hospital improved from 39% to 45%, and Nakasero Hospital maintained 45%. Case Hospital remained at 28%, with its score largely attributable to SSL and basic technical safeguards rather than a documented organizational security framework. Although these results show stability or improvement in technical controls, they do not necessarily reflect comprehensive security governance, particularly in relation to documented risk assessments, incident response protocols, and staff training obligations required under data protection law.

As in the previous assessment, transparency reporting remains entirely absent across all four hospitals. None has published a transparency report. Internal data breach resolution mechanisms also remain largely undeveloped. IHK Uganda showed limited improvement, increasing from 0% to 17%, suggesting early steps toward breach management processes.

However, Lubaga Hospital, Nakasero Hospital, and Case Hospital maintained 0%, indicating no visible breach detection, reporting, or notification frameworks. The continued absence of structured breach response mechanisms represents one of the most significant compliance vulnerabilities in the sector, particularly given the sensitivity of health information and statutory notification obligations.

Institution-specific analysis reinforces these patterns. IHK Uganda continues to demonstrate the most comprehensive privacy governance framework. Its privacy policy is accessible and readable, clearly defines categories and purposes of data collection, provides opt-out options for behavioural marketing, subjects retention to legal requirements, and specifies lawful disclosures, including court-ordered access. However, it still lacks detailed breach handling procedures, limiting its overall accountability posture. Lubaga Hospital's improvements in policy publication and rights recognition are commendable, but weaknesses in third-party governance and breach management constrain its compliance maturity. Nakasero Hospital maintains strong registration and policy accessibility but has regressed in third-party transparency and data subject rights clarity. Case Hospital remains the weakest performer, with no accessible privacy policy, no articulated third-party framework, no rights mechanisms, and minimal security safeguards beyond technical encryption.

Compared to last year, the most notable positive changes include Lubaga Hospital's introduction of a privacy policy and improved rights recognition, IHK Uganda's modest progress in breach management, and slight improvements in third-party disclosures. However, the decline in Nakasero Hospital's third-party transparency and the continued absence of accountability mechanisms across most institutions temper these gains.

Overall, Uganda's private healthcare sector demonstrates partial progress in transparency and formal compliance but remains significantly deficient in accountability, breach preparedness, and comprehensive third-party governance. While policy publication has improved, particularly at Lubaga Hospital, effective implementation mechanisms remain underdeveloped. Without strengthened breach management systems, clearer third-party controls, and sustained enforcement oversight, healthcare providers remain exposed to regulatory liability and reputational harm, and patient data protection remains inadequately safeguarded.

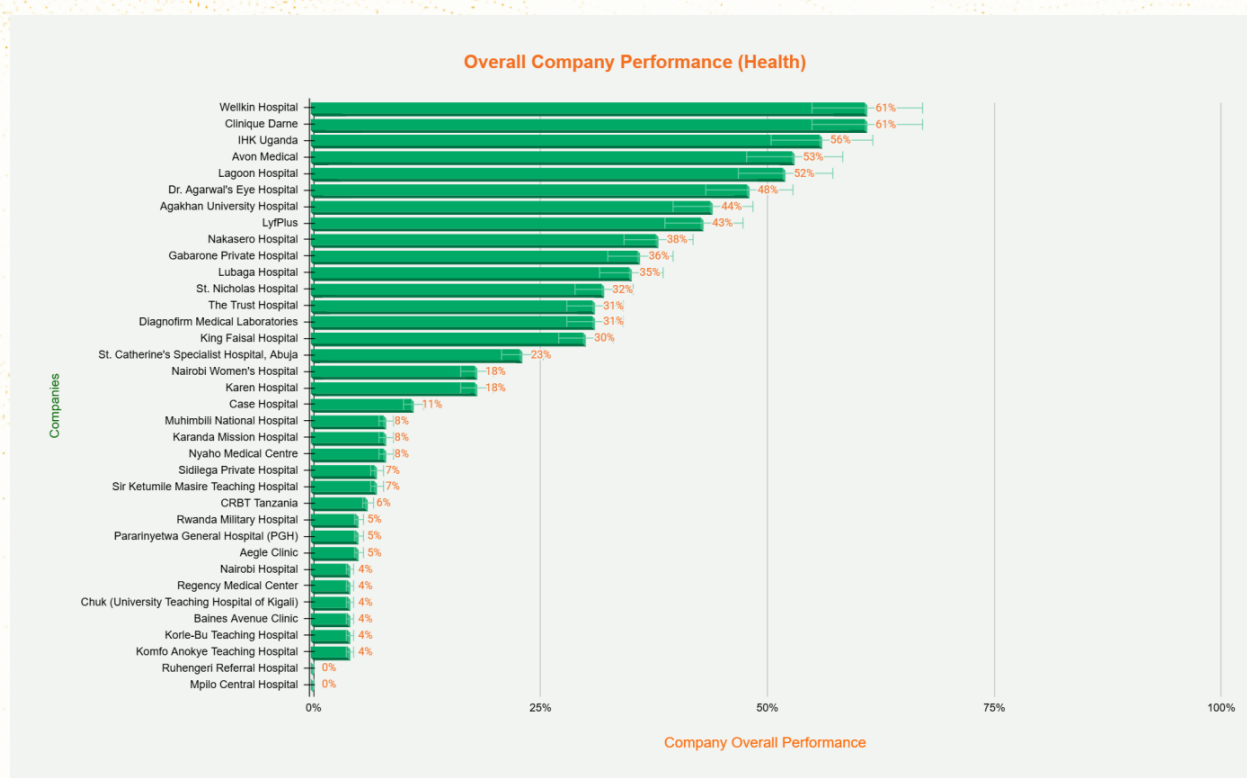
3.4.7.3 Comparison of companies/entities within the sector

High-Performing Jurisdictions: Emerging Compliance Leaders and Trajectories

Mauritius and, to a lesser extent, Uganda and Nigeria now emerge as the strongest-performing jurisdictions in the health sector, although overall compliance remains moderate rather than robust.

Mauritius leads the sector, with Wellkin Hospital and Clinique Darne both scoring 61%, improving from last year's mid-40% range. This upward trajectory suggests more consistent implementation of privacy policies, stronger data security controls, and greater institutional awareness of health data protection obligations. Dr. Agarwal's Eye Hospital (48%) also shows improvement from last year's lower scores, although Aegle Clinic (5%) demonstrates that compliance maturity is uneven even within higher-performing jurisdictions.

Uganda shows incremental progress at the upper end. IHK Uganda (56%) has marginally improved from 55%, consolidating its position as a relative sector leader. However, other Ugandan facilities, such as Nakasero Hospital (38%) and Lubaga Hospital (35%), have declined or stagnated compared to last year, indicating that gains are not yet sector-wide.



Nigeria's leading private hospitals; Avon Medical (53%) and Lagoon Hospital (52%) now score above 50%, reflecting moderate improvements from last year's high-40% range. These scores indicate growing recognition of patient data rights and improved security practices, though compliance remains incomplete.

Despite these positive developments, no health facility exceeds 61%, underscoring that even emerging leaders remain only partially aligned with data protection laws governing sensitive health information.

Mid-Range Performers: Partial Compliance and Structural Gaps (Change Over Time)

Most health facilities cluster within the mid-range (30%–45%), reflecting partial compliance and slow progress over time.

Kenya exemplifies this pattern. Aga Khan University Hospital (44%) has declined from last year's 50%, suggesting stagnation or regression in privacy governance. Nairobi Women's Hospital and Karen Hospital remain low at 18%, though marginally improved from last year's lowest scores, highlighting persistent inconsistencies within the same regulatory environment.

Tanzania also remains largely mid-to-low performing. LyfPlus (43%) shows slight improvement from 40%, but major public facilities such as Muhimbili National Hospital (8%) and Regency Medical Center (4%) remain critically weak, with little evidence of sustained reform.

Botswana and Ghana similarly exhibit mixed mid-range performance. Gaborone Private Hospital (36%) and Diagnofirm Medical Laboratories (31%) show modest gains, while Ghana's Trust Hospital (31%) has stagnated or declined slightly from last year's mid-30% range.

Across this tier, improvements tend to be limited to baseline measures such as privacy policy availability or basic security controls. Structural gaps persist in consent management, breach response, staff accountability, and transparency around data sharing.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

A substantial number of health facilities continue to exhibit systemic compliance failures, particularly in public and teaching hospitals, with scores below 20% and, in some cases, at or near zero.

Rwanda's public hospitals including Rwanda Military Hospital (5%), CHUK (4%), and Ruhengeri Referral Hospital (0%) remain among the weakest performers, showing little improvement from last year. Zimbabwe presents a similarly concerning picture, with Mpilo Central Hospital (0%), Parirenyatwa General Hospital (5%), and Baines Avenue Clinic (4%) reflecting entrenched deficiencies in privacy governance.

In Kenya, Nairobi Hospital (4%) remains critically non-compliant, showing no meaningful improvement year-on-year. Ghana's major public hospitals, Korle-Bu Teaching Hospital and Komfo Anokye Teaching Hospital (both at 4%) also remain extremely weak, despite the sensitive and large-scale processing of health data.

These persistently low scores point to systemic challenges, including limited institutional capacity, weak enforcement of data protection laws, and lack of prioritisation of patient data rights in public health systems.

Key Cross-Cutting Implications

Several cross-cutting implications emerge across the health sector. First, overall performance remains low relative to the sensitivity of health data, with no facility demonstrating strong compliance with data protection laws. Even the highest scores reflect partial and fragile compliance.

Second, year-on-year improvements are concentrated among a small number of private facilities, while public hospitals consistently underperform.

This suggests structural and resourcing constraints, rather than lack of legal frameworks, are driving non-compliance in many jurisdictions.

Third, accountability mechanisms such as transparency reporting, internal breach response procedures, and clear data-sharing disclosures remain largely absent across all performance tiers. These gaps significantly increase the risk of data breaches, misuse of patient information, and erosion of public trust.

In conclusion, while modest progress is visible in a few jurisdictions, the health sector remains one of the most vulnerable in terms of privacy and data protection compliance. Without targeted regulatory enforcement, sector-specific guidance, and sustained investment in privacy-by-design practices, patient data across East and Southern Africa will continue to face elevated legal, ethical, and security risks.

3.4.8 Digital Loans Sector Analysis

3.4.8.1 Overview of the sector and data collectors evaluated

The digital loan sector in East, Southern, and West Africa has grown rapidly, driven by mobile technology, fintech innovation, and limited access to traditional banking. Countries such as Kenya, Uganda, Tanzania, Rwanda, Mauritius, Zimbabwe, Nigeria, Ghana, and Botswana increasingly rely on mobile-based lending platforms to expand financial inclusion. Kenya and Nigeria lead in market maturity, while Rwanda, Mauritius, and Botswana show steady growth under evolving regulatory frameworks. Ghana and Zimbabwe's markets are developing, often amid economic or regulatory challenges.

While digital lending improves access to credit, it relies heavily on collecting sensitive personal and financial data including mobile records, transactions, geolocation, and social media activity which raises significant privacy and consumer protection concerns. Data protection laws exist across the region, but enforcement and sector-specific oversight remain uneven. Kenya and Nigeria have taken some regulatory action, whereas Uganda, Tanzania, Zimbabwe, Ghana, and Botswana face monitoring limitations. Even in more regulated countries like Rwanda and Mauritius, rapid fintech growth challenges compliance.

Common risks include limited transparency, inadequate consent for data sharing, weak security safeguards, inaccessible or incomplete privacy policies, and aggressive debt recovery practices that may violate privacy rights. Cross-border operations further complicate enforcement, leaving consumers with few avenues for redress. Overall, the sector highlights a dual reality: it promotes financial inclusion but exposes borrowers to privacy, security, and regulatory risks.

Strengthening enforcement, improving transparency, and implementing sector-specific guidance are critical to ensure digital lending supports inclusion without compromising consumer protection.

Analysis of compliance with each criterion

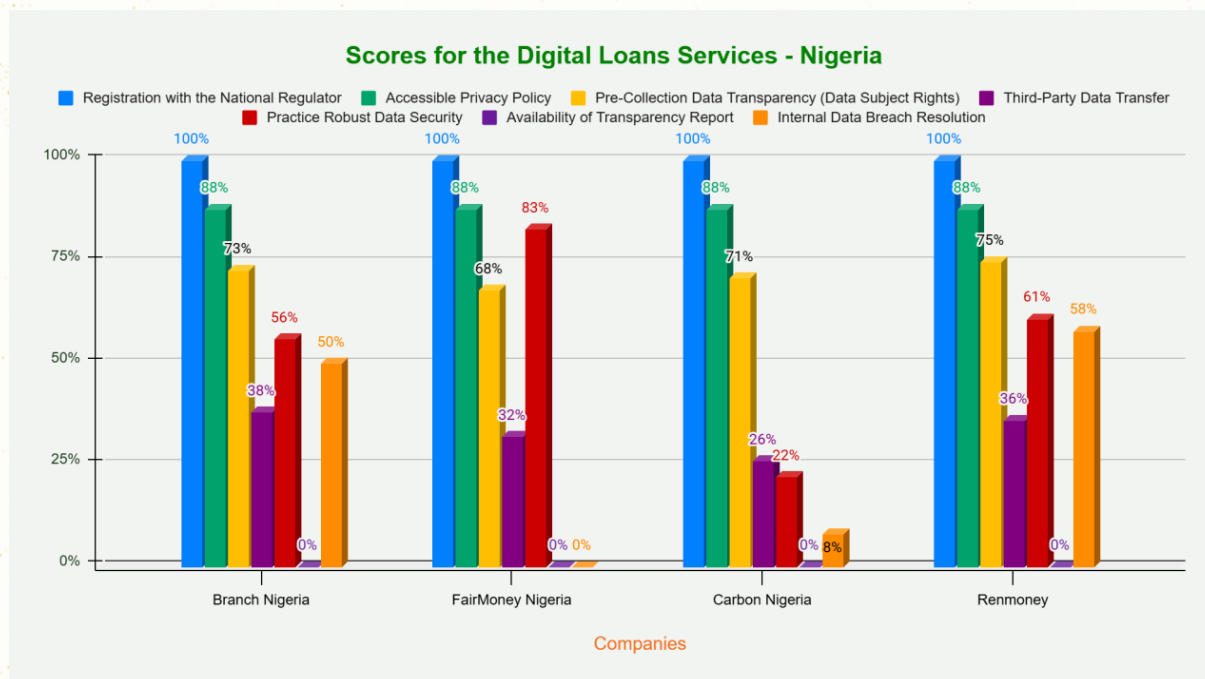
This assessment covers a total of 36 digital lending entities, with four platforms selected from each participating country. From Nigeria, the platforms assessed were Branch Nigeria, FairMoney Nigeria, Carbon Nigeria, and Renmoney. Ghana was represented by Fido Ghana, M-Kopa Ghana, CedisPay, and Izwe Ghana. In Botswana, the selected entities were Pachi Micro Solutions, Letshego, Bayport Botswana, and ExpressCredit Botswana. Rwanda's sample included Spenn, Save, Kiva, and Pezesha Rwanda.

For Tanzania, the assessment covered PesaX Tanzania, Branch International Tanzania, MkopoWako Tanzania, and TwigaLoan. Mauritius was represented by Finclub, Fundkiss, and Cim Finance. Zimbabwe's platforms included Ecocash, Zi-

buko Capital, InnBucks, and eShagi. In Kenya, the selected entities were Branch International Kenya, Tala Kenya, Zenka, and LendPlus. Finally, Uganda's sample comprised Dove Cash, Mango Cash, iSente, and Quick Sente.

a. *Branch Nigeria, FairMoney Nigeria, Carbon Nigeria and Renmoney in Nigeria*

The assessment of the four digital lending platforms reveals a sector that has achieved formal compliance with foundational regulatory requirements but continues to face significant operational and accountability gaps in core areas of data protection. All assessed platforms fulfilled registration requirements with the national data protection regulator, each attaining a perfect score. This demonstrates clear awareness of statutory obligations and formal alignment with regulatory expectations.



In addition, all platforms made their privacy policies accessible, reflecting a commitment to basic transparency. However, while accessibility was consistent, the depth, clarity, and operational substance of these policies varied considerably.

Across the platforms, there was visible effort to recognize and implement data subject rights. Renmoney recorded the highest score in this area, followed closely by Branch Nigeria, Carbon Nigeria, and FairMoney Nigeria. These results indicate a growing sector-wide awareness of the importance of enabling individuals to access, correct, or request deletion of their personal data and to escalate complaints where necessary. Nonetheless, the moderate range of scores suggests that implementation frameworks remain underdeveloped in certain respects. Mechanisms such as defined response timelines, structured escalation procedures, and clear articulation of legal limitations require further strengthening to ensure that rights are not only acknowledged in policy but consistently operationalized in practice.

The most significant area of concern across all platforms relates to third-party data sharing. Digital lending operations inherently involve extensive information exchange with credit bureaus, verification services, collection agencies, analytics providers, and regulatory authorities. Despite this, compliance performance in this category was uniformly low. Branch Nigeria recorded the highest score among the four, followed by Renmoney, FairMoney Nigeria, and Carbon Nigeria, but all scores remained below acceptable thresholds for a high-risk sector. This pattern indicates systemic weaknesses in third-party governance, including limited disclosure of data processing safeguards, insufficient clarity around cross-border transfers, and inadequate evidence of structured oversight mechanisms. Given the volume and sensitivity of borrower data processed including identity documents, Bank Verification Numbers, financial histories, device information, and behavioral analytics weak third-party governance substantially heightens regulatory, operational, and reputational risk.

Performance in data security measures was uneven across the platforms. FairMoney Nigeria achieved the highest score in this category, suggesting relatively stronger technical and organizational safeguards. Renmoney and Branch Nigeria demonstrated moderate levels of data security implementation, while Carbon Nigeria's score was significantly lower. Considering the sensitive nature of financial and identity data handled by digital lenders, gaps in documented security controls and risk-based safeguards create material exposure to unauthorized access, fraud, and regulatory sanctions.

The disparity in scores highlights inconsistent sector maturity in applying comprehensive data protection safeguards.

Transparency and breach accountability mechanisms also remain underdeveloped. None of the assessed platforms currently publishes a transparency report, limiting public insight into data practices, government requests, or incident management statistics. While some platforms demonstrated effort to establish internal data breach resolution mechanisms, the maturity of these frameworks varies considerably. Renmoney and Branch Nigeria show developing internal processes, whereas Carbon Nigeria and FairMoney Nigeria scored extremely low in this area. Given statutory obligations to notify regulators and, where applicable, affected data subjects within prescribed timelines, weak breach management structures create significant compliance vulnerability.

At an individual platform level, Renmoney demonstrates relatively stronger privacy governance within the high-risk digital lending environment. Its privacy documentation reflects awareness of the extensive categories of data collected and provides detailed explanations of processing purposes, including credit assessment, fraud prevention, loan servicing, debt recovery, and regulatory compliance. The company outlines defined retention periods, such as maintaining credit records for the duration of the loan relationship plus five years, and provides for deletion of marketing data upon request. It also describes its third-party relationships with relative clarity and offers multiple channels for data subject engagement and complaint escalation.

Although improvements are still required in third-party governance and public transparency, Renmoney reflects comparatively high privacy maturity.

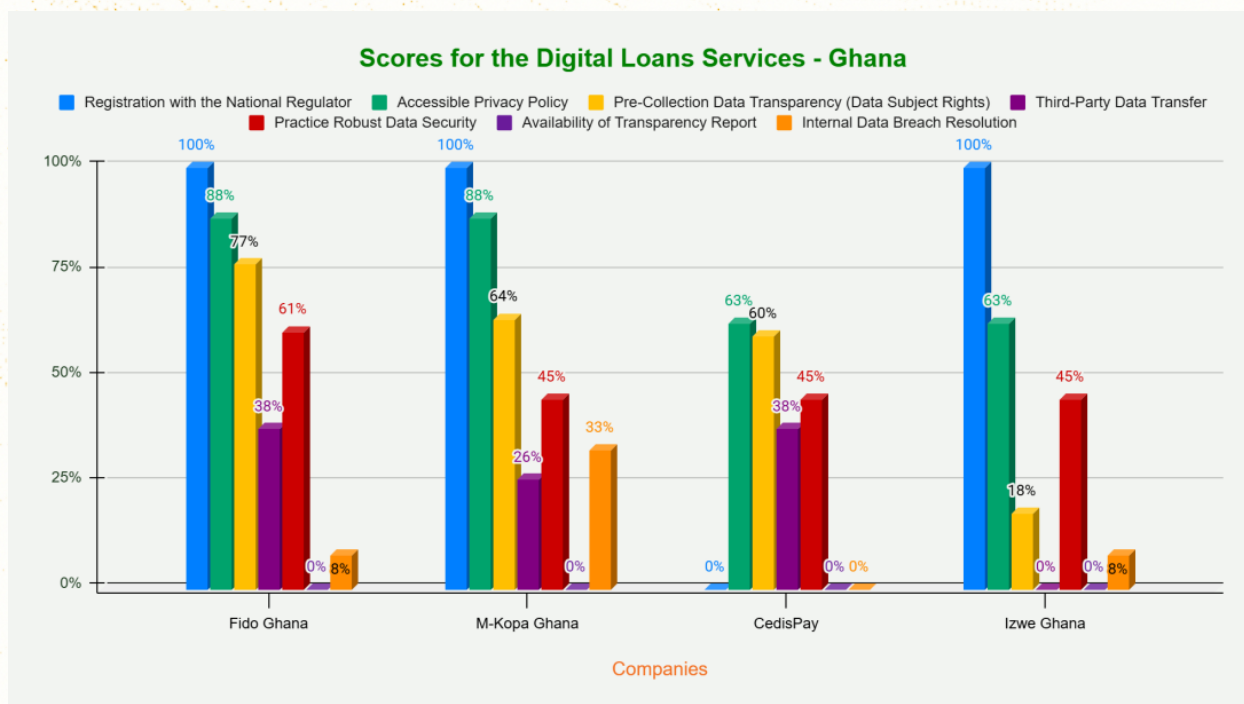
Branch Nigeria demonstrates moderate compliance, with policies addressing core requirements for digital lending operations. The company outlines general categories of borrower data collected and identifies primary purposes of processing, such as credit assessment and loan management. While it acknowledges third-party sharing arrangements and provides basic rights mechanisms, disclosures relating to retention timelines and structured governance processes are less comprehensive, suggesting that compliance structures are present but not fully institutionalized.

FairMoney Nigeria similarly reflects moderate compliance. It provides contact information, acknowledges extensive data collection for credit assessment, and demonstrates comparatively strong performance in data security measures. However, transparency around retention practices, third-party safeguards, and breach management mechanisms remains limited. As a result, although certain technical safeguards appear robust, governance documentation and accountability frameworks require further development.

Carbon Nigeria demonstrates basic compliance but lacks the depth and comprehensiveness expected for a platform engaged in extensive financial data processing. While fundamental disclosures are present, its overall privacy framework appears underdeveloped relative to the operational risks inherent in digital lending. Low performance in third-party governance, data security, and breach management suggests elevated regulatory and operational exposure.

Overall, the sector exhibits strong formal compliance in terms of registration and policy publication but weaker operational compliance in high-risk areas such as third-party oversight, breach accountability, and structured security governance. The absence of transparency reporting further limits public accountability. While there is clear awareness of data protection obligations, compliance maturity remains uneven and, in some instances, fragile. Strengthening third-party governance frameworks, formalizing breach response procedures, enhancing transparency, and embedding risk-based security controls would significantly improve alignment with data protection laws and reduce regulatory exposure across Nigeria's digital lending ecosystem.

b. *Fido Ghana, M-Kopa Ghana, CedisPay and Izwe Ghana in Ghana*



The assessment of four digital lending platforms operating in Ghana (Fido Ghana, M-Kopa Ghana, CedisPay, and Izwe Ghana) reveals a sector that demonstrates partial structural compliance with data protection requirements, but with significant weaknesses in operational transparency, third-party governance, and breach accountability. While certain platforms reflect growing privacy maturity, the overall compliance landscape remains uneven and, in some cases, fragile.

Three of the four assessed platforms (Fido Ghana, M-Kopa Ghana, and Izwe Ghana) have fulfilled registration requirements with the national data protection regulator, each attaining a perfect score. Their registrations remain valid through late 2026, reflecting formal recognition of statutory obligations and alignment with foundational regulatory requirements. In contrast, CedisPay is not registered and remains inactive, representing a critical compliance failure. As of July 15, 2025, this pattern suggests a generally positive sectoral trend toward formal compliance, but also highlights the regulatory risk posed by entities operating without registration.

All four platforms maintain publicly available privacy policies, although visibility and accessibility vary. Fido Ghana and M-Kopa Ghana lead in accessibility and readability, followed by CedisPay and Izwe Ghana. While the presence of policies indicates awareness of transparency obligations under Ghana's data protection framework, the quality and comprehensiveness of disclosures differ substantially. Fido Ghana demonstrates relatively strong transparency, providing detailed descriptions of data categories collected and outlining extensive user rights.

However, its retention timelines are vaguely defined, and it lacks a clearly articulated complaint mechanism. M-Kopa Ghana offers comprehensive disclosures, including recognition of regulator complaint channels and structured user rights, but permits third-party marketing with consent and provides limited clarity regarding law enforcement access. CedisPay clearly describes data categories, purposes of processing, and certain third-party disclosures while barring advertisers; however, it omits opt-in or opt-out controls for marketing, fails to define retention timelines in detail, and does not adequately outline complaint rights. Izwe Ghana performs weakest in this area, offering only broad descriptions of data collection, vague retention standards, extensive third-party and advertiser sharing provisions, and minimal recognition of core data subject rights or law enforcement disclosure conditions.

Implementation of data subject rights across the platforms reflects similar disparities. Fido Ghana records the strongest performance in this category, followed by M-Kopa Ghana and CedisPay, while Izwe Ghana scores significantly lower. Although all platforms demonstrate some effort to acknowledge user rights, Izwe's limited recognition of core rights raises substantial concerns regarding compliance with statutory obligations relating to access, rectification, erasure, and objection to processing. These gaps undermine accountability and reduce users' practical ability to exercise control over their personal data.

Third-party data sharing represents one of the most significant compliance risks across the sector. All four platforms share personal data with external entities as part of their lending operations, yet compliance scores in this category re-

main low. Fido Ghana and CedisPay record the highest performance, though still below acceptable levels, followed by M-Kopa Ghana, while Izwe Ghana scores zero. Fido permits sharing with affiliates, vendors, service providers, payment processors, credit bureaus, and government authorities, but does not name specific entities and lacks clear reporting channels for misuse or breach. M-Kopa shares data with service providers, credit agencies, debt collectors, and, with consent, marketing companies, yet does not clearly specify the categories of data shared or the conditions governing law enforcement access. CedisPay allows transfers to telecom operators, utilities, mobile money providers, and subcontractors, excluding advertisers, and limits law enforcement access to formal legal obligations. Izwe Ghana allows broad sharing, including cross-border transfers and disclosures in the context of business transfers, but provides virtually no detail on specific third parties, categories of shared data, safeguards, or reporting channels.

The low compliance levels in this area expose facilities to elevated regulatory and reputational risks, particularly given the sensitivity of financial and identity data processed in digital lending.

In relation to data security, all platforms demonstrate some level of technical implementation, particularly in SSL certification. Fido Ghana holds an A+ SSL rating and references encryption and authorized access controls in its privacy documentation, resulting in the highest overall security score among the group. M-Kopa Ghana, CedisPay, and Izwe Ghana each maintain A-level SSL ratings but perform poorly in security header configurations and provide only general references to security safeguards without specifying encryption standards, access controls, or documented breach response procedures. Although SSL implementation indicates baseline transport-layer protection, weak header configurations and vague policy disclosures reduce overall confidence in the robustness of security frameworks and limit demonstrable compliance with the requirement to implement appropriate technical and organizational safeguards.

Transparency and accountability mechanisms remain underdeveloped across all four platforms. None has published a transparency report detailing data-sharing requests, government access demands, or incident statistics. The absence of such reporting limits public oversight and reduces demonstrable accountability under data protection principles.

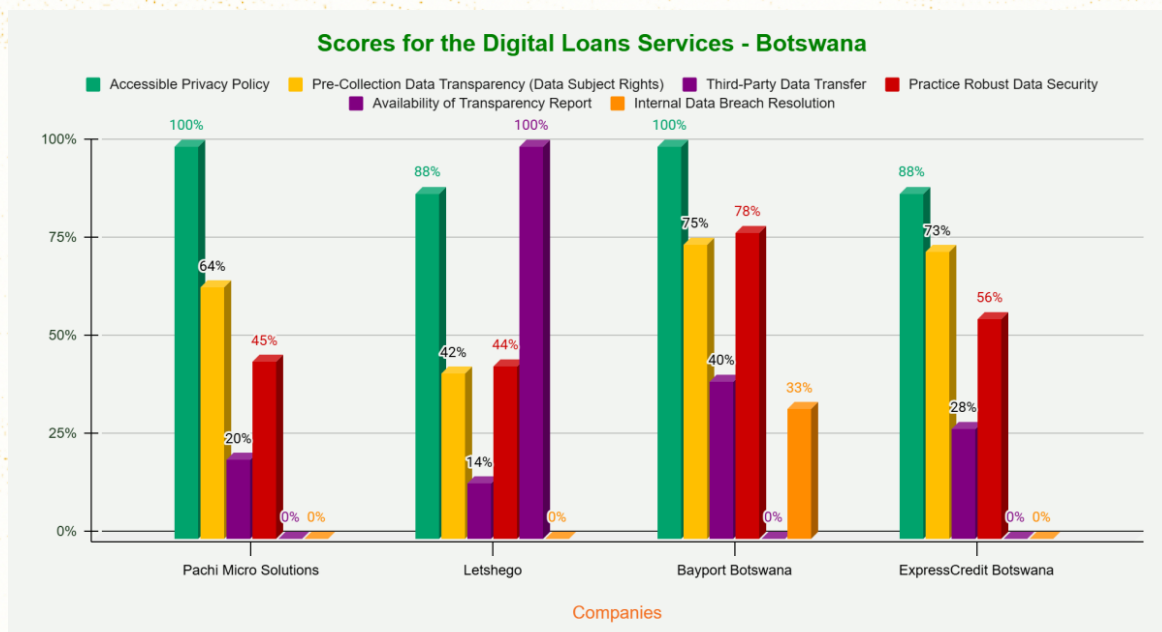
Internal data breach resolution mechanisms show similarly weak performance. M-Kopa Ghana records the strongest score in this category, providing multiple reporting channels including email, hotlines, and physical contacts. However, it does not clearly define investigation timelines, procedural safeguards, or notification obligations. Fido Ghana emphasizes technical safeguards such as SSL encryption but provides minimal detail regarding internal breach procedures, timelines, user notification protocols, or escalation pathways. Izwe Ghana references general technical and organizational measures but offers very limited procedural guidance on incident handling. CedisPay provides no meaningful guidance on breach reporting or management. These deficiencies create significant compliance exposure, particularly in light of statutory obligations requiring timely regulator notification and, where applicable, communication to affected data subjects.

Overall, the assessment indicates that while formal compliance indicators such as registration and policy publication, are present in most cases, substantive operational compliance remains inconsistent. The strongest performers, particularly Fido Ghana and M-Kopa Ghana, demonstrate growing privacy governance maturity but still exhibit weaknesses in retention clarity, third-party specificity, and breach procedural transparency. CedisPay's lack of registration and absence of breach governance represent critical compliance failures. Izwe Ghana's limited recognition of data subject rights and minimal third-party accountability create elevated regulatory risk.

The principal implications for privacy practices within Ghana's digital lending sector are clear. Third-party governance remains insufficiently structured, breach response frameworks are inadequately documented, and transparency reporting is entirely absent. While technical safeguards such as SSL are widely implemented, broader organizational and procedural controls require strengthening to ensure full alignment with Ghana's data protection laws. Without improvements in accountability, procedural clarity, and demonstrable oversight, the sector remains vulnerable to regulatory enforcement, reputational harm, and diminished user trust.

c. Pachi Micro Solutions, Letshego, Bayport Botswana and ExpressCredit Botswana in Botswana

The assessment of the four lending institutions operating in Botswana (Pachi Micro Solutions, Bayport Botswana, Letshego, and ExpressCredit Botswana) reveals significant structural weaknesses in regulatory compliance, despite observable efforts in certain areas of privacy governance. While some institutions demonstrate emerging maturity in policy development and security safeguards, the absence of demonstrable registration compliance and weak accountability mechanisms present substantial regulatory and operational risks.



Most notably, there was no evidence to demonstrate compliance with registration requirements with the national data protection regulator for any of the assessed institutions. This represents a foundational compliance gap. Registration is a core statutory obligation under data protection law and serves as the basis for regulatory oversight and accountability. The absence of verifiable registration raises concerns about formal recognition of data processing activities and may expose the institutions to enforcement action, penalties, and reputational harm. It also signals potential weaknesses in internal compliance governance structures.

Despite this fundamental gap, all institutions have made efforts to provide accessible privacy policies. Pachi Micro Solutions and Bayport Botswana lead in this area, each achieving full scores for accessibility, while Letshego and ExpressCredit Botswana scored slightly lower but still reflect strong visibility and availability of privacy notices. This indicates sector-wide awareness of transparency obligations and a willingness to inform customers about data practices. However, the presence of accessible policies does not necessarily equate to substantive compliance, as effectiveness depends on the depth, clarity, and operational alignment of the disclosures.

In terms of data subject rights, there is demonstrable but uneven progress. Bayport Botswana records the strongest performance, followed closely by ExpressCredit Botswana and Pachi Micro Solutions, while Letshego trails significantly. The results suggest that while mechanisms for access, correction, and other user rights are acknowledged in several cases, implementation maturity varies. Lower scores indicate that some institutions may lack clearly defined procedures, timelines, or escalation channels necessary to give full practical effect to statutory rights. This inconsistency weakens accountability and may limit data subjects' ability to exercise meaningful control over their personal information.

Third-party data sharing emerges as one of the most critical areas of concern across all institutions. Each platform engages in data sharing with external parties, which is typical within lending operations involving credit bureaus, service providers, and other financial intermediaries. However, compliance scores in this category are uniformly low. Bayport Botswana performs comparatively better than its peers, yet still achieves only a modest score, followed by ExpressCredit Botswana, Pachi Micro Solutions, and Letshego with progressively weaker results. These findings indicate limited transparency regarding the categories of third parties engaged, the specific data shared, applicable safeguards, and oversight mechanisms.

Weak governance of third-party relationships significantly heightens regulatory risk, particularly given the sensitivity of financial and identity data processed by lending institutions.

Data security measures reflect comparatively stronger performance across the institutions, though important gaps remain. Bayport Botswana leads in this category, suggesting more structured technical and organizational safeguards. ExpressCredit Botswana demonstrates moderate security implementation, while Pachi Micro Solutions and Letshego show similar but less robust performance. Although these results indicate awareness of the obligation to protect personal data through appropriate safeguards, the variation in scores suggests inconsistent application of risk-based security controls. In a sector handling sensitive financial data, insufficiently documented or implemented safeguards could undermine compliance with statutory security requirements.

Transparency and accountability mechanisms are notably underdeveloped. None of the assessed institutions has published a transparency report detailing government data requests, third-party disclosures, or data protection performance metrics. The absence of such reporting limits public oversight and reduces demonstrable accountability.

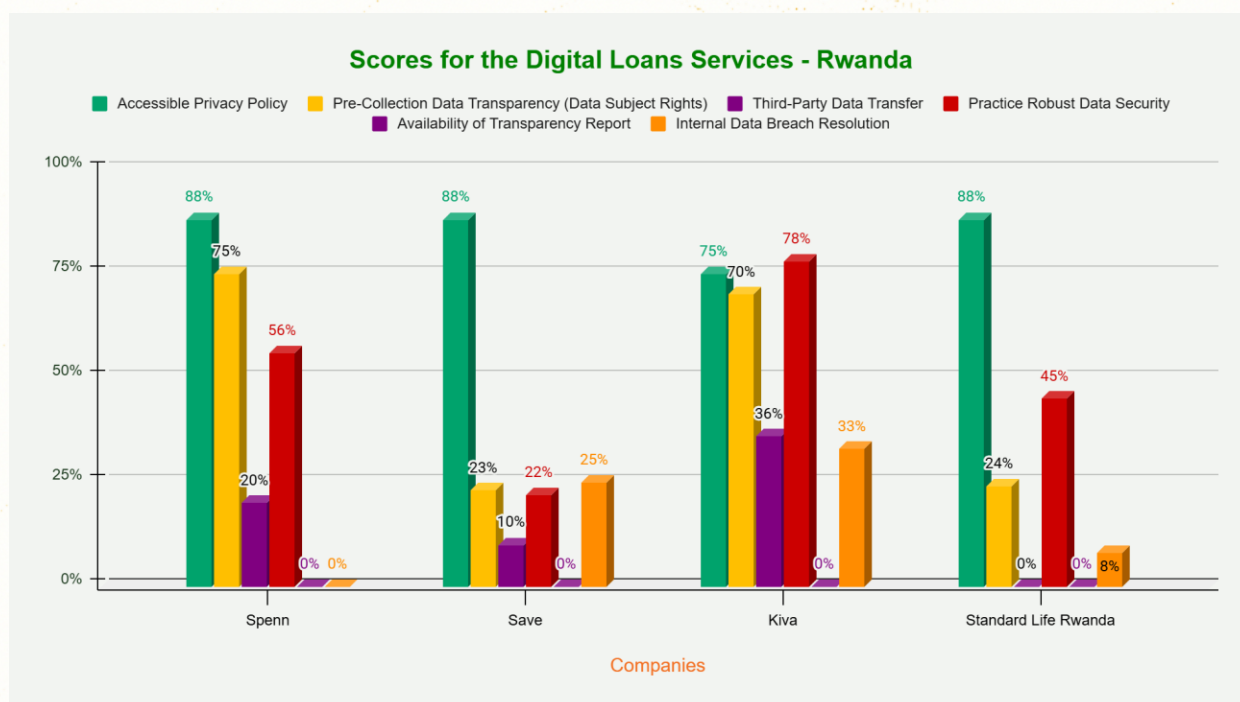
Similarly, internal data breach resolution mechanisms are largely inadequate. Bayport Botswana is the only institution that demonstrates visible effort in this area, yet its score remains modest. The remaining institutions show no measurable evidence of structured breach response frameworks. Given statutory obligations to detect, investigate, and notify regulators and affected individuals of qualifying data breaches within prescribed timelines, the absence of documented breach procedures presents significant compliance exposure. Weak incident response governance increases the risk of delayed notification, regulatory penalties, and erosion of customer trust.

Overall, the findings indicate that while Botswana's lending sector shows progress in policy accessibility and, to some extent, data security, it lacks foundational regulatory alignment and robust accountability structures. The absence of verifiable registration compliance is particularly concerning, as it undermines the legitimacy of other privacy efforts. Furthermore, weak third-party governance, limited breach response mechanisms, and the absence of transparency reporting collectively point to immature privacy management frameworks.

For these institutions to achieve meaningful compliance with data protection laws, priority attention must be given to formal regulatory registration, strengthening third-party oversight arrangements, institutionalizing structured breach response procedures, and enhancing demonstrable accountability. Without these improvements, the sector remains exposed to regulatory enforcement, operational disruption, and diminished stakeholder confidence.

d. *Spenn, Save, Kiva and Standard Life Rwanda in Rwanda*

The 2025 assessment of digital lending and financial service platforms in Rwanda (Spenn, Save, Kiva, and Standard Life Rwanda) indicates incremental progress in certain aspects of privacy governance when compared with the previous year, but also reveals persistent structural weaknesses that continue to undermine full compliance with data protection laws. While there are measurable improvements in transparency, user rights articulation, and technical safeguards for some providers, core accountability mechanisms remain underdeveloped, and foundational regulatory compliance gaps persist.



Most significantly, there was no evidence to demonstrate compliance with registration requirements with the national data protection regulator for any of the assessed institutions. This mirrors the concern identified in the prior review, where regulatory alignment was also weak. The continued absence of demonstrable registration compliance represents a fundamental legal risk. Registration is not merely administrative; it anchors regulatory oversight, affirms lawful processing status, and signals institutional commitment to data governance. Its absence undermines other privacy efforts and exposes the facilities to potential enforcement action.

In terms of accessible privacy policies, the sector shows relative stability with modest improvement in quality but some shifts in leadership. In the current assessment, Spenn, Save, and Standard Life Rwanda lead with strong accessibility scores, while Kiva follows closely, though its policy remains lengthy and less readable for the average user. Compared to last year, when Save led with a perfect score and Spenn and Kiva followed, accessibility remains broadly strong across the sector. The key change is not in the existence of policies, these remain in place but in their refinement and prominence. However, readability challenges persist, particularly for Kiva, whose detailed but complex policy may limit practical user comprehension despite substantive coverage.

Substantive transparency and data subject rights protections show clearer evolution. Spenn now emerges as the strongest overall performer in user rights articulation, providing clearer contact details, defined purposes for data collection, specified data categories, and articulated retention timelines.

This represents progress from the previous year, when Spenn lacked contact details and provided only conditional rights in certain areas. Kiva continues to perform relatively strongly, maintaining robust descriptions of data purposes and offering extensive user rights, including complaint mechanisms. However, its continued reliance on advertising partnerships and behavioral marketing practices moderates its compliance standing.

By contrast, Save and Standard Life Rwanda demonstrate limited improvement. Save continues to provide reasons for data collection and identify categories of data but still omits clear retention timelines and comprehensive complaint rights. Although it now includes some channels for engagement, its failure to articulate opt-in or opt-out marketing controls and structured deletion rights reflects ongoing compliance weaknesses. Standard Life Rwanda performs similarly poorly, with vague and conditional rights, incomplete data disclosure, and unspecified retention periods. These deficiencies largely mirror last year's findings, indicating stagnation in privacy governance maturity for these providers.

Third-party data sharing remains a critical area of concern, though performance patterns have shifted. In the prior assessment, Spenn led in third-party compliance with a comparatively strong score, while Kiva and Save trailed. In the current review, Kiva leads, though still at a modest level, reflecting improved transparency regarding affiliates, service providers, and platform partners. Nevertheless, it does not specify the precise data types shared. Spenn's performance in this category has declined relative to last year, as it now provides limited detail on third-party entities and data categories. Save continues to show weak transparency in third-party arrangements, and Standard Life Rwanda records the lowest performance, permitting broad third-party processing without identifying entities, safeguards, or reporting channels. Despite some reordering among the platforms, overall sector compliance on third-party governance remains low. This ongoing weakness poses significant legal and operational risk, given the sensitivity of financial and identity data processed within digital lending ecosystems.

Data security is an area where measurable improvement is evident, particularly for Kiva. Last year, Kiva led with moderate performance, while Spenn and Save lagged and all platforms failed security header assessments. In the current review, Kiva demonstrates strong SSL implementation and a high security header score, marking a significant technical improvement and strengthening its overall compliance posture. Spenn shows moderate performance with documented internal security measures, including blockchain-secured transaction history and compliance-related retention practices, though it continues to fail on security headers. Standard Life Rwanda maintains acceptable SSL certification but weak header configuration. Save remains the weakest performer in this category, referencing little to no specific data security measures in its policy. While progress is visible for Kiva and, to a lesser extent, Spenn, inconsistent implementation of layered technical safeguards across the sector continues to limit full compliance with statutory security obligations.

Transparency reporting remains entirely absent, unchanged from last year. None of the assessed entities has published a transparency report disclosing data access requests, government demands, or breach statistics. This persistent gap reflects a sector-wide reluctance or immaturity in proactive accountability practices. The absence of transparency reporting reduces stakeholder trust and limits demonstrable compliance with openness principles embedded in data protection frameworks.

Internal data breach resolution mechanisms show marginal improvement but remain inadequate. In the previous assessment, only Save and Kiva demonstrated limited effort, with very low scores across the sector. In the current review, Kiva leads with a modest but improved score, indicating more visible reporting channels and safeguards. Save demonstrates incremental progress, while Standard Life Rwanda shows minimal procedural clarity. Spenn, despite stronger overall policy articulation this year, performs poorly in structured breach response governance. Although there is slight movement toward formalization, the overall maturity of incident response frameworks remains weak. The continued absence of clearly defined timelines, investigation procedures, and notification protocols creates substantial regulatory exposure, particularly in a high-risk financial services environment.

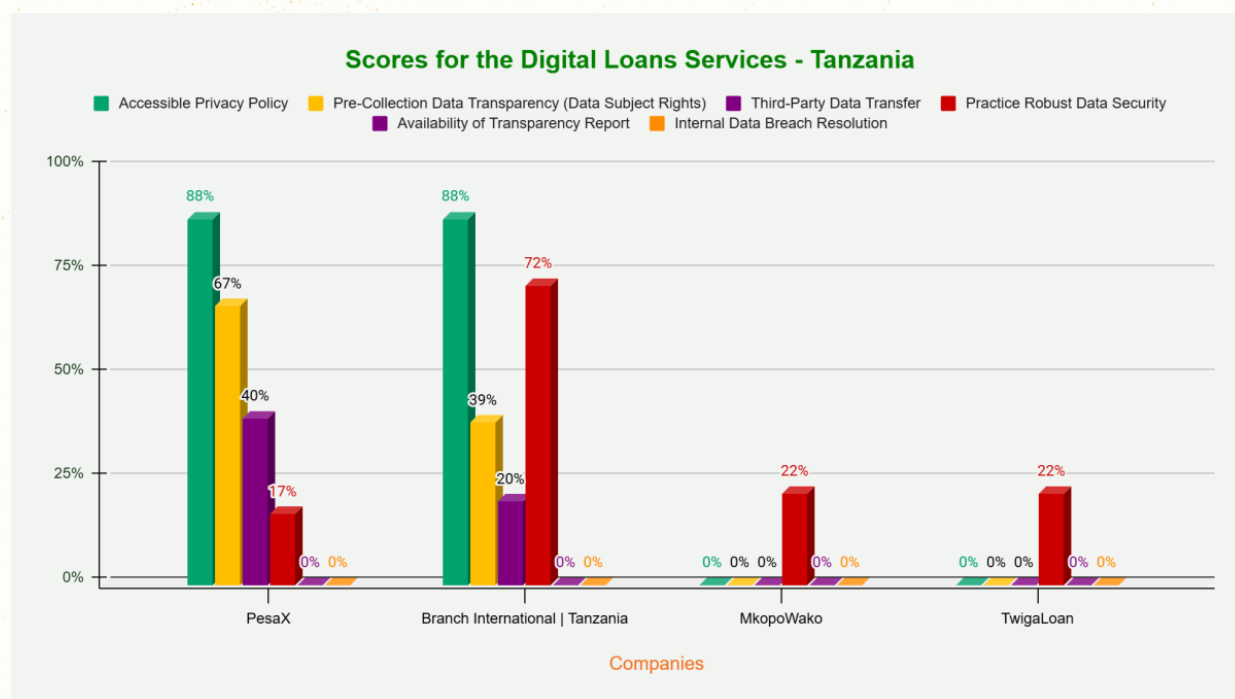
In comparative terms, the sector demonstrates gradual improvement in policy refinement, articulation of user rights,

and, in Kiva's case, technical security controls. However, foundational gaps identified last year particularly in registration compliance, third-party governance specificity, transparency reporting, and structured breach management largely remain unresolved. Save and Standard Life Rwanda show limited advancement, suggesting stagnation in privacy governance development. Spenn has strengthened its user rights framework but regressed in third-party transparency, while Kiva has improved significantly in technical safeguards but continues to rely on advertising-linked data practices.

Overall, the trajectory indicates incremental but uneven progress rather than systemic reform. While some platforms are evolving toward stronger alignment with data protection principles, sector-wide compliance maturity remains moderate at best. Without demonstrable regulatory registration, strengthened third-party oversight, institutionalized breach response frameworks, and proactive transparency reporting, the facilities remain exposed to regulatory scrutiny, operational disruption, and reputational risk. Continued improvement will require moving beyond policy publication toward fully embedded, demonstrable accountability mechanisms aligned with Rwanda's data protection law.

e. *PesaX Tanzania, Branch International Tanzania, MkopoWako Tanzania and TwigaLoan in Tanzania*

The 2025 assessment of digital lending platforms in Tanzania (PesaX, Branch International Tanzania, MkopoWako, and TwigaLoan) shows a mixed pattern of improvement and regression when compared with the previous year. While certain platforms have made notable progress in transparency and user rights articulation, structural weaknesses persist across the sector, particularly in regulatory registration, third-party governance, transparency reporting, and breach accountability. Overall, compliance maturity remains uneven and, in several respects, stagnant.



Most fundamentally, there is still no visible evidence that any of the assessed platforms has fulfilled registration requirements with the national data protection regulator. This mirrors last year's position and represents a continuing foundational compliance gap. Registration is a core statutory requirement under Tanzania's data protection framework, and the absence of demonstrable compliance undermines the legitimacy of other privacy measures. Without regulatory registration, these platforms operate in a posture of legal vulnerability, exposing themselves to potential enforcement action and reputational damage.

In the area of accessible privacy policies, the sector reflects both improvement and decline. This year, only PesaX and Branch International Tanzania achieved strong accessibility scores. PesaX shows the most significant improvement, moving from a score of 0% last year to 88% in the current assessment. This shift indicates a meaningful effort to establish baseline transparency through a publicly available and reasonably readable privacy policy. Branch International Tanzania maintains its prior strong performance, demonstrating consistency in policy visibility and accessibility. In contrast, MkopoWako, which previously scored moderately well, and TwigaLoan now record no measurable performance in this category. MkopoWako's decline from 63% to 0% marks a substantial regression in transparency, while TwigaLoan's continued absence of visible policy disclosures reflects ongoing non-compliance. Compared to last year, therefore, transparency gains by PesaX are offset by deterioration at MkopoWako and continued stagnation at TwigaLoan.

Pre-collection data transparency and recognition of data subject rights show a similar pattern of divergence. PesaX records a significant improvement, rising from 0% to 67%, demonstrating enhanced disclosure regarding data processing purposes and greater acknowledgment of user rights prior to data collection. Branch International Tanzania records a slight decline, falling from 42% to 39%, though it remains one of the stronger performers in this area. MkopoWako experiences a dramatic drop from 63% last year to 0%, suggesting either removal of previously available information or failure to maintain compliance structures. TwigaLoan continues to score 0%, reflecting persistent non-recognition of core data subject rights. These developments indicate that while one new entrant has strengthened its privacy posture, the broader sector has not collectively progressed. Instead, compliance improvements appear isolated rather than systemic.

Third-party data sharing remains a critical area of concern. All platforms were found to share personal data with third parties, yet compliance levels remain low. PesaX shows marked improvement, rising from 0% last year to 40%, thereby becoming the strongest performer in this category. This suggests increased transparency regarding external data disclosures. However, even this leading score remains modest and signals incomplete compliance. Branch International Tanzania declines slightly from 24% to 20%, while MkopoWako and TwigaLoan continue to record no measurable compliance. Compared with last year, the sector has not achieved substantive progress in third-party governance. While PesaX's improvement is notable, overall performance indicates continued weaknesses in specifying third-party entities, clarifying data categories shared, articulating legal justifications, and documenting safeguards. Given the sensitivity of financial and identity data processed by digital lenders, inadequate third-party oversight creates significant regulatory and consumer protection risks.

In contrast, data security demonstrates relative stability, though with limited advancement. Branch International Tanzania maintains its leading position with a strong score of 72%, supported by a high SSL server rating. However, while its technical safeguards appear robust at the transport layer, policy disclosures remain general and lack detailed explanation of internal controls. MkopoWako and TwigaLoan maintain their prior modest scores of 22%, reflecting limited but consistent implementation of security measures. PesaX records a slight decline in this area, dropping from 22% last year to 17%, indicating potential weakening in documented safeguards or technical configurations. Compared with the previous assessment, therefore, there is no substantial sector-wide improvement in comprehensive security governance.

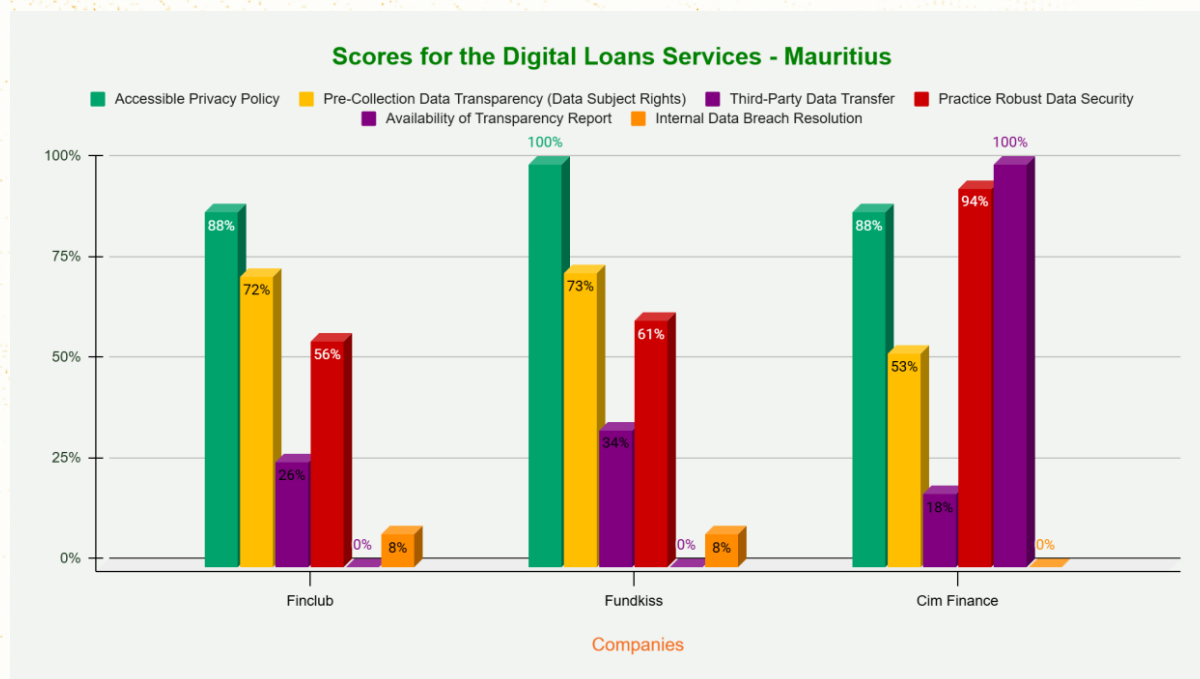
While baseline protections exist, the absence of detailed technical, organizational, and procedural disclosures limits confidence in full compliance with statutory security obligations.

Transparency reporting and internal data breach resolution remain the weakest areas across the sector, with no observable change from last year. None of the platforms has published a transparency report detailing government requests, third-party disclosures, or incident statistics. Similarly, there is no demonstrable evidence of structured internal data breach resolution mechanisms across any of the assessed entities. This continued absence of formalized breach response frameworks such as defined reporting timelines, user notification procedures, and regulatory escalation pathways poses a serious compliance risk. Under data protection law, timely breach notification and accountability are not optional; failure to institutionalize such mechanisms increases exposure to regulatory penalties and reputational harm.

When viewed comparatively against last year's findings, the sector's trajectory is uneven. PesaX demonstrates the most significant improvement, moving from near-total non-performance to moderate compliance in transparency, user rights articulation, and third-party disclosure. Branch International Tanzania remains the most stable performer, maintaining strong accessibility and security scores but showing slight declines in certain transparency metrics. MkopoWako exhibits the most pronounced regression, losing ground in areas where it previously demonstrated moderate compliance. TwigaLoan remains unchanged at a minimal compliance level.

Overall, while individual platforms have made targeted improvements, the Tanzanian digital lending sector has not achieved systemic progress in data protection compliance. Core weaknesses identified last year particularly, the absence of regulatory registration, inadequate third-party governance, lack of transparency reporting, and failure to institutionalize breach response mechanisms remain unresolved. Incremental gains by certain providers are offset by stagnation or regression among others. As a result, the sector continues to face substantial legal, operational, and reputational risks. Meaningful alignment with Tanzania's data protection laws will require not only accessible policies and technical safeguards, but demonstrable regulatory registration, strengthened third-party oversight, and fully operational accountability frameworks embedded across all platforms.

f. *Finclub, Fundkiss and Cim Finance in Mauritius*



Just as in the previous year, none of the platforms demonstrated any visible effort to comply with registration requirements with the national data protection regulator. This continued omission remains a significant compliance gap, as registration is a foundational obligation under the Data Protection Act 2017 and signals accountability to regulatory oversight. The absence of progress in this area suggests that, despite improvements in certain operational practices, formal regulatory alignment remains weak across the sector.

At the same time, all three platforms maintained strong performance in making their privacy policies accessible. Fundkiss retained its leading position with a perfect score of 100%, unchanged from last year. FinClub and Cim Finance each maintained scores of 88%, also unchanged. This consistency demonstrates sustained commitment to transparency at the point of access to information. From a compliance perspective, clear and visible privacy notices are essential to meeting statutory transparency obligations and to fostering user trust. However, accessibility alone does not guarantee substantive compliance, as the quality and completeness of disclosures remain equally important.

In relation to pre-collection data transparency and the observance of data subject rights, the sector recorded notable shifts compared to last year. Fundkiss improved significantly from 52% to 73%, moving from last place to joint leader. FinClub, which had led in the previous year with 77%, declined slightly to 72%. Cim Finance also experienced a marginal decrease, from 54% to 53%. These changes indicate that while overall performance remains moderate, leadership in this area has shifted. Fundkiss's improvement suggests a strengthening of its disclosures around data collection purposes and user rights, enhancing its alignment with legal requirements concerning informed consent and fair processing. FinClub's slight decline, though not dramatic, suggests stagnation or minor gaps in maintaining best practice standards. Cim Finance's marginal drop signals limited progress in deepening transparency obligations. Collectively, the data suggests incremental improvement but no sector-wide transformation in embedding robust user empowerment mechanisms.

Third-party data sharing remains the weakest area of compliance across all platforms, despite some movement compared to last year. All platforms, as before, share user data with third parties. Fundkiss improved from 24% to 34%, FinClub declined from 36% to 26%, and Cim Finance rose from 0% to 18%. Although Cim Finance's increase represents progress from a baseline of no compliance, overall scores remain low across the board. These persistently weak results raise significant compliance concerns, particularly given that data sharing and cross-border transfers are heavily regulated under the Data Protection Act 2017 and comparable international standards such as the GDPR. Insufficient specificity about third-party recipients, safeguards, and categories of shared data increases regulatory risk and may expose the platforms to enforcement action or reputational harm in the event of misuse or breach by external partners.

Data security practices present a contrasting picture of stability. Cim Finance maintained its leading position with 94%, while Fundkiss and FinClub sustained their previous scores of 61% and 56%, respectively. The absence of change suggests that security frameworks have neither significantly improved nor deteriorated. Cim Finance's consistently high score indicates mature technical and organisational safeguards, reinforcing resilience against unauthorised access or data loss. However, for Fundkiss and FinClub, maintaining mid-range scores without improvement suggests that security invest-

ments have plateaued. Given the increasing sophistication of cyber threats, static performance may not be sufficient to meet evolving legal expectations regarding “appropriate technical and organisational measures.”

Transparency reporting remains largely unchanged. Cim Finance continued to be the only platform publishing a transparency report, retaining a perfect score of 100%, while Fundkiss and FinClub again scored 0%. This sustained disparity reinforces Cim Finance’s relative strength in public accountability and openness about its data governance practices. Transparency reporting contributes positively to compliance culture, demonstrating proactive disclosure beyond minimum legal requirements.

The continued absence of such reporting by the other platforms limits public visibility into their data handling practices and may weaken stakeholder confidence.

Internal data breach resolution mechanisms show mixed and concerning trends. FinClub and Fundkiss improved slightly from 0% to 8%, indicating initial steps toward formalising internal processes. In contrast, Cim Finance declined from 17% to 0%, eliminating the limited progress it had previously made. Overall, performance in this area remains critically low. The absence of clear internal breach response procedures, defined timelines, impartial investigation guarantees, and structured reporting channels poses substantial compliance risks. Under data protection law, prompt detection, documentation, and notification of breaches are mandatory obligations. Weak internal frameworks could delay response times, increase harm to affected individuals, and heighten exposure to regulatory penalties.

A closer review of the privacy policies reinforces these scoring patterns. FinClub’s policy is formally aligned with the Data Protection Act 2017 and references international standards such as the GDPR. It defines lawful bases for processing, outlines categories of collected data, and describes retention periods of up to seven years or longer where legally required. It also recognises user rights and provides complaint mechanisms through its Data Protection Officer and the Mauritius Data Protection Office. These features indicate structural alignment with statutory requirements. However, its reduced score in third-party data transfers suggests that, in practice, disclosures around external data sharing may lack sufficient granularity or safeguards.

Fundkiss’s policy remains highly accessible and transparent in structure, providing detailed descriptions of collected data and contact information. Its improvement in pre-collection transparency is reflected in clearer articulation of purposes and rights. Nevertheless, retention periods remain vaguely defined as “required by law,” and third-party disclosures lack specificity. Although user rights are recognised and consent is required for targeted marketing, limited detail on security safeguards and breach handling procedures weakens demonstrable accountability. The absence of clearly defined breach notification obligations may expose the company to legal vulnerability in the event of an incident.

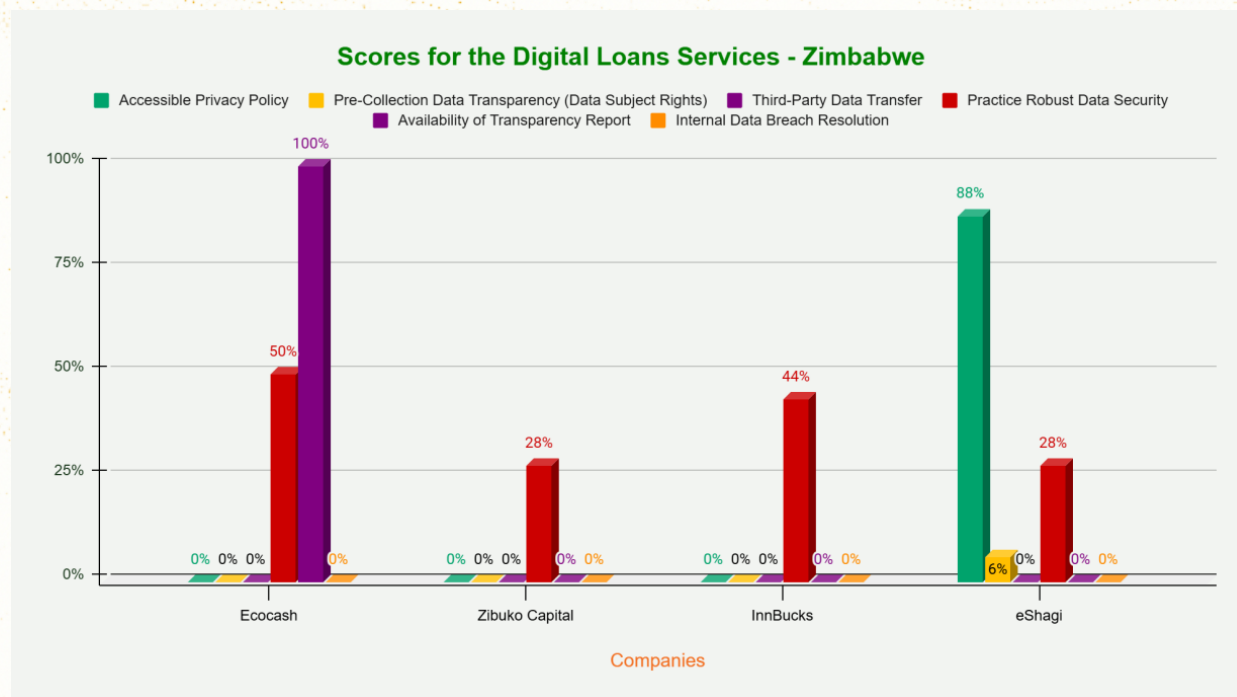
Cim Finance’s policy is visible and structured but omits key contact details and provides only general retention language. While it continues to lead in data security and transparency reporting, its decline in breach resolution scoring suggests a potential gap between formal policy commitments and internal procedural robustness. The absence of explicit user breach notification procedures or detailed reporting channels limits practical compliance effectiveness.

Compared to last year, the overall trajectory of the sector can be characterised as incremental rather than transformative. Accessibility of privacy policies and security safeguards remain stable. Leadership in pre-collection transparency has shifted from FinClub to Fundkiss. Third-party data transfer compliance remains the most significant structural weakness, despite modest improvements by Fundkiss and Cim Finance. Internal breach management continues to be critically underdeveloped across the sector, with no platform demonstrating strong compliance in this area. Registration with the national regulator remains entirely unaddressed.

In conclusion, while certain improvements, particularly by Fundkiss in transparency and by Cim Finance in maintaining strong security and reporting practices indicate gradual maturation of privacy governance, systemic compliance gaps persist. Weaknesses in regulatory registration, third-party data transfer safeguards, and internal breach resolution mechanisms continue to expose the platforms to regulatory enforcement risks, reputational damage, and potential erosion of user trust. Without substantive progress in these high-risk areas, the sector’s privacy practices remain only partially aligned with the full requirements of applicable data protection laws.

g. Ecocash, Zibuko Capital, InnBucks and eShagi in Zimbabwe

The current assessment of the digital loans sector reveals a marked regression in several core areas of data protection compliance when compared with last year’s findings. As in the previous review, none of the platforms demonstrated visible effort to fulfil registration requirements with the national regulator. This continued absence of regulatory registration remains a foundational compliance gap. Registration is a basic accountability obligation under data protection law, and failure to demonstrate compliance in this area weakens regulatory oversight and signals limited institutional commitment to formal governance standards.



In contrast to this stagnation, there has been a significant shift in the accessibility of privacy policies. eShagi emerged this year as the only platform demonstrating meaningful effort, scoring 88%, a substantial improvement from 0% last year. This indicates a notable step toward transparency and suggests a developing recognition of the importance of informing users about data practices. However, this positive development is offset by sharp declines elsewhere. EcoCash, which previously led the sector with a perfect score of 100%, dropped to 0%, while InnBucks declined from 75% to 0%. Zibuko Capital maintained its previous score of 0%.

This reversal is significant. Last year, EcoCash and InnBucks were recognised for comparatively strong transparency through accessible privacy policies. Their current absence of demonstrable accessibility raises concerns about diminished openness and reduced user awareness of data handling practices. Without accessible policies, users are deprived of essential information regarding the nature, purpose, and scope of data processing, undermining the principle of informed consent and exposing these platforms to heightened regulatory and reputational risk.

The regression is even more pronounced in the area of data subject rights and pre-collection transparency. This year, only eShagi made any effort, scoring a modest 6%, up from 0%. EcoCash dropped from 65% to 0%, and InnBucks from 49% to 0%, while Zibuko Capital again remained at 0%. In last year's analysis, EcoCash and InnBucks had demonstrated relative strength in this category, indicating some recognition of users' rights to access, correct, or object to the processing of their personal data.

Their complete decline to zero suggests either the withdrawal of previously available safeguards or a lack of demonstrable evidence of their continued implementation. From a compliance perspective, this represents a serious setback. Respect for data subject rights is central to modern data protection frameworks, and failure to operationalise these rights exposes organisations to legal sanctions and erodes consumer trust.

Third-party data sharing presents an equally troubling trajectory. All platforms continue to share data with third parties, yet compliance scores have fallen dramatically. InnBucks dropped from 70% to 0%, and EcoCash from 24% to 0%, while eShagi and Zibuko Capital maintained 0% from last year. Previously, EcoCash and InnBucks had shown measurable effort in regulating and disclosing third-party transfers, particularly EcoCash with a relatively strong 70% score. The complete erosion of these safeguards suggests either diminished transparency or weakened contractual and organisational controls governing data sharing. Given that third-party transfers are among the highest-risk aspects of data processing, particularly where cross-border transfers or financial data are involved, this decline significantly heightens compliance risks. Inadequate oversight of third parties can lead to unlawful disclosures, loss of control over personal data, and liability for downstream misuse.

In the area of data security, the sector presents a more mixed picture. All platforms demonstrated some effort to maintain security safeguards, though performance shifted. EcoCash continues to lead with 50%, despite a decline from 67%. InnBucks improved from 28% to 44%, reflecting strengthened technical or organisational security controls. Zibuko Capital

dropped from 45% to 28%, while eShagi maintained its previous score of 28%. Compared to last year, where EcoCash led at 67% and Zibuko Capital followed at 45%, the overall trend suggests a levelling downward, with the exception of InnBucks' improvement. While the presence of some security controls is positive, declining or stagnant scores may indicate insufficient adaptation to evolving cybersecurity threats. Under data protection law, security measures must be "appropriate" and responsive to risk; therefore, failure to continuously strengthen safeguards may result in non-compliance over time.

Transparency reporting shows a noteworthy development. EcoCash is now the only platform publishing a transparency report, achieving a perfect score of 100%, up from 0% last year. The other platforms remain at 0%, unchanged. This marks a positive shift for EcoCash, signalling enhanced openness regarding its data governance practices. Transparency reports contribute to accountability by informing the public about data requests, disclosures, and oversight mechanisms. However, the absence of similar reporting by the other platforms limits sector-wide transparency and constrains stakeholder scrutiny.

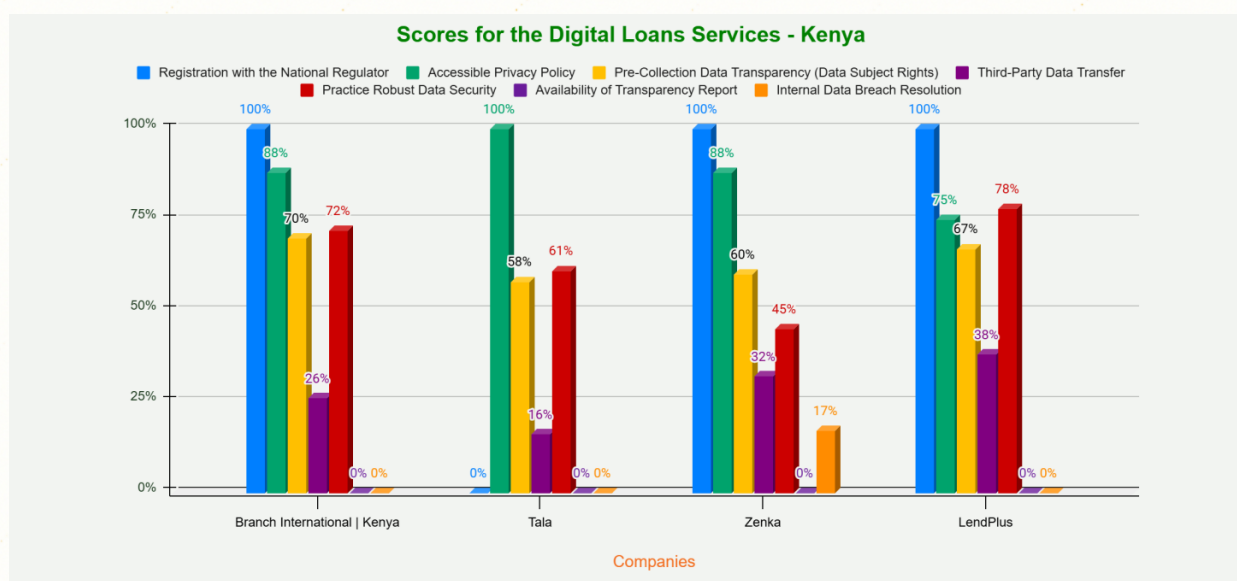
As in the previous year, none of the platforms demonstrated any effort to establish internal data breach resolution mechanisms. Scores remain at 0% across the board. This persistent weakness is particularly concerning. Effective breach management frameworks including internal reporting channels, investigation procedures, user notification timelines, and mitigation strategies are mandatory components of data protection compliance. Without them, platforms risk delayed responses to incidents, greater harm to affected individuals, and increased exposure to regulatory penalties.

Overall, the comparison with last year reveals a sector that has regressed in critical transparency and accountability measures, despite isolated improvements. eShagi's emergence in privacy policy accessibility represents a positive development, and InnBucks' improved security score suggests incremental operational strengthening. EcoCash's adoption of a transparency report also marks progress in public accountability. However, these gains are overshadowed by the widespread decline in privacy policy accessibility, data subject rights observance, and third-party data transfer compliance.

The current findings indicate that the digital loans sector is struggling to maintain consistent compliance with data protection laws. The erosion of previously demonstrated safeguards, particularly by EcoCash and InnBucks, signals instability in privacy governance frameworks. Persistent failure to address regulatory registration and breach management further compounds compliance vulnerabilities. Unless the platforms adopt sustained and comprehensive data protection strategies, grounded in transparency, user rights protection, secure third-party oversight, and formal regulatory engagement, they remain exposed to legal enforcement risks, reputational damage, and diminished consumer trust.

h. *Branch International Kenya, Tala Kenya, Zenka and LendPlus in Kenya*

The current assessment of the leading digital lending platforms shows measurable progress in certain compliance areas, alongside persistent structural weaknesses that continue to affect alignment with data protection law. Compared with last year, the most notable improvement is in regulatory registration. Branch International, Zenka and LendPlus each achieved a perfect score of 100% for fulfilling registration requirements with the national regulator. Branch International and LendPlus improved from 88%, while Zenka maintained its previous perfect score. In contrast, Tala Kenya declined from 100% and no longer demonstrates full compliance in this area.



This shift represents an important development. Registration with the regulator is a foundational legal obligation and signals formal recognition of oversight authority. The improvement by Branch International and LendPlus suggests strengthening institutional alignment with statutory requirements, likely influenced by heightened regulatory scrutiny in the sector. Tala's decline, however, raises compliance concerns, particularly given its previous leadership position. Failure to maintain registration undermines accountability and exposes a platform to potential enforcement action.

All platforms continue to demonstrate visible effort in maintaining accessible privacy policies. Tala now leads with 100%, improving from 75%. Branch International maintained its score of 88%, Zenka improved from 75% to 88%, and LendPlus declined from 88% to 75%. Compared to last year, where Branch International and LendPlus led, leadership has shifted to Tala. This overall consistency indicates that transparency through published privacy notices remains embedded practice across the sector. Given the data-intensive nature of digital lending, where algorithmic credit scoring relies on behavioural and financial data, accessible privacy policies are essential for meeting transparency and informed consent obligations. However, accessibility alone does not guarantee substantive compliance; the completeness and specificity of disclosures remain critical.

Performance in observing data subject rights reflects moderate but uneven progress. Branch International remains the leader at 70%, though slightly down from 72%. LendPlus improved significantly from 54% to 67%, demonstrating stronger recognition of user rights. Zenka declined from 64% to 60%, while Tala improved marginally from 56% to 58%. Compared to last year, the ranking order remains broadly similar, but LendPlus shows the most meaningful upward movement. These scores suggest that platforms are gradually operationalising rights such as access, correction, and objection. Nevertheless, declines for Branch International and Zenka indicate that maintaining compliance requires sustained effort. Since digital lending decisions can materially affect individuals' access to credit, weak implementation of data subject rights may expose platforms to legal challenges, particularly where automated decision-making is involved.

Third-party data sharing continues to represent the weakest area of compliance, despite some improvements. All platforms share user data with third parties, yet compliance scores remain low. LendPlus leads at 38%, improving from 20%. Zenka declined from 46% to 32%. Branch International improved from 16% to 26%, and Tala improved from 6% to 16%. Compared to last year, there is some overall upward movement except for Zenka's decline, but the scores remain modest. Given that digital lenders routinely share data with credit reference bureaus, analytics providers, and marketing partners, inadequate disclosure and safeguards in third-party transfers create substantial regulatory risk. Data protection laws impose strict conditions on onward transfers, particularly where sensitive financial or behavioural data are involved. Persistently low scores suggest incomplete contractual safeguards, limited transparency regarding recipients, or insufficient user notification mechanisms.

In the area of data security, performance remains relatively stable. LendPlus maintained a strong score of 78%, as did Branch International at 72%. Tala declined from 78% to 61%, while Zenka maintained 45%. Compared to last year, there is general stability, with Tala showing the only significant drop. The maintenance of relatively high security scores for Branch International and LendPlus indicates sustained investment in technical and organisational safeguards. However, Zenka's comparatively lower and unchanged score suggests room for strengthening resilience against evolving cybersecurity threats. Given the sensitivity of financial and behavioural data processed in algorithmic lending models, inadequate or declining security measures could result in serious legal and reputational consequences in the event of a breach.

As in the previous year, none of the platforms publish transparency reports; all scored 0% again. This continued absence of public reporting limits external accountability and weakens public confidence. Transparency reports are increasingly regarded as best practice, particularly in sectors involving automated profiling and significant economic impact on individuals. Their absence suggests that, despite regulatory pressure, platforms remain reluctant to disclose detailed information about data requests, government access, or internal governance practices.

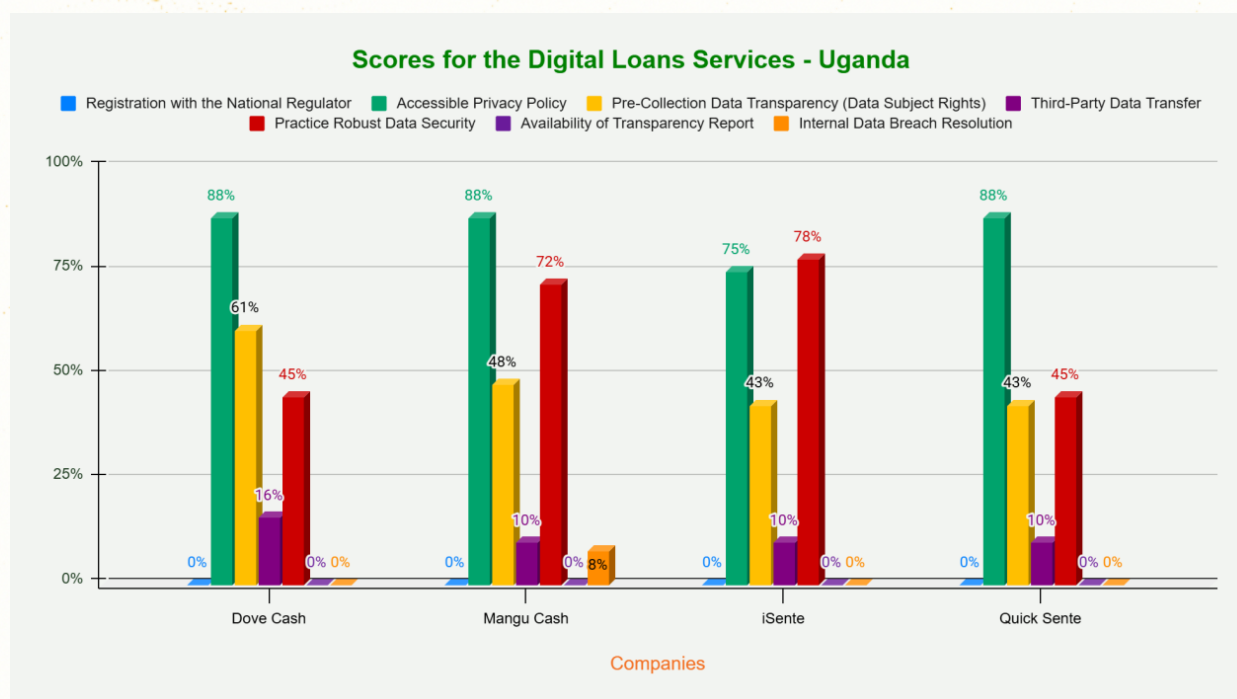
Internal data breach resolution mechanisms also remain an area of serious concern. Zenka maintained a modest score of 17%, unchanged from last year. Branch International remained at 0%. Tala declined from 17% to 0%, and LendPlus fell from 8% to 0%. Compared to last year, there has been regression rather than improvement. Effective breach response frameworks including internal reporting channels, defined investigation timelines, and clear user notification procedures are mandatory components of modern data protection compliance. The widespread absence of demonstrable mechanisms indicates vulnerability to delayed incident response and potential non-compliance with statutory breach notification requirements.

Overall, compared with last year's analysis, the sector demonstrates progress in regulatory registration and moderate improvements in third-party transfer practices for some platforms. Privacy policy accessibility remains consistently strong, and data security safeguards are largely maintained. However, declines in internal breach resolution readiness, the absence of transparency reports, and continuing weaknesses in third-party data governance indicate that compliance maturation remains incomplete.

The overall trajectory suggests that leading digital lenders are responding to regulatory scrutiny and enforcement pressure, particularly in formal registration and public-facing transparency measures. Nevertheless, significant gaps persist in operational accountability mechanisms. Given that these platforms rely on algorithmic analysis of extensive personal, financial, and behavioural data to determine access to credit, incomplete compliance in areas such as third-party transfers, breach response, and transparency reporting poses heightened legal and reputational risks. Without sustained investment in comprehensive privacy governance frameworks, the sector may struggle to fully meet evolving data protection standards and maintain user trust in an increasingly regulated digital finance environment.

i. *Dove Cash, Mangu Cash, iSente and Quick Sente in Uganda*

The current assessment of digital loan providers indicates a sector that remains structurally weak in regulatory compliance, with limited progress since last year and regression in key areas. Most notably, none of the platforms now demonstrate compliance with registration requirements before the national regulator. Mangu Cash, which previously achieved a perfect score of 100% for registration, dropped to 0%, while Dove Cash, iSente and Quick Sente each maintained their prior scores of 0%. This marks a significant regression compared to last year, when Mangu Cash stood out as the only compliant entity. Registration is a foundational requirement under data protection law and signals formal accountability to the regulator. The complete absence of demonstrable compliance across the sector raises concerns about weak regulatory engagement and exposes these platforms to enforcement risk.



In contrast, privacy policy accessibility remains one of the few stable areas of performance. Dove Cash, Mangu Cash and Quick Sente each maintained strong scores of 88%, unchanged from last year, while iSente declined from 88% to 75%. This suggests that, despite broader compliance gaps, most platforms continue to prioritise having visible and readable privacy notices. However, accessibility does not necessarily equate to substantive compliance. The quality, completeness and operationalisation of the commitments contained in those policies remain uneven.

Performance in recognising and operationalising data subject rights shows modest improvement overall.

Dove Cash remains the leader at 61%, though slightly down from 63%. Mangu Cash improved significantly from 37% to 48%, while iSente and Quick Sente each improved to 43%, up from 37% and 33% respectively. Compared to last year, this reflects incremental progress in embedding user rights frameworks. Nonetheless, the scores remain moderate, indicating that while rights such as access, rectification and restriction may be acknowledged, full implementation particularly concerning erasure and complaint rights remains incomplete. Weak protection of data subject rights is especially problematic in digital lending, where automated decisions directly affect individuals' access to credit and financial opportunities.

Third-party data transfers remain consistently weak and have deteriorated in some cases. All platforms share personal data with third parties, yet compliance scores are low. Dove Cash leads with only 16%, down from 24%, while Mangu Cash, iSente and Quick Sente each maintained 10% from last year. The stagnation and decline in this area highlight persistent opacity regarding the nature of shared data, the identity of recipients, and applicable safeguards. Given that

digital lenders routinely interact with advertisers, analytics providers and potentially credit reference agencies, insufficient transparency and contractual control over third-party transfers pose significant legal and reputational risks. Data protection laws impose strict obligations on controllers to ensure that downstream processors handle personal data lawfully; failure to do so may result in joint liability for misuse.

Data security practices present a more varied picture. iSente now leads with 78%, improving from 72%. Mangu Cash maintained a strong 72%. Dove Cash held steady at 45%, while Quick Sente declined sharply from 72% to 45%. Compared to last year, security remains one of the stronger compliance areas overall, though performance is inconsistent. While relatively higher scores suggest the presence of technical safeguards, such as secure hosting or encryption measures, policy disclosures often lack specificity. For example, Mangu Cash references security measures and advises users on password management but does not clearly detail internal technical controls. In a sector handling sensitive financial and behavioural data, insufficiently articulated security frameworks may undermine compliance with statutory obligations requiring “appropriate technical and organisational measures.”

Transparency reporting remains entirely absent. As in the previous year, none of the platforms published a transparency report. This continued omission limits public accountability and prevents users from understanding how frequently data is shared with government agencies or other third parties.

The absence of transparency reporting is consistent with broader sectoral weaknesses and reflects limited adoption of best practices in proactive disclosure.

Internal data breach resolution mechanisms also remain critically underdeveloped. Mangu Cash maintained a modest score of 8%, reflecting only vague references to breach handling, while Dove Cash, iSente and Quick Sente each maintained 0%. Compared to last year, there has been no meaningful improvement. Policies generally lack clear timelines for reporting and investigation, guarantees of impartiality, or defined notification procedures. In practice, this means that in the event of a data breach, users may not be informed promptly, and internal response processes may lack structure and accountability. Under data protection law, such deficiencies can lead to regulatory sanctions and increased harm to affected individuals.

A closer examination of policy content reinforces these findings. Mangu Cash’s privacy policy is accessible and written in clear language. It outlines categories of data collected and states that data is retained “as required by law,” but does not specify precise retention periods. It recognises certain data subject rights, such as access and rectification, and permits opt-out from behavioural marketing. However, it does not clearly provide for the right to erasure or detailed complaint procedures before the regulator. Although categories of third-party recipients are listed, the specific nature of the data shared is not disclosed. While multiple communication channels are provided, breach handling procedures lack defined timelines and structured reporting processes.

Quick Sente similarly maintains an accessible policy that clearly explains the purpose of data collection and lists categories of data gathered. However, it provides limited contact information, relies on general retention language, and scores zero on internal breach resolution. These patterns indicate that while formal policy documents exist, operational accountability mechanisms remain weak.

In comparison with last year, the sector shows modest gains in data subject rights recognition and some improvements in security for specific platforms, particularly iSente. However, it has regressed significantly in regulatory registration compliance and experienced declines in third-party transfer transparency and, in some cases, data security. Transparency reporting and breach resolution remain unchanged at critically low levels.

Overall, the persistent absence of registration, transparency reporting and robust breach management frameworks suggests systemic compliance immaturity. Given the sensitive nature of financial data processed by these platforms, ongoing weaknesses expose them to regulatory penalties, reputational harm and erosion of user trust. Without comprehensive improvements in governance, transparency and incident management, the sector risks remaining structurally vulnerable under evolving data protection enforcement regimes.

3.4.8.3 Comparison of companies/entities within the sector



High-Performing Jurisdictions: Emerging Compliance Leaders and Trajectories

Nigeria and Mauritius emerge as the strongest-performing jurisdictions in the digital lending sector, reflecting comparatively more mature privacy governance, though still short of full compliance.

Nigeria now leads the sector, with Renmoney (60%), Branch Nigeria (58%), and FairMoney Nigeria (53%) outperforming regional peers. Compared to last year, when leading Nigerian platforms clustered in the mid-40% range, these scores indicate tangible progress in implementing accessible privacy policies, strengthening data security measures, and improving transparency around data processing. However, even the highest-performing Nigerian platforms remain below 65%, highlighting persistent gaps in accountability mechanisms such as internal breach response and oversight of third-party data sharing.

Mauritius also demonstrates a positive trajectory. Cim Finance (59%) continues to perform strongly, consolidating its position from last year's high-50% range, while Fundkiss (46%) and Finclub (42%) show modest improvement. These results suggest more consistent compliance with formal data protection requirements, reflecting Mauritius's relatively mature regulatory environment. Nonetheless, compliance remains partial, particularly in relation to onward data transfers and transparency reporting.

Botswana shows signs of emerging leadership at the upper-middle tier. Bayport Botswana (54%) now ranks among the stronger performers, indicating progress from last year's mid-40% range. Letshego (48%) and ExpressCredit Botswana (41%) also show incremental gains, suggesting growing institutional attention to privacy compliance within the digital credit ecosystem.

Mid-Range Performers: Partial Compliance and Structural Gaps (Change Over Time)

Kenya, Ghana, and Rwanda largely occupy the mid-range performance band, with companies demonstrating partial compliance but limited progress in closing structural gaps.

In Kenya, Branch International (51%) and LendPlus (51%) have improved significantly from last year's mid-30% scores, indicating better privacy disclosures and enhanced security practices. Zenka (49%) remains stable, while Tala (34%) has declined from last year's high-40% performance, suggesting regression or stagnation in compliance efforts. These mixed outcomes highlight uneven institutional commitment within the same regulatory environment.

Ghana shows moderate improvement. Fido Ghana (53%) and M-Kopa Ghana (51%) now sit just above the 50% threshold, reflecting progress from last year's mid-40% range. However, Izwe Ghana (33%) and CedisPay (29%) continue to lag, indicating that compliance gains are not sector-wide.

Rwanda presents a similar pattern. Kiva (49%) and Spenn (40%) show improved or stable performance compared to last year, while Save (28%) and Standard Life Rwanda (28%) remain weak. This suggests that while some platforms are investing in privacy governance, structural gaps persist, particularly in consent management and third-party data sharing transparency.

Across this tier, improvements tend to focus on visible compliance measures such as publishing privacy policies while more complex obligations, including breach preparedness and accountability frameworks, remain underdeveloped.

Low-Performing Jurisdictions: Systemic Compliance Challenges and Regression

Several jurisdictions continue to face systemic compliance challenges, with some platforms showing stagnation or regression compared to last year.

Tanzania remains the weakest-performing jurisdiction. MkopoWako (4%) and TwigaLoan (4%) remain critically non-compliant, showing no meaningful improvement. While Branch International Tanzania (37%) and PesaX (35%) perform better, their scores still reflect substantial gaps in transparency, data security, and regulatory alignment. These results indicate structural weaknesses in oversight and enforcement within the digital lending sector.

Uganda also remains largely low-performing. Although Mangu Cash (32%) improved slightly from last year's 45% leader position, it has been overtaken by peers in other jurisdictions. Dove Cash (30%), iSente (29%), and Quick Sente (27%) continue to show limited compliance, suggesting stagnation in privacy governance and weak operationalisation of data protection requirements.

Zimbabwe shows mixed but generally poor performance. While Ecocash (25%) remains the strongest local performer, its score has declined from last year's low-40% range, indicating regression. eShagi (20%), InnBucks (7%), and Zibuko Capital (5%) remain critically weak, reflecting deep-rooted compliance failures.

These jurisdictions are characterised by minimal transparency, weak security controls, and an absence of effective internal breach response mechanisms, exposing users to heightened privacy and data protection risks.

Key Cross-Cutting Implications

Several cross-cutting themes emerge across the digital loan services sector. First, overall performance has improved modestly at the top end, with more platforms now scoring above 50% compared to last year. However, no company exceeds 60%, underscoring that compliance remains partial even among sector leaders.

Second, improvements are uneven and largely driven by private-sector platforms operating in jurisdictions with stronger regulatory frameworks. Public enforcement gaps and limited supervisory capacity appear to contribute significantly to persistent underperformance in countries such as Tanzania, Uganda, and Zimbabwe.

Third, high-risk compliance areas remain consistently weak across all tiers. Transparency around third-party data sharing, internal data breach resolution mechanisms, and accountability reporting are notably absent, despite their centrality to data protection laws.

In conclusion, while the digital lending sector shows signs of gradual maturation, privacy compliance remains fragmented and fragile. Without stronger regulatory enforcement, clearer sector-specific guidance, and deeper institutional investment in privacy-by-design practices, many platforms will continue to expose users to significant data protection risks and regulatory liability.

3 Comparative Review Of Data Protection Regimes In Assessed Countries

This section explores the data protection ecosystems of Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya, and Uganda, outlining the key legislative instruments, compliance obligations, and enforcement mechanisms that define each country's approach to privacy governance. It contrasts national efforts to secure personal data, assess conformity with international and regional standards, and respond to persistent challenges such as data retention, user rights protection, and cross-border data flows. Through this comparative analysis of legal and institutional structures, the report uncovers emerging regional patterns, implementation gaps, and exemplary practices shaping the evolution of data protection across Africa.

3.1 Nigeria's Data Protection Regime

Context and background

Nigeria, Africa's most populous nation with over 220 million citizens, also boasts the continent's largest economy, one increasingly propelled by a dynamic and rapidly expanding digital ecosystem. Digital transformation has reshaped how Nigerians access financial services, engage in commerce, and interact with government institutions. Nowhere is this transformation more evident than in the financial technology (fintech) sector, where innovations such as mobile money, digital lending, and online banking have extended financial inclusion to previously underserved populations across both urban and rural areas.

Yet, this rapid digital growth has simultaneously magnified concerns around personal data protection and privacy. Vast amounts of user information are being collected and processed daily by fintech firms, e-commerce platforms, telecommunications operators, mobile app developers, and government agencies. In an economy increasingly powered by data, the safeguarding of personal information has become not just a regulatory imperative, but a matter of public trust and national security.

The scope of data collection within Nigeria's digital economy is extensive, often reaching deeply into individuals' private lives. Fintech lenders, for instance, gather detailed personal information such as Bank Verification Numbers (BVNs), transaction histories, SMS logs, contact lists, device identifiers, and geolocation data to assess creditworthiness.

E-commerce platforms compile comprehensive consumer profiles based on browsing histories, purchase behaviors, payment details, and demographic data. Telecommunications operators maintain vast subscriber databases containing call logs, location data, and financial transaction records via mobile money services. Meanwhile, government agencies collect citizen information through digital identity programs, tax and electoral systems, immigration services, and e-government platforms.

While this data-driven ecosystem supports financial inclusion, innovation, and improved service delivery, it also exposes individuals to significant risks when personal data is misused, inadequately protected, or accessed without authorization.⁷ Before the advent of comprehensive privacy legislation, Nigeria's regulatory environment was fragmented and ill-equipped to address these emerging challenges. Sector-specific rules such as confidentiality obligations under banking and telecommunications laws offered limited protection, lacking a coherent, cross-sector framework grounded in the principles of consent, purpose limitation, and individual rights.

These regulatory gaps were most visible in the digital lending sector, where numerous reports emerged of predatory practices involving unauthorized access to users' contacts, messages, and device data. Some lenders went so far as to harass borrowers' acquaintances when loans were overdue, exploiting the permissions granted during app installation.

7 Aderonke Alex-Adedipe and Nuratulahi Yishawu. (2024). "Regulation of Digital Money Lenders and Protection of Privacy Rights in Nigeria." Retrieved from <https://pavestoneslegal.com/regulation-of-digital-money-lenders-and-protection-of-privacy-rights-in-nigeria/>.

Such practices not only violated individual privacy rights but also eroded public confidence in digital financial services, undermining the very financial inclusion goals that digital innovation sought to advance.

Positive developments and emerging issues

Nigeria's data protection trajectory mirrors the broader dynamics of rapidly digitalizing economies in the Global South, where technological adoption often outpaces regulatory evolution and institutional capacity. Over the past decade, the country has undergone an extraordinary digital transformation, driven by mobile phone penetration exceeding 100%, widespread internet adoption, and a flourishing fintech ecosystem catering to the nation's large unbanked and underbanked population.

This transformation has produced a complex data ecosystem that spans multiple sectors, regulatory mandates, and technological infrastructures.

While it has accelerated economic inclusion and service innovation, it has also exposed deep vulnerabilities in privacy protection and data governance.

The financial technology sector encapsulates both the promise and the peril of Nigeria's digital transformation. Digital lending platforms have extended credit to millions of individuals previously excluded from formal banking systems, leveraging alternative data and machine learning algorithms to assess risk. Yet, these models often rely on highly intrusive data collection practices harvesting device information, social media activity, communication patterns, and geolocation data. Weak oversight and limited transparency around data use have intensified concerns about consent, proportionality, and the ethical deployment of emerging technologies.

Similarly, the e-commerce sector has grown exponentially, facilitating billions of dollars in annual transactions while compiling granular consumer behavior data. At the same time, Nigeria's government-led digitization efforts including the National Identity Management System (NIMS), the Bank Verification Number (BVN) scheme, and multiple e-government service platforms have established vast repositories of citizen information intended to streamline service delivery and reduce fraud.

However, incidents such as the 2024 XpressVerify scandal, in which sensitive data including National Identification Numbers (NINs), BVNs, driver's licenses, and passport records were discovered for sale online for as little as ₦100, underscored the systemic weaknesses in Nigeria's data governance architecture. The breach highlighted not only the inadequacy of security safeguards but also the urgent need for coherent, enforceable, and transparent data protection frameworks.⁸

Nigeria's initial regulatory response began with the Nigeria Data Protection Regulation (NDPR) of 2019, issued by the National Information Technology Development Agency (NITDA). While the NDPR established foundational data protection principles and compliance obligations, its limited scope, weak enforcement mechanisms, and overlapping institutional roles restricted its impact. The absence of a dedicated authority hindered the regulation's effectiveness in addressing cross-sectoral privacy risks emerging across Nigeria's expanding digital economy.

The most transformative milestone in Nigeria's data protection landscape has been the enactment of the Nigeria Data Protection Act (NDPA) 2023, which replaced the NDPR with a comprehensive, legally binding framework aligned with international standards. The NDPA represents the culmination of extensive multi-stakeholder advocacy, legislative consultation, and policy development, establishing the Nigeria Data Protection Commission (NDPC) as an independent statutory regulator with expanded powers of oversight, investigation, and enforcement.

The transition from a regulatory instrument to a fully-fledged Act marks a paradigm shift in Nigeria's data governance approach from fragmented, sector-specific oversight to a unified, rights-based framework comparable to the EU General Data Protection Regulation (GDPR). The NDPA codifies seven core data protection principles: lawfulness and transparency; purpose limitation; data minimization; accuracy; storage limitation; security; and accountability. It also enshrines comprehensive rights for data subjects, including access, rectification, erasure, portability, objection to processing, and the right to lodge complaints with the NDPC.⁹

The establishment of the NDPC as an independent enforcement authority has been pivotal in strengthening institutional capacity and regulatory credibility. Unlike NITDA, whose dual mandate created conflicts between technology promotion and data oversight, the NDPC operates exclusively to uphold privacy standards and protect citizens' rights. Since

8 Paradigm Initiative. (2024). "Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira." Retrieved from <https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/>.

9 Mercy King'ori. (2023). "Nigeria's New Data Protection Act, Explained." Retrieved from <https://fpf.org/blog/nigerias-new-data-protection-act-explained/>.

commencing operations in 2024, the Commission has initiated more than 1,368 investigations across multiple sectors and imposed landmark penalties, setting new precedents for data accountability across Africa.¹⁰ These investigations address systemic issues affecting millions of Nigerian consumers and demonstrate the commission's focus on protecting vulnerable populations from predatory data practices.¹¹

A defining example of this enforcement momentum was the \$220 million fine imposed on Meta Platforms in 2024 for discriminatory data practices and privacy violations, the largest such penalty ever issued by a regulator in the Global South. This unprecedented action underscored Nigeria's willingness to hold global technology firms accountable under domestic privacy standards. Similarly, Multichoice Nigeria was fined ₦766.2 million for unauthorized cross-border data transfers and inadequate user consent practices, reinforcing the NDPC's commitment to compliance and consumer protection.¹²

Despite significant progress, Nigeria's data protection environment continues to face evolving challenges shaped by technological innovation, cross-border integration, and institutional capacity constraints. The proliferation of artificial intelligence (AI) and machine learning across both public and private sectors introduces complex risks related to automated decision-making, algorithmic bias, and the secondary use of personal data for model training. These technologies often involve extensive data processing that tests the limits of principles such as consent and data minimization.

Cross-border data transfers remain another critical area of concern. As Nigerian organizations increasingly rely on global cloud services and international technology partnerships, compliance with the NDPA's adequacy and safeguard requirements poses both operational and legal complexities. Nigeria's own adequacy recognition by other jurisdictions particularly, the European Union remains pending, which may affect data flows essential to international trade and investment.

The digital lending sector continues to present persistent privacy risks despite efforts by the Central Bank of Nigeria and other financial regulators to curb abusive practices. The tension between financial innovation and privacy protection remains pronounced, as lenders depend on extensive personal data for credit scoring, raising questions about proportionality, informed consent, and users' ability to exercise their rights.

Government-led digital identity and data integration initiatives, while promising greater efficiency and reduced corruption, have also amplified privacy risks. Efforts to link national databases covering identity, taxation, immigration, and social services introduce single points of failure and magnify the impact of potential data breaches. The XpressVerify incident demonstrated the urgency of stronger cybersecurity measures, inter-agency coordination, and independent oversight.

Emerging technologies such as blockchain, cryptocurrency, and the Internet of Things (IoT) present additional regulatory frontiers. Their decentralized and data-intensive architectures challenge traditional legal frameworks, demanding ongoing dialogue between regulators, innovators, and civil society to ensure that privacy protections evolve in tandem with technological progress.

Legal and institutional framework

As earlier observed, the Nigeria Data Protection Act (NDPA) 2023 represents a landmark achievement in African digital governance, establishing one of the continent's most comprehensive and enforceable data protection regimes. Spanning 155 sections, the Act creates a robust regulatory structure encompassing legal principles, institutional arrangements, enforcement mechanisms, and individual rights.

Its broad scope applies to all entities; public or private, local or foreign that process personal data within Nigeria, or that process the data of individuals located in Nigeria, regardless of the processor's geographic location. This extraterritorial reach ensures that international organizations offering goods or services to Nigerian residents, or monitoring their online behavior, are subject to Nigerian data protection law.¹³ The provision aligns Nigeria with international best practice under the GDPR's "targeting and monitoring" test, reinforcing the principle of data sovereignty.

10 Steve Aya. (2025). "Nigeria Targets 1,368 Firms in Landmark Data Protection Crackdown." Retrieved from <https://www.thisdaylive.com/2025/09/02/nigeria-targets-1368-firms-in-landmark-data-protection-crackdown/>.

11 Frank Eleanya. (2025). "Nigeria's NDPC battles three loan shark breaches daily." Retrieved from <https://techcabal.com/2025/09/10/nigerias-ndpc-battles-three-loan-shark-breaches-daily/>.

12 ALT Advisory. (2024). "Nigeria: Meta fined \$220 million for breaching data protection and consumer laws." Retrieved from <https://dataprotection.africa/nigeria-meta-fined-220-million-for-breaching-data-protection-and-consumer-laws/>; Samson Akintaro. (2025). "Breaking: NDPC fines Multichoice Nigeria ₦766.2 million for violating NDP Act." Retrieved from <https://nairametrics.com/2025/07/06/breaking-ndpc-fines-multichoice-nigeria-n766-2-million-for-violating-ndp-act/>.

13 SecurePrivacy. (2025). "Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025." Retrieved from <https://secureprivacy.ai/blog/nigeria-data-protection-law>.

The NDPA harmonizes previously fragmented sectoral laws and embeds privacy protection as a fundamental right rather than a mere compliance requirement. By codifying clear obligations, it provides legal certainty to businesses while ensuring that data subjects retain meaningful control over their information.

The NDPA establishes seven foundational data protection principles that serve as the cornerstone of lawful and ethical data processing:

1. **Lawfulness and Transparency** – All processing must have a legitimate legal basis and be conducted in a transparent manner, ensuring that data subjects understand how their information is used.
2. **Purpose Limitation** – Data must be collected for specified, explicit, and legitimate purposes and cannot be repurposed in ways incompatible with those objectives.
3. **Data Minimization** – Processing should be limited to data that is adequate, relevant, and necessary for the intended purpose.
4. **Accuracy** – Data controllers are obligated to maintain accurate and up-to-date information, correcting or deleting inaccuracies promptly.
5. **Storage Limitation** – Data must not be retained longer than necessary for its intended use, and organizations must implement defined retention and deletion policies.
6. **Security and Integrity** – Controllers and processors must employ appropriate technical and organizational measures to safeguard data from unauthorized access, loss, or misuse.
7. **Accountability** – Organizations bear the ultimate responsibility for demonstrating compliance with all principles through documented governance frameworks and audits.¹⁴

The NDPA also strengthens data subject rights, empowering individuals to:

- Access their personal data and understand how it is processed;
- Request rectification or erasure of inaccurate or unlawfully held information;¹⁵
- Object to certain types of processing, including direct marketing;
- Restrict processing under specific conditions; and
- Request data portability where technically feasible.

These rights are supported by accessible redress mechanisms through the NDPC, which can issue binding decisions, enforce compliance, and impose penalties.

The creation of the Nigeria Data Protection Commission (NDPC) as an independent statutory body marks a pivotal advance in institutional governance. Freed from ministerial control, the NDPC possesses a focused mandate encompassing policy formulation, regulatory oversight, investigation, enforcement, and public education.

The Commission's independence is safeguarded through secure funding provisions, transparent appointment procedures, and fixed tenures for its leadership. This design aligns Nigeria's institutional model with global regulatory standards, enhancing credibility, continuity, and enforcement autonomy.

Organizations that process large volumes of data or conduct high-risk processing are required to appoint Data Protection Officers (DPOs) with appropriate qualifications and independence. The DPO serves as the compliance focal point within the organization, responsible for monitoring adherence, advising management, and acting as the contact point for both data subjects and the NDPC. This requirement institutionalizes internal accountability and professionalizes data protection compliance as a distinct corporate function.

14 KPMG Nigeria. (2023). "The Nigeria Data Protection Act, 2023: A Review of the Key Compliance Provisions and their Implications for Nigerian Businesses." Retrieved from <https://assets.kpmg.com/content/dam/kpmg/ng/pdf/the-nigeria-data-protection-act-2023.pdf>.

15 Nigeria Data Protection Commission. (2024). "About Us." Retrieved from <https://ndpc.gov.ng/about-us/>.

The NDPA mandates registration for all Data Controllers and Processors of Major Importance (DCPMIs) entities that process personal data of more than 20,000 individuals, generate annual turnover exceeding ₦100 million, or engage in cross-border data transfers. Registration includes submission of detailed processing inventories, risk assessments, and security frameworks.

Organizations undertaking high-risk processing such as large-scale profiling, biometric data collection, or processing involving vulnerable groups must conduct Data Protection Impact Assessments (DPIAs) to identify, assess, and mitigate risks before commencing operations.

In the event of a personal data breach, the NDPA requires notification to the NDPC within 72 hours of discovery if the breach is likely to pose a risk to data subjects.¹⁶ Affected individuals must also be informed where the breach presents a high risk to their rights or freedoms. Notifications must outline the breach's nature, scope, likely consequences, and remedial actions taken.

Nigeria's approach to cross-border data flows seeks to balance data sovereignty with economic integration in the global digital economy. The NDPA prohibits transfers to jurisdictions without adequate protection unless appropriate safeguards such as binding corporate rules, standard contractual clauses, or explicit data subject consent are implemented.¹⁷

The NDPC is empowered to conduct adequacy assessments and may designate certain countries or regional frameworks as offering equivalent protection. Nigeria has expressed intent to pursue mutual adequacy arrangements with other African jurisdictions and, eventually, with the European Union, a move that would significantly strengthen its digital trade competitiveness.

The NDPA grants the NDPC a comprehensive suite of enforcement powers, including authority to:

- Conduct audits and on-site inspections;
- Demand access to relevant documents or systems;
- Impose administrative fines and compliance orders;
- Suspend or restrict data processing operations; and
- Refer criminal violations for prosecution.

Penalties are proportionate to the severity of violations. Corporations may face fines ranging from ₦10 million to ₦10 billion, or up to 2% of annual global turnover, whichever is higher, while individuals may be fined between ₦2 million and ₦10 million. Serious breaches involving national security, children's data, or large-scale violations may attract criminal sanctions of up to three years' imprisonment. By combining deterrent penalties with structured compliance support, the NDPC has demonstrated a balanced approach asserting regulatory authority while promoting collaboration and capacity-building.¹⁸

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.
- Information on complaints received, investigations conducted, and penalties imposed, particularly in high-profile cases, remains largely unavailable.
- An assessment of the NDPC'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.

¹⁶ Mercy King'ori, op. cit.

¹⁷ SecurePrivacy, op. cit.

¹⁸ Sylvester Enoghase. (2025). "Wema Bank, Bet9ja Under Investigation For Data Privacy Breach – NDPB." Retrieved from <https://independent.ng/wema-bank-bet9ja-under-investigation-for-data-privacy-breach-ndpb/>.

- Efforts to educate citizens and businesses on their data privacy rights, complaint mechanisms, and compliance obligations. Nigeria 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 Nigeria's data protection implementation.

In sum, Nigeria's evolving data protection landscape reflects a maturing digital governance ecosystem that balances innovation with rights protection. The NDPA 2023 and the establishment of the NDPC have positioned Nigeria as a continental leader in privacy regulation, offering a model for other African jurisdictions.

Yet, sustained progress will depend on continued institutional strengthening, inter-agency collaboration, and international cooperation, particularly in addressing AI governance, cross-border data flows, and cyber resilience. If effectively implemented, Nigeria's data protection framework can serve not only as a legal safeguard but also as a strategic enabler of trust, inclusion, and sustainable digital growth across Africa.

3.2 Ghana's Data Protection Regime

Context and background

Ghana has positioned itself as a regional leader in establishing a structured and comprehensive data protection regime. This report provides a detailed assessment of Ghana's data protection and privacy compliance landscape across key sectors; telecommunications, e-commerce, online betting, banking and finance, insurance, healthcare, government agencies, and digital lending highlighting both advancements and ongoing compliance gaps.¹⁹

The framework articulates clear obligations for organizations that collect, store, or process personal data, emphasizing transparency, fairness, security, and accountability in line with internationally recognized privacy principles. It further promotes the rights of data subjects while mandating organizational accountability through registration, monitoring, and enforcement mechanisms aimed at ensuring lawful processing of personal data.²⁰

Despite these achievements, compliance across sectors remains inconsistent. A number of organizations either lack explicit privacy policies or fail to make them publicly accessible. Others operate with expired certifications, undefined data retention timelines, weak recognition of user rights, and inadequate disclosures on third-party data transfers. Notable exceptions include leading entities such as MTN, Stanbic Bank, Hollard Insurance, and The Trust Hospital, which demonstrate comparatively stronger privacy and security governance frameworks.²¹ These discrepancies underscore systemic challenges related to regulatory oversight, institutional capacity, and uneven compliance awareness among data controllers and processors.

Positive Developments and Emerging Issues

The DPC has undertaken several initiatives aimed at strengthening compliance and building public trust in data governance. These include:

- Digitization of registration and reporting systems, enabling online submission and renewal of licenses;
- Public awareness and training campaigns targeting both the private sector and government agencies;
- Annual stakeholder conferences and sectoral roundtables on data protection compliance; and
- Partnerships with international and regional bodies, including the Network of African Data Protection Authorities (NADPA) and the Global Privacy Assembly (GPA).²²

These initiatives have improved registration rates among large corporations and fostered a gradual increase in compliance awareness.

¹⁹ Data Protection Commission, *Annual Compliance Report*, Accra, 2024.

²⁰ Data Protection Act, 2012 (Act 843).

²¹ Author's assessment based on sectoral privacy policy review, 2025.

²² DPC, *Public Engagement and Awareness Strategy*, 2023.

However, emerging challenges continue to test the resilience of Ghana's data protection framework. Rapid digitization across fintech, digital lending, e-health, and online betting sectors has introduced new complexities in data flows and third-party processing. Additionally, the use of biometric and surveillance technologies in public administration and private service delivery has heightened concerns regarding proportionality, consent, and data retention practices.²³

Legal and Institutional Framework

Ghana's data protection regime derives its legitimacy from the 1992 Constitution, which enshrines the right to privacy under Article 18(2), safeguarding individuals from unlawful interference with their correspondence, communications, and personal affairs.²⁴ This constitutional guarantee provides the foundation for subsequent legislative and policy interventions in data protection.

The principal legislation governing data protection in Ghana is the Data Protection Act, 2012 (Act 843). The Act provides a comprehensive framework for the lawful collection, processing, and use of personal data. It defines the obligations of data controllers and data processors, establishes the rights of data subjects, and sets out mechanisms for enforcement and redress.²⁵

Act 843 codifies fundamental Data Protection Principles, requiring that personal data be:

- Processed fairly and lawfully;
- Collected for specific, explicit, and legitimate purposes;
- Adequate, relevant, and not excessive;
- Accurate and kept up to date;
- Retained only as long as necessary; and
- Secured through appropriate technical and organizational safeguards.²⁶

Data subjects are entitled to various rights under the Act, including:

- The right of access to personal information held about them;
- The right to prevent processing likely to cause harm or distress;
- The right to object to processing for direct marketing; and
- The right to rectification, blocking, erasure, or destruction of inaccurate or unlawfully held personal data (Section 42, Act 843).²⁷

Act 843 establishes the Data Protection Commission (DPC) as the statutory authority responsible for administering and enforcing the Act.²⁸ The DPC's core functions include:

- Maintaining the Data Protection Register of all registered data controllers and processors;
- Monitoring and auditing compliance with Act 843;
- Receiving and investigating complaints from data subjects;
- Issuing information and enforcement notices; and
- Imposing administrative sanctions or initiating legal proceedings against non-compliant entities.²⁹

The DPC also conducts public awareness campaigns and provides sector-specific compliance guidance. Nevertheless, limited financial and technical resources have hindered the Commission's ability to carry out consistent audits and large-scale enforcement operations.³⁰

²³ Privacy International, *Biometric Data and Privacy in Africa*, 2022.

²⁴ Constitution of the Republic of Ghana, 1992, Article 18(2).

²⁵ Act 843, Sections 1–5.

²⁶ *Ibid.*, Section 17.

²⁷ *Ibid.*, Section 42.

²⁸ Act 843, Part II.

²⁹ DPC, *Functions and Mandate Overview*, 2023.

³⁰ DPC, *Institutional Capacity Assessment Report*, 2022.

Under Part IV of Act 843, all data controllers and processors must register with the DPC prior to processing personal data. Section 52 prohibits unregistered entities from engaging in data processing activities.³¹ Despite this mandatory requirement, compliance levels remain low, particularly among small and medium-sized enterprises (SMEs) and digital startups, many of which lack awareness of their statutory obligations.

Part V of Act 843 places stricter controls on the processing of sensitive personal data, including information relating to health, genetics, biometrics, race, ethnicity, and political affiliation. Certain categories of processing require prior authorization from the DPC to ensure adequate safeguards against misuse.³²

Section 40 of the Act restricts the transfer of personal data outside Ghana to jurisdictions that do not offer an adequate level of protection. Transfers may only occur if the data subject consents or if adequate contractual or organizational safeguards are in place.³³ While the provision aligns with international standards, operational guidance and enforcement remain limited, and Ghana has not yet published an official list of countries deemed to offer adequate protection.

Complementary Legislation includes;

Act 843 is complemented by other legal instruments, including:

- The Electronic Transactions Act, 2008 (Act 772), which provides for the confidentiality and protection of personal information in electronic communications; and
- The Cybersecurity Act, 2020 (Act 1038), which established the Cyber Security Authority (CSA) and created a framework for reporting and managing cybersecurity incidents, including those involving personal data breaches.³⁴

Together, these statutes form a multi-layered framework for data governance and protection in Ghana's digital economy.

Institutional Capacity and Regulatory Updates

Recent institutional reforms indicate growing momentum toward stronger governance and transparency. The DPC has:

- Developed a centralized compliance database to track registration status and enforcement actions;
- Introduced self-assessment tools for organizational compliance reporting;
- Expanded staff capacity through technical training and partnerships with academic and international institutions; and
- Initiated consultations on amending Act 843 to address new issues, including children's data protection, breach reporting obligations, and adequacy determinations for cross-border data transfers.³⁵

In addition, the DPC has expressed plans to publish annual compliance and enforcement reports, enhance collaboration with the Cyber Security Authority, and expand public engagement on digital rights and privacy protection³⁶.

Challenges and Enforcement Dynamics

Despite notable progress, enforcement remains one of the weakest elements of Ghana's data protection regime. The DPC faces persistent resource and capacity constraints, which limit its ability to conduct regular audits, investigate breaches, and impose timely sanctions³⁷.

The absence of comprehensive data breach notification procedures and sector-specific regulations further complicates enforcement. Moreover, Act 843 has not been substantively amended since 2012, leaving it partially misaligned with global best practices such as the EU General Data Protection Regulation (GDPR) and the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention)³⁸.

³¹ Act 843, Section 52.

³² Ibid., Part V.

³³ Ibid., Section 40.

³⁴ Electronic Transactions Act, 2008 (Act 772); Cybersecurity Act, 2020 (Act 1038).

³⁵ DPC, Regulatory Reform Consultation Paper, 2024.

³⁶ Cyber Security Authority, Collaborative Enforcement Strategy, 2024.

³⁷ DPC, Compliance Audit Findings, 2024.

³⁸ AU, Malabo Convention on Cybersecurity and Data Protection, 2014.

Direct outreach to obtain specific enforcement data, institutional capacity information, and regulatory updates from Ghana's Data Protection Commission (DPC) did not yield responses. Consequently, the assessment faced challenges in acquiring official or current data on enforcement performance and institutional operations.

The assessment sought to obtain insights in the following key areas:

- **Public Register and Registration Data:** Information on the availability of a public register of data controllers and processors, including statistics on active versus inactive registrations. While Ghana has established a registration framework under the Data Protection Act, 2012 (Act 843), publicly accessible and regularly updated statistics on registration compliance remain limited.
- **Complaints, Investigations, and Sanctions:** Data on complaints received, investigations conducted, and administrative or monetary penalties imposed, particularly in significant or high-profile cases. Such enforcement metrics were not publicly available at the time of reporting, limiting visibility into the DPC's oversight activities.
- **Institutional Capacity:** An assessment of the DPC's staffing levels, technical infrastructure, budgetary allocations, and collaborative arrangements with domestic and international counterparts to support enforcement and compliance monitoring. Publicly accessible information on these parameters is minimal.
- **Regulatory and Policy Updates:** Information on the issuance of operational guidelines, sector-specific codes of conduct, or legislative amendments to address emerging challenges in privacy, cybersecurity, and cross-border data transfers. Available documentation indicates ongoing discussions on revising Act 843, but no substantive amendments have yet been enacted.
- **Public Education and Awareness:** Insights into efforts to enhance citizens' and organizations' understanding of data privacy rights, complaint mechanisms, and compliance responsibilities. While the DPC has conducted periodic awareness campaigns and stakeholder training, detailed statistics on outreach impact or coverage were unavailable.
- **Compliance Monitoring and Risk-Based Audits:** Information on proactive investigations, compliance audits, and risk-based monitoring, particularly in high-risk sectors such as telecommunications, finance, and healthcare. No comprehensive data was made available to indicate the frequency, scope, or outcomes of such enforcement activities.

Despite these targeted inquiries, no official regulatory responses were received, making it difficult to fully evaluate the extent, consistency, and overall effectiveness of Ghana's data protection enforcement regime. The absence of publicly available enforcement data underscores broader challenges related to institutional transparency, reporting practices, and resource constraints within the DPC, which collectively hinder independent assessment of compliance outcomes and regulatory impact.

Nevertheless, the DPC has made efforts to enhance cooperation with sector regulators such as the Bank of Ghana (BoG), the National Communications Authority (NCA), and the National Information Technology Agency (NITA) to harmonize regulatory approaches and share compliance intelligence³⁹.

Ghana's data protection regime stands as one of the most mature and comprehensive in the West African subregion. The legislative foundation, anchored in constitutional guarantees and operationalized through Act 843 has established a strong framework for protecting personal data and ensuring organizational accountability.

However, the sustainability of these gains depends on strengthening the institutional autonomy, technical capacity, and financial stability of the DPC. Modernizing the legislative framework to address cross-border data flows, biometric data processing, and breach notifications is equally critical.

With continued policy reform, regional cooperation, and sectoral compliance alignment, Ghana is well positioned to consolidate its leadership in privacy governance and contribute meaningfully to the development of a harmonized African data protection ecosystem⁴⁰.

³⁹ Bank of Ghana, *Data Governance in Financial Institutions*, 2023.

⁴⁰ Author's synthesis based on stakeholder interviews, 2025.

3.3 Botswana's Data Protection Regime

Context and background

Botswana is a landlocked country in Southern Africa, bordered by South Africa to the south and east, Namibia to the west, and Zimbabwe to the northeast. With a population of approximately 2.5 million people as of 2025, Botswana is characterized by a young demographic profile over 60% of the population is under 30 years old, and the median age is 23.4 years.⁴¹ The country's official language is English, while Setswana remains the most widely spoken language.

Geographically, much of Botswana's landmass is covered by the Kalahari Desert, limiting agricultural potential and driving the economy toward sectors such as mining, services, and information and communications technology (ICT).⁴² As an upper-middle-income country, Botswana enjoys a reputation for political stability, low corruption, and a safe environment for business and investment.⁴³

The country's youthful population has been a key driver of digital growth and innovation, particularly in mobile technology and digital financial services. The government's development blueprint Vision 2036 articulates four foundational pillars: (1) sustainable economic development; (2) human and social development; (3) sustainable environment; and (4) governance, peace, and security.⁴⁴ Central to this vision is digital transformation, which is positioned as a catalyst for economic diversification, public sector efficiency, and social inclusion.

Under Vision 2036, Botswana has launched strategic initiatives such as the National ICT Policy (Maitlamo)⁴⁵ and the Digital Transformation Strategy,⁴⁶ both aimed at strengthening ICT infrastructure, enhancing connectivity, promoting e-governance, and fostering innovation. These frameworks emphasize security, confidentiality, and responsible data handling, even though explicit data privacy provisions were initially limited.

The Digital Transformation Strategy envisions a "smart, sustainable society" by applying a whole-of-government approach to digitize service delivery, improve efficiency, and extend digital access to underserved communities.⁴⁷ Initiatives such as Smart Villages and digital inclusion programs are bridging the urban-rural digital divide.⁴⁸ Additionally, the growth of mobile banking, e-commerce, and e-government platforms has expanded access to services while also increasing the urgency of safeguarding personal information within an evolving digital ecosystem.⁴⁹

Positive Developments and Emerging Issues

Botswana's commitment to data protection has evolved in parallel with its broader digital transformation agenda. The recognition of personal data as a critical national asset has prompted legal and institutional reforms aimed at enhancing privacy, trust, and accountability in the digital economy.⁵⁰

Key positive developments include:

- The enactment of comprehensive data protection legislation and the establishment of an independent regulatory body;⁵¹
- Integration of data privacy principles within national ICT and digital transformation policies;⁵²
- Ongoing public sector digitization that emphasizes security and responsible information management;⁵³ and
- Increased private sector compliance efforts, particularly among financial and telecommunications entities.⁵⁴

41 Statistics Botswana, *Population and Housing Census 2022: Analytical Report* (Stats Botswana 2023).

42 UNDP, *Human Development Report: Botswana* (UNDP 2024).

43 World Bank, *Botswana Country Data* (World Bank 2024).

44 Government of Botswana, *Vision 2036* (2016).

45 Ministry of Transport and Communications, *Maitlamo: National ICT Policy* (2007).

46 Ministry of Communications, Knowledge and Technology, *Digital Transformation Strategy 2022–2027*.

47 Ibid.

48 Government of Botswana, *Smart Botswana/Smart Villages Programme* (publication year applicable).

49 GSMA, *Mobile Internet Connectivity Report – Sub-Saharan Africa* (latest edition).

50 NADPA, *Annual Activity Report* (latest year).

51 Data Protection Act 2018 (Botswana).

52 Ministry of Transport and Communications (n 45).

53 Digital Transformation Strategy (n 46).

54 BOCRA, *Annual Report* (latest year).

However, emerging issues remain. Rapid digitalization driven by fintech, e-health, and mobile money services has expanded the volume and complexity of data processing activities.⁵⁵ While this growth enhances service access, it also exposes users to higher privacy and cybersecurity risks. Low public awareness of data privacy rights, inadequate reporting mechanisms for breaches, and limited institutional capacity continue to undermine effective implementation.⁵⁶

Moreover, balancing innovation and regulation remains a pressing challenge. As Botswana pursues technological advancement and cross-border data exchange, it must ensure that privacy protection keeps pace with digital expansion, especially in high-risk sectors such as finance, telecommunications, and healthcare.⁵⁷

Legal and institutional framework

Botswana's first data protection law, the Data Protection Act of 2018, represented an important milestone in recognizing privacy as a fundamental right. The Act outlined the rights of individuals and imposed obligations on data controllers and processors to ensure lawful, fair, and secure processing of personal data. However, several weaknesses hindered its effectiveness, including:

- The exclusion of certain government data processing activities from compliance obligations;
- Limited coverage of personal or household data processing;
- Ambiguity regarding the Act's application to cross-border data controllers; and
- Implementation delays due to ministerial extensions and regulatory gaps.⁵⁸

These shortcomings resulted in limited enforcement and minimal impact on data protection practices.

The enactment of the Data Protection Act, 2024 (effective January, 2025)⁵⁹, which repealed and replaced the 2018 Act, marked a significant advancement in Botswana's privacy framework. The new legislation introduces several salient reforms, including:

- **Enhanced Investigative Powers:** The Information and Data Protection Commission (IDPC) is granted expanded authority to conduct searches, seizures, and detentions during investigations, provided that procedural safeguards such as judicial warrants or written consent from premises owners are observed.⁶⁰
- **Strengthened Accountability Measures:** The Act mandates data controllers and processors to implement robust technical and organizational safeguards, clearly define roles in multi-controller arrangements, and formalize processing agreements particularly where foreign entities or third parties are involved.⁶¹
- **Local Representation:** Foreign data controllers operating in Botswana must appoint local representatives to ensure accountability and regulatory oversight.⁶²
- **Reclassification of Processors:** Processors acting beyond their authorized instructions may now be deemed data controllers, making them directly liable for compliance obligations.⁶³
- **Legitimate Restrictions:** Certain legal provisions may restrict data processing rights, but only when such limitations are necessary, proportionate, and consistent with constitutional and democratic principles.⁶⁴
- **Institutional Independence:** The Act establishes a more autonomous Commission by introducing dedicated divisions for Data Protection and Access to Information, imposing term limits and age caps for Commissioners, and mandating institutional separation from executive influence.⁶⁵

⁵⁵ Bank of Botswana, *Fintech and Digital Financial Services Report* (latest year).

⁵⁶ ODPC public awareness updates (where applicable).

⁵⁷ GSMA (n 49).

⁵⁸ Government Gazette (Botswana), notices on commencement extensions.

⁵⁹ Government of Botswana, *Data Protection Act 2024* (Botswana, 14 January 2025) https://www.gov.bw/sites/default/files/2025-01/Data_Protection_Act_2024.pdf accessed 14 November 2025.

⁶⁰ Data Protection Act 2024 (Botswana).

⁶¹ Data Protection Act 2024 (Botswana).

⁶² Data Protection Act 2024 (Botswana).

⁶³ Data Protection Act 2024 (Botswana).

⁶⁴ Constitution of Botswana (as amended).

⁶⁵ Data Protection Act 2024 (Botswana).

Collectively, these provisions bring Botswana's data protection framework closer to international standards, such as the EU General Data Protection Regulation (GDPR)⁶⁶ and the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention).⁶⁷

Enforcement dynamics and challenges

The Office of the Data Protection Commissioner (ODPC) operating under the new Information and Data Protection Commission serves as the enforcement authority responsible for ensuring compliance with the 2024 Act.⁶⁸ The Office has begun initiating investigations, particularly in the financial and telecommunications sectors, where unauthorized data sharing and marketing practices have been observed.⁶⁹

Furthermore, the Commission responded to the direct outreach seeking specific enforcement data, including statistics on complaints, investigations, sanctions, and resource allocations.⁷⁰ However, as a newly established institution and with the Data Protection Act, 2024 having only come into effect in early 2025 there is currently limited enforcement activity to report.⁷¹

The Commission is still in the process of building its institutional capacity, developing operational frameworks, and establishing reporting mechanisms necessary for effective oversight and enforcement. Consequently, publicly available enforcement data remain scarce, making it difficult to comprehensively assess the scope of regulatory activity and institutional performance at this stage.

The above notwithstanding, several enforcement and institutional challenges are evident:

- **Limited Institutional Capacity:** The ODPC continues to face resource shortages, including staffing, technical expertise, and funding constraints, which hinder effective monitoring, auditing, and enforcement.
- **Regulatory Independence:** Despite legislative reforms, questions persist regarding the Commission's autonomy due to its administrative placement under the Ministry of State President, potentially affecting perceived impartiality.
- **Low Public Awareness:** Many citizens remain unaware of their rights under the new law or of available complaint and redress mechanisms, limiting bottom-up enforcement through public participation.⁷²
- **Data Breach Management:** Comprehensive procedures for breach notification and response are still being developed, and there is no central repository for breach reporting or publication of enforcement outcomes.⁷³
- **Transparency Deficits:** The absence of a publicly accessible register of data controllers and processors, as well as limited disclosure of enforcement statistics, hampers accountability.⁷⁴

Despite these challenges, Botswana's data protection authority has shown commitment to institutional growth through staff training, public education campaigns, and engagement with regional partners such as the Network of African Data Protection Authorities (NADPA).⁷⁵ Continued capacity building, regulatory transparency, and inter-agency collaboration will be essential to strengthen enforcement credibility and build public trust in the regime.

Botswana's evolving data protection regime demonstrates a clear trajectory toward stronger privacy governance and digital accountability. The enactment of the Data Protection Act, 2024, the establishment of a more independent regulatory body, and the integration of privacy principles into national ICT strategies signify substantial progress.⁷⁶ Nevertheless, the effectiveness of enforcement will depend on closing institutional capacity gaps, improving transparency, and increasing public awareness of privacy rights. As Botswana advances its digital transformation agenda, achieving an equitable balance between innovation, economic growth, and data privacy will be vital for sustainable and inclusive digital development.⁷⁷

66 Regulation (EU) 2016/679 (GDPR).

67 African Union, *Malabo Convention* (2014).

68 Data Protection Act 2024 (Botswana).

69 ODPC (Botswana), Enforcement Updates (if published).

70 Ibid.

71 Ibid.

72 ODPC Public Education Programmes.

73 Data Protection Act 2024, Part on Breach Procedures.

74 IDPC Compliance and Registration Notices.

75 NADPA, *Annual Activity Report*.

76 Data Protection Act 2024 (Botswana).

77 Vision 2036 (n 44); Digital Transformation Strategy (n 53).

Rwanda Data Protection Regime

Context and Background

Rwanda continues to position itself as a regional leader in digital transformation, anchored in long-term strategies such as Vision 2050 and the Smart Rwanda Master Plan.⁷⁸ As reflected in the 2024 analysis, ICT remains central to Rwanda's ambition to build a knowledge-based economy, supported by near-universal 4G coverage, high mobile penetration, and strong growth in mobile money and e-government services.⁷⁹ Between 2024 and 2025, this trajectory has largely been sustained. Digital services continue to expand across telecommunications, fintech, e-commerce, online betting, healthcare, and public administration. The increasing digitisation of justice systems (e.g., IECMS), financial services, and public platforms has deepened data-driven governance and commercial activity.⁸⁰

However, as in 2024, this transformation entails large-scale collection and processing of sensitive personal data including financial, biometric, health, and location data across both public and private sectors. While digital innovation advances inclusion and efficiency, it also intensifies risks relating to privacy, cybersecurity, profiling, and cross-border data transfers. The central policy tension remains unchanged: how to sustain innovation while safeguarding constitutional privacy guarantees and data protection rights.⁸¹

Positive Developments and Emerging Issues

A major milestone, already noted in 2024 and retained for 2025, is the enactment of Law No. 058/2021 Relating to the Protection of Personal Data and Privacy (DPP Law).⁸² The two-year compliance grace period ended in October 2023, marking the transition from normative adoption to expected operational compliance.

Institutionally, the establishment of the Data Protection and Privacy Office (DPPO) within the National Cyber Security Authority (NCSA) in 2022 represented an important step toward operationalising the framework.⁸³ Public sensitisation campaigns (e.g., Tekana Online), publication of complaint forms and transfer authorisation templates, and issuance of initial regulatory guidance signalled early implementation efforts.

For 2025, these developments remain relevant and should be retained as indicators of institutional progress. However, emerging concerns identified in 2024 persist:

- Limited publicly accessible compliance data (e.g., no comprehensive public register of controllers/processors).
- Minimal transparency regarding investigations, sanctions, or enforcement statistics.
- Limited secondary regulations or sector-specific guidance to clarify operational obligations.

New and continuing issues for 2025 include increasing reliance on cross-border cloud services, AI-driven analytics, and expanded fintech ecosystems, which heighten the urgency for clearer adequacy rules, supervisory coordination, and technical oversight mechanisms.

Legal and Institutional Framework

Rwanda's data protection regime is grounded in Law No. 058/2021, which provides a comprehensive legal basis governing collection, processing, storage, transfer, and protection of personal data.⁵ The law aligns with international and regional instruments, including the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and principles comparable to the GDPR.⁸⁴

Key elements of the framework include:

- Broad definition of personal data (including biometric and sensitive data).
- Lawful processing principles (lawfulness, fairness, purpose limitation, proportionality).
- Recognition of data subject rights (access, rectification, erasure, restriction, objection, portability).

⁷⁸ Government of Rwanda, *Vision 2050* and Smart Rwanda Master Plan.

⁷⁹ 2024 Analysis – Rwanda's Data Protection Regime (ICT penetration, mobile subscriptions, financial inclusion statistics).

⁸⁰ 2024 Analysis – Implementation of Rwanda Integrated Electronic Case Management System (IECMS).

⁸¹ Constitution of the Republic of Rwanda, Article 23 (Right to Privacy).

⁸² Law No. 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy.

⁸³ Law No. 26/2017 Establishing the National Cyber Security Authority; establishment of the DPPO (March 2022).

⁸⁴ African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention); EU General Data Protection Regulation (GDPR).

- Mandatory security safeguards and breach notification obligations.
- Requirements for appointment of Data Protection Officers (DPOs) in high-risk processing contexts.
- Conditions governing cross-border data transfers based on adequacy or appropriate safeguards.

Enforcement authority rests with the National Cyber Security Authority, which maintains the registry of controllers and processors, receives complaints, conducts investigations, and may impose administrative sanctions.⁸⁵ Sector regulators including Rwanda Utilities Regulatory Authority (telecommunications and betting), National Bank of Rwanda (financial services), and Rwanda Information Society Authority (ICT systems and e-government infrastructure) play complementary roles.

Compared to 2024, the legal framework itself remains stable and robust on paper. The core structure does not require revision; rather, the emphasis for 2025 shifts toward operationalisation, regulatory detailing, and institutional strengthening.

Enforcement Dynamics and Challenges

The primary continuity between 2024 and 2025 lies in the implementation gap. While Rwanda's legal framework is comprehensive, enforcement dynamics remain relatively opaque. Just like last year, efforts were 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. However, direct outreach to obtain specific data and detailed status updates on enforcement and monitoring efforts proved unsuccessful. Moreover, the lack of direct responses from the DPPO made it difficult to assess the full scope of enforcement effectiveness and implementation progress.

Key challenges however retained from the 2024 assessment include:

1. ***Institutional Independence and Capacity*** – The DPPO operates under the NCSA, limiting its administrative and financial autonomy.⁶ Resource constraints may affect staffing, audit capacity, and proactive investigations.
2. ***Limited Transparency*** – There is no fully accessible public database of registered data controllers and processors, nor regular publication of enforcement statistics.
3. ***Regulatory Gaps*** – Few detailed implementing regulations, dispute resolution mechanisms, or appellate procedures have been publicly elaborated.
4. ***Low Public Awareness*** – Citizen understanding of complaint procedures and enforceable rights remains limited.
5. ***Limited Proactive Oversight*** – There is little publicly available evidence of sector-wide audits or risk-based investigations in high-risk sectors such as telecoms, finance, and health.

This assessment suggests incremental progress but no structural transformation in enforcement visibility. As digital ecosystems expand and cross-border processing intensifies, the absence of consistent public reporting and robust sanctioning practice risks weakening deterrence and public trust.

Accordingly, the core priority moving forward remains bridging the gap between legal design and practical enforcement through enhanced regulatory independence, transparent reporting, sector-specific guidance, capacity building, and strengthened inter-agency coordination.

Tanzania Data Protection Regime

Context and Background

Tanzania, officially the United Republic of Tanzania, is a federal constitutional republic comprising Mainland Tanzania and Zanzibar. According to the 2022 National Housing and Population Census, the country had a population of 61,741,120, which has continued to grow.⁸⁶ As of January 2025, Tanzania recorded over 48 million internet users, reflecting rapid digital uptake across sectors.⁸⁷

⁸⁵ Law No. 058/2021, Articles relating to supervisory authority powers and sanctions.

⁸⁶ National Housing and Population Census, 2022 (United Republic of Tanzania).

⁸⁷ National digital usage statistics, January 2025.

As noted in the 2024 analysis, Tanzania's digital expansion has been accompanied by increased data generation through telecommunications, financial services, online platforms, and government systems. While not all privacy concerns are internet-based, the digital ecosystem has become the principal medium for the collection, processing, and transfer of personal data both lawfully and unlawfully.

The 2024 assessment emphasized the transition from fragmented sectoral privacy protections to a unified statutory regime.

That transition remains central in 2025. The enactment of the Personal Data Protection Act (PDPA) marked a structural shift in Tanzania's governance framework, positioning data protection as a cross-cutting regulatory priority rather than a sector-specific concern. However, the key issue moving into 2025 is no longer legislative absence but effective implementation, transparency, and regulatory maturity.

Positive Developments and Emerging Issues

A major development retained from the 2024 review is the operationalisation of the Personal Data Protection Act, 2022, which came into effect on 1 May 2023.⁸⁸ The formal launch of the Personal Data Protection Commission (PDPC) on 3 April 2024 marked a critical institutional milestone.⁸⁹ The 2024 analysis highlighted Tanzania's progress in establishing registration mechanisms for data controllers and processors, initiating awareness campaigns, and developing subsidiary regulations including the Personal Data Protection (Personal Data Collection and Processing) Regulations and the Complaints Settlement Procedures. These foundational steps remain valid indicators of institutional commitment in 2025.

However, several emerging and continuing issues persist:

- Limited public access to a comprehensive and searchable register of data controllers and processors.
- Minimal publicly available enforcement statistics (complaints received, investigations conducted, penalties imposed).
- Broad statutory exemptions relating to national security and law enforcement, raising proportionality concerns.
- Expanding surveillance-related data systems, including subscriber databases and equipment registers, which heighten privacy risks.

The rapid growth of digital finance, mobile services, and data-driven public administration in 2025 further intensifies the need for proactive oversight, particularly in high-risk sectors such as telecommunications, banking, and health services.

Legal and Institutional Framework

The constitutional foundation for privacy in Tanzania is found in Article 16 of the Constitution of the United Republic of Tanzania, which guarantees the right to privacy, family life, residence, and private communications.⁹⁰ However, Article 16(2) permits statutory limitations where prescribed by law, establishing a qualified not absolute right. Prior to the PDPA, privacy protections were dispersed across sectoral statutes, including the Electronic and Postal Communications Act, 2010 (EPOCA), the Cybercrimes Act, the Banking and Financial Institutions Act, and related regulations.⁹¹ The PDPA consolidated these fragmented provisions into a comprehensive regime governing personal data processing across public and private entities. The PDPA incorporates core data protection principles aligned with global standards (including GDPR-inspired principles), such as:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation and accuracy
- Security safeguards
- Accountability

⁸⁸ Personal Data Protection Act, 2022 (Tanzania), effective 1 May 2023.

⁸⁹ Launch of the Personal Data Protection Commission, 3 April 2024.

⁹⁰ Constitution of the United Republic of Tanzania, Article 16.

⁹¹ Electronic and Postal Communications Act, 2010 and related regulations; Cybercrimes Act; Banking and Financial Institutions Act.

The Act applies to data controllers and processors established in Tanzania, as well as extraterritorial entities processing personal data within Tanzania. Its application extends to Zanzibar only in respect of Union matters, consistent with the constitutional structure.⁹² The PDPA provides:

- Mandatory registration of controllers and processors
- Consent-based processing requirements
- Enhanced safeguards for sensitive personal data (e.g., biometric, financial, genetic, political, religious, health-related data)
- Rights of data subjects (access, rectification, erasure, objection to direct marketing, restriction, compensation)
- Regulation of cross-border data transfers based on adequacy or safeguards

Tanzania is a State Party to the International Covenant on Civil and Political Rights (ICCPR), which protects the right to privacy under Article 17.⁹³ The Human Rights Committee's General Comment No. 16 further affirms that personal data collection and storage must be regulated by law and subject to safeguards, reinforcing Tanzania's domestic obligations. The primary data protection regulator is the Personal Data Protection Commission, established under Section 6 of the PDPA.⁹⁴ The Commission is mandated to:

- Monitor compliance
- Register controllers and processors
- Investigate complaints
- Conduct public awareness
- Advise government
- Promote international cooperation

The Commission is headed by a Director General appointed by the President, while the Minister of ICT appoints members of its Board and hears appeals relating to registration decisions.⁹⁵

Other relevant institutions include:

- Tanzania Communications Regulatory Authority (TCRA), which regulates telecommunications and maintains the Central Equipment Identification Register (CEIR).
- The TCRA Content Committee, which addresses consumer complaints under Online Content Regulations.
- The Tanzania Police Force Cybercrimes Unit, enforcing the Cybercrimes Act.
- The Ministry of ICT, responsible for sectoral policy oversight.

Compared to 2024, the institutional architecture remains intact. The PDPC is now formally operational, but its regulatory footprint remains in an early stage of consolidation.

Enforcement Dynamics and Challenges

The central continuity between 2024 and 2025 is the limited visibility of enforcement outcomes. As in the previous assessment, efforts were undertaken to engage with Tanzania's data protection regulator, the Personal Data Protection Commission, to obtain direct insights into key regulatory areas including registration of data controllers and processors, enforcement actions, institutional capacity, public engagement, and compliance monitoring. However, direct outreach to secure specific data and detailed updates on enforcement trends and supervisory activities was unsuccessful. The absence of substantive responses from the Commission limited the ability to comprehensively evaluate enforcement effectiveness, regulatory priorities, and the overall progress of implementation under Tanzania's data protection framework.

⁹² Constitution of the United Republic of Tanzania (Union and non-Union matters).

⁹³ International Covenant on Civil and Political Rights (ICCPR), Article 17; General Comment No. 16.

⁹⁴ Personal Data Protection Act, 2022 (Tanzania), effective 1 May 2023.

⁹⁵ Personal Data Protection Act, provisions relating to appointment and appeals.

Although Tanzania has established a comprehensive statutory framework and an operational regulator, enforcement transparency remains constrained. Key retained challenges include:

1. **Transparency Deficits** – There is limited publicly accessible data on registration statistics, complaint volumes, investigations, or sanctions.
2. **Regulatory Capacity** – Limited publicly available information on staffing levels, technological resources, and budget allocations makes it difficult to assess enforcement readiness.
3. **Broad Exemptions** – National security and law enforcement carve-outs may undermine proportionality if not narrowly interpreted.
4. **Surveillance Concerns** – Provisions requiring subscriber data retention and centralised equipment identification databases raise risks of overreach.
5. **Limited Proactive Oversight** – There is little public evidence of systematic audits or risk-based compliance reviews in high-risk sectors.

While Tanzania's legal foundation remains robust and largely unchanged from 2024, the 2025 status quo suggests that implementation maturity is still evolving. The transition from legislative establishment to consistent enforcement reporting, audit activity, and public accountability will determine whether the PDPA achieves its intended protective impact.

To consolidate gains, priority actions for 2026 include:

- Publishing periodic enforcement and compliance reports;
- Establishing a fully accessible public registry of data controllers and processors;
- Clarifying operational guidelines and sector-specific codes of conduct;
- Strengthening institutional capacity and inter-agency coordination;
- Enhancing stakeholder engagement and international cooperation.

Sustained improvements in transparency and enforcement practice will be critical to building public trust and positioning Tanzania as a credible data governance leader within the region.

Mauritius' Data Protection Regime

Context and Background

Mauritius is a small island state in the Indian Ocean with a population of approximately 1.26 million (2022).⁹⁶ Over the past five decades, it has transitioned from a mono-crop sugar economy to an upper-middle-income country, driven by political stability, economic diversification, and strong institutions. Key sectors including tourism, financial services, ICT, fisheries, and manufacturing now contribute significantly to GDP, with financial and ICT services alone accounting for a substantial share of economic activity.⁹⁷

The 2024 analysis underscored Mauritius' reputation as one of Africa's leaders in regulatory governance, including in data protection. That positioning remains largely intact in 2025. However, increasing digitisation of financial services, cross-border business processing, and e-government platforms continues to intensify personal data flows, raising new questions about regulatory adaptability, enforcement transparency, and technological oversight.

While the COVID-19 pandemic temporarily disrupted economic performance, recovery measures have stabilised growth. The policy emphasis in 2025 remains on strengthening digital trust to support Mauritius' role as a financial and ICT hub—making effective data protection governance a strategic priority rather than merely a compliance obligation.

Positive Developments and Emerging Issues

As noted in the 2024 assessment, Mauritius maintains one of the most advanced statutory data protection frameworks in Africa through the Data Protection Act 2017 (DPA), in force since 15 January 2018.⁹⁸ The DPA replaced the 2004 Act and was designed to align domestic law with the EU General Data Protection Regulation (GDPR).

⁹⁶ Statistics Mauritius, Population Census 2022.

⁹⁷ World Bank, Mauritius Economic Overview (Upper-Middle-Income Classification).

⁹⁸ Data Protection Act 2017 (Mauritius), in force 15 January 2018.

A significant milestone retained from the 2024 review is Mauritius' status as the first African country to sign and ratify Convention 108+ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).⁹⁹ This international commitment reinforces the country's ambition to align with global standards and enhance cross-border data adequacy.

Positive developments retained for 2025 include:

- Continued annual reporting obligations by the Data Protection Commissioner to the National Assembly.¹⁰⁰
- Mandatory appointment of Data Protection Officers (DPOs) by controllers and processors.
- Issuance of sector-specific guidance (including financial data protection guidance).
- Ongoing public awareness and capacity-building initiatives.

However, as identified in 2024 and still relevant in 2025, several emerging issues persist:

- Limited publicly available enforcement statistics (investigations, sanctions, administrative fines).
- Insufficient transparency regarding compliance rates and audit outcomes.
- Expanding digital surveillance measures (e.g., SIM registration requirements under ICT legislation).
- Tension between constitutional privacy interpretation and broader international standards following *Madhewoo v The State of Mauritius* (2016).¹⁰¹

Thus, while Mauritius' normative framework remains strong, enforcement visibility and regulatory reporting continue to shape perceptions of institutional maturity.

Legal and Institutional Framework

The Constitution of Mauritius (1968) provides foundational protections under Sections 3 and 9, safeguarding individual liberty and protection of the home and property.¹⁰² However, the Supreme Court's decision in *Madhewoo v The State of Mauritius* (2016) adopted a narrow interpretation of constitutional privacy, limiting it primarily to the home, body, and property rather than recognising a broad, overarching right to privacy.

This interpretation remains unchanged in 2025 and continues to distinguish Mauritius' constitutional privacy framework from broader interpretations under instruments such as the ICCPR and the African Charter. Article 22 of the Mauritian Civil Code offers statutory protection of private life, though without constitutional status.¹⁰³

The primary legislation governing data protection is the Data Protection Act 2017.¹⁰⁴ The Act:

- Establishes principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, integrity, and accountability.
- Grants data subjects rights of access, rectification, erasure ("right to be forgotten"), objection, restriction, and protection against automated decision-making.
- Imposes stricter safeguards for special categories of personal data.
- Regulates cross-border data transfers.
- Mandates appointment of Data Protection Officers.
- Requires registration of data controllers and processors (valid for three years).

⁹⁹ Convention 108+ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), ratified by Mauritius, 4 September 2020.

¹⁰⁰ Data Protection Act 2017, Section 55 (Annual Report to National Assembly).

¹⁰¹ *Madhewoo v The State of Mauritius* [2016] SCJ (Supreme Court of Mauritius).

¹⁰² Constitution of Mauritius (1968), Sections 3 and 9.

¹⁰³ Mauritian Civil Code, Article 22.

¹⁰⁴ Data Protection Act 2017 (Mauritius), in force 15 January 2018.

Non-compliance may result in fines or criminal sanctions, reinforcing the Act's deterrent intent.

Complementary legislation includes the Information and Communication Technologies Act and the Cybersecurity and Cybercrime Act 2021, which strengthen digital security but may also introduce surveillance-related implications.¹⁰⁵

The central supervisory authority is the Data Protection Office, headed by the Data Protection Commissioner.¹⁰⁶ The Commissioner is empowered to:

- Register controllers and processors;
- Conduct investigations and audits;
- Issue enforcement notices;
- Seek court orders to preserve data;
- Submit annual reports to Parliament.

Supporting institutions include:

- The Ministry of Technology, Communication and Innovation (policy oversight and IT Security Unit).
- Information and Communication Technologies Authority (ICTA), responsible for licensing and oversight in telecommunications and broadcasting under the ICT Act 2002.

Compared to 2024, the institutional framework remains stable and functionally operational. The emphasis for 2025 is less on structural reform and more on demonstrating measurable regulatory outcomes.

Enforcement Dynamics and Challenges

The 2024 assessment identified enforcement transparency not legislative weakness as the principal gap in Mauritius' regime. This observation remains largely valid in 2025. Consistent with the previous review period, outreach was made to Mauritius's supervisory authority, the Data Protection Office, to obtain first-hand information on registration processes, enforcement actions, institutional capacity, public awareness efforts, and compliance monitoring.

In this instance, the Office was responsive and provided substantive input on its regulatory activities and oversight functions. This constructive engagement strengthened the reliability of the analysis and allowed for a clearer assessment of enforcement performance, operational capacity, and the overall implementation status of Mauritius's data protection framework.

The **Data Protection Office (DPO)** continues to demonstrate an active and increasingly systematised regulatory approach, combining registration oversight, complaints handling, inspections, public engagement, and international co-operation. The Office submits an annual report to the National Assembly, enhancing institutional transparency and parliamentary accountability.¹⁰⁷

Mauritius maintains a publicly accessible digital register of data controllers and processors through the DPO's online platform. The register is searchable by entity name, strengthening transparency and enabling public verification of compliance status. As of the 2024–2025 reporting period:

- **22,699 controllers** are registered
- **1,847 processors** are registered
- **7,425 controllers** require renewal
- **330 processors** require renewal

¹⁰⁵ Cybersecurity and Cybercrime Act 2021 (Mauritius); Information and Communication Technologies Act 2002.

¹⁰⁶ Data Protection Act 2017 (Mauritius), in force 15 January 2018.

¹⁰⁷ Data Protection Office of Mauritius, Annual Reports, available at: <https://dataprotection.govmu.org/Pages/Downloads/Annual-Reports.aspx>

The introduction of the “e-DPO” **integrated digital system** has significantly strengthened compliance oversight. The platform operates 24/7 and facilitates:

- Online registration and renewal (with e-payment functionality)
- Automated issuance of digitally signed certificates
- Online complaint submission
- Electronic filing of breach notifications and Data Protection Impact Assessments (DPIAs)

This digitised infrastructure enhances administrative efficiency, improves accessibility for regulated entities, and supports structured monitoring of compliance obligations.

Enforcement activity in 2024 reflects a strong concentration of complaints relating to **CCTV surveillance, unlawful disclosure of personal data and right of access**, indicating heightened public awareness around surveillance and workplace privacy.

CCTV cases accounted for a significant proportion of complaints:

- **39 closed cases** involving private premises, resolved following joint inspections with the Police. In most instances, cameras were either confined to respondents’ premises or repositioned following regulatory intervention.
- **104 ongoing cases** requiring further site inspections and technical verification, often complicated by property disputes or non-cooperation of parties.
- **4 workplace CCTV cases**, raising concerns about constant monitoring of employees. Two were closed following inspections; one remains ongoing; and one was resolved through a formal hearing convened by the Data Protection Commissioner, resulting in corrective repositioning of cameras and reinforced necessity-based placement principles.

These cases demonstrate a corrective and mediation-oriented enforcement approach, supported by police collaboration where site verification is required.

17 complaints were registered in 2024 involving unlawful disclosure:

- Unauthorized sharing of customer information by employees (6 cases)
- Disclosure of personal data to colleagues (5 cases)
- Unauthorized use of employee email accounts (2 cases)
- Misfiling and disclosure of sensitive financial records (1 case – closed following corrective measures)
- Use of biometric data (fingerprints/facial recognition) without consent (2 cases – ongoing)
- Alleged unlawful interception of private communications (1 case – ongoing, with police assistance)

Of the 17 cases:

- **3 were closed** after evidence review and remedial action
- **14 remain under investigation**

The DPO’s approach includes formal written notices referencing statutory provisions, requests for internal compliance documentation, cross-examination of safeguards, and, where necessary, on-site inspections and security audits. Biometric data cases have been treated with heightened scrutiny, with emphasis on consent and proportionality.

Right of Access Case: One complaint concerning access to CCTV footage was resolved after on-site verification confirmed that no personal data was processed or stored.

Overall, case resolution timelines vary depending on complexity, cooperation of parties, and whether police involvement is required.

Beyond reactive complaint handling, the DPO conducted **four compliance inspections** under the Data Protection Act during the reporting period. The Office prioritises sectors handling high volumes of sensitive data, particularly:

- Financial services
- Management and corporate services
- Telecommunications

This reflects a risk-based supervisory model focused on sectors with systemic data exposure.

The DPO is staffed by officers with **legal, IT, and administrative expertise**, enabling multidisciplinary investigations. However, staffing levels remain critically constrained, limiting proactive oversight and international engagement.

The Office's operating budget for FY 2024–2025 stands at **Rs 5.6 million**, which must support regulatory operations, digital infrastructure, inspections, training, and public engagement activities.

For criminal enforcement under the Data Protection Act, the DPO relies on police collaboration. The Commissioner may delegate investigative powers to police officers under statutory authority, and there is an identified need for a dedicated prosecution unit with seconded officers to streamline enforcement.

Mauritius is pursuing alignment with international standards through:

- Ongoing discussions with the **European Commission** toward EU adequacy recognition
- A draft Data Protection Bill under consideration
- Proposed regulations clarifying the role and responsibilities of Data Protection Officers
- A draft e-Privacy framework
- Proposed Freedom of Information legislation
- Consideration of constitutional amendments to reinforce digital privacy rights

This reform trajectory signals a strategic shift toward strengthening cross-border data transfer safeguards and enhancing Mauritius' global competitiveness.

The DPO maintains active participation in global and regional privacy networks, including:

- The **Global Privacy Assembly**
- The **Global Privacy Enforcement Network**
- The **Council of Europe**
- The **Organisation for Economic Co-operation and Development**
- The **African Union**
- The Francophone Association of Personal Data Protection Authorities (AFAPDP)

In October 2024, the Data Protection Commissioner was elected President of AFAPDP. In May 2025, the Commissioner was elected Chair of the African Union Data Governance Committee and Co-Chair of the Common Thread Network (CTN). These leadership roles enhance Mauritius' influence in continental and global data governance discourse.

Public awareness remains a core pillar of regulatory strategy. In 2024, the DPO:

- Conducted nationwide sensitisation campaigns on television and radio
- Organized a youth-focused workshop attended by approximately 400 students and educators
- Trained over 455 Data Protection Officers across public and private sectors
- Participated in professional forums, including engagements with the Mauritius Institute of Directors and pri-

vate-sector consultancies on AI and ethical data governance

- Delivered a Human Rights Day presentation on digital privacy for children

The e-DPO system further enhances public accessibility by enabling 24/7 complaint submission and breach reporting.

Despite operational progress, the DPO faces:

- Severe staffing shortages
- Resource limitations
- Dependence on police for criminal enforcement
- Need for enhanced prosecutorial mechanisms

A central strategic priority is achieving **EU adequacy status**, which is expected to strengthen cross-border data flows, elevate regulatory standards, and enhance Mauritius' standing as a trusted digital jurisdiction.

Overall, the **Data Protection Office** demonstrates a structured and increasingly mature oversight model, characterised by a transparent and searchable registration regime, active complaint handling supported by corrective enforcement measures, continued digitalisation of regulatory processes through the e-DPO system, issuance of sector-specific guidance, and growing leadership within regional and international data governance networks.

However, the long-term sustainability of this oversight framework will depend on strengthening staffing levels, enhancing prosecutorial support mechanisms, and increasing financial resources to match the Office's expanding regulatory mandate.

Notwithstanding these capacity constraints, Mauritius remains comparatively advanced within the region. This position is underpinned by strong statutory alignment with GDPR-inspired principles, binding international commitments including the International Covenant on Civil and Political Rights and the Convention 108+, as well as institutional continuity supported by structured Data Protection Officer Compliance obligations.

In summary, the assessment reflects continuity rather than regression. Mauritius retains its standing as a regional leader in data protection governance. Nonetheless, more detailed enforcement reporting, enhanced transparency metrics, and greater proactive regulatory disclosure would further strengthen public confidence and consolidate its international credibility.

Zimbabwe's Data Protection Regime

Context and Background

Zimbabwe has an estimated population of 16,951,171, with an annual growth rate of approximately 1.89%, accounting for about 0.205% of the global population.¹⁰⁸ Zimbabwe's digital ecosystem has expanded rapidly in recent years. As reported to Parliament in 2024 by the Portfolio Committee on ICT, Postal and Courier Services, mobile penetration reached 97.5%, internet penetration stood at 73.3%, smartphone penetration at 55%, while active mobile and internet data subscriptions were 14.7% and 10.6% respectively.¹⁰⁹

The 2024 analysis highlighted Zimbabwe's accelerating digital transformation, supported by mobile money platforms, fibre expansion, and e-government services. That trajectory continues into 2025. However, as noted in 2024, rapid digitisation has intensified the collection and processing of sensitive personal data, increasing privacy and cybersecurity risks. The constitutional right to privacy and the operationalisation of the Data Protection Act therefore remain central to Zimbabwe's digital governance agenda.

Positive Developments and Emerging Issues

The enactment of the Cyber and Data Protection Act, 2021 marked a significant milestone, providing Zimbabwe with its first comprehensive data protection regime.¹¹⁰ As retained from the 2024 assessment, the Act:

- Grants enforceable rights to data subjects (access, correction, deletion, objection);

¹⁰⁸ World Population Data Estimates, 2024.

¹⁰⁹ Report of the Portfolio Committee on ICT, Postal and Courier Services on Mobile and Internet Connectivity, Parliament of Zimbabwe (2024).

¹¹⁰ Cyber and Data Protection Act [Chapter 12:07], 2021.

- Differentiates between sensitive and non-sensitive data;
- Mandates breach notification within 24 hours;
- Establishes cross-border transfer safeguards;
- Creates whistleblowing provisions;
- Integrates cybercrime amendments into the Criminal Law (Codification and Reform) Act.

The 2022 Cyber and Data Protection Regulations further operationalised compliance through licensing, DPO appointment requirements, certification programmes, and a Code of Conduct framework.¹¹¹ Zimbabwe's hosting of the 6th Privacy Symposium Africa and ongoing DPO training initiatives (noted in 2024) remain positive indicators of awareness-building and institutional capacity development.

However, the emerging issues identified in 2024 remain largely unresolved in 2025:

- Absence of a publicly accessible register of data controllers and processors;
- Limited publication of enforcement statistics (investigations, fines, compliance rates);
- Concerns about regulatory independence due to the designation of the telecom regulator as Data Protection Authority;
- Perceived over-regulation through licensing requirements;
- Ongoing surveillance concerns linked to SIM registration and interception frameworks.

Thus, while the normative framework is now established, implementation maturity and transparency remain defining challenges.

Legal and Institutional Framework

The Constitution of Zimbabwe (2013) provides robust protection of privacy under Section 57, which guarantees protection against unlawful search, seizure, interference with communications, and disclosure of health information.¹¹² Section 62(3) further provides the right to correction or deletion of inaccurate information held by the State.¹¹³

Judicial interpretation has reinforced the breadth of this right. In *Ethel Tsitsi Mpezeni v Zimbabwe Electoral Commission*, the High Court affirmed that Section 57 extends beyond its listed clauses. Similarly, in *NetOne Cellular (Pvt) Ltd & Another v Econet Wireless (Pvt) Ltd & Another*, the Court confirmed that the right to privacy protects both natural and juristic persons from state and third-party intrusion.¹¹⁴

Compared to 2024, the constitutional framework remains stable and continues to provide a strong normative foundation. Zimbabwe is a State Party to the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right to privacy under Article 17.¹¹⁵ UN Human Rights Committee General Comment No. 16 clarifies that states must regulate the collection, storage, and processing of personal data by law and ensure rectification rights.¹¹⁶

These obligations reinforce domestic protections under Section 57 and the Cyber and Data Protection Act.

The primary legislation is the Cyber and Data Protection Act, 2021.¹¹⁷ The Act:

- Designates the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as Data Protection Authority;
- Establishes lawful processing principles (necessity, fairness, transparency, proportionality);
- Imposes explicit consent requirements for sensitive data;

¹¹¹ Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2022.

¹¹² Constitution of Zimbabwe Amendment (No. 20) Act, 2013, Section 57.

¹¹³ Constitution of Zimbabwe Amendment (No. 20) Act, 2013, Section 62(3).

¹¹⁴ *NetOne Cellular (Pvt) Ltd & Another v Econet Wireless (Pvt) Ltd & Another* (High Court of Zimbabwe).

¹¹⁵ International Covenant on Civil and Political Rights, Article 17.

¹¹⁶ UN Human Rights Committee, General Comment No. 16 (1988), Article 17 (Right to Privacy).

¹¹⁷ Cyber and Data Protection Act [Chapter 12:07], 2021.

- Requires breach notification within 24 hours;
- Regulates cross-border transfers based on adequacy;
- Provides whistleblower protection mechanisms;
- Creates offences and penalties for cybercrime and unlawful data interference.

Complementary legislation includes:

- The Access to Information and Protection of Privacy Act (AIPPA), governing personal information held by public bodies;
- The Interception of Communications Act (2007), permitting lawful interception under ministerial warrant;
- Postal and Telecommunications (Subscriber Registration) Regulations (2013, revised 2014), mandating SIM registration and establishing a Central Subscriber Information Database under POTRAZ oversight;
- The National Registration Act, regulating biometric and identity data collection.

Compared to 2024, the legal framework remains intact and operational. However, persistent concerns remain regarding proportionality in interception powers and surveillance-related data consolidation. POTRAZ functions as both telecommunications regulator and Data Protection Authority under Section 5 of the Cyber and Data Protection Act.³ Its powers include:

- Investigation and audit of controllers;
- Issuance of compliance orders;
- Licensing of data controllers and processors;
- Management of the Central Subscriber Information Database;
- Publication of guidelines and codes of conduct.

Other institutional actors include:

- The Zimbabwe Electoral Commission (ZEC), which maintains biometric voter databases;
- The Ministry of ICT, Postal and Courier Services, responsible for policy and regulatory oversight;
- Law enforcement agencies investigating cybercrime offences.

The institutional framework identified in 2024 remains unchanged. However, overlapping mandates and resource constraints continue to affect enforcement capacity.

Enforcement Dynamics and Challenges

The 2024 assessment identified enforcement transparency and regulatory independence as the most significant gaps in Zimbabwe's regime. These concerns persist in 2025. In line with the previous assessment, efforts were undertaken to engage Zimbabwe's **Postal and Telecommunications Regulatory Authority of Zimbabwe**, to obtain direct insight into registration systems, enforcement activity, institutional capacity, public outreach initiatives, and compliance monitoring under the national data protection framework.

The Authority responded positively and furnished substantive information regarding its regulatory operations and oversight mechanisms. This cooperative engagement enhanced the credibility of the present analysis and enabled a more informed evaluation of enforcement trends, operational effectiveness, and the overall state of implementation of Zimbabwe's data protection regime.

Since assuming the mandate, POTRAZ has progressively operationalised licensing, complaint handling, sectoral guidance, and supervisory oversight mechanisms, reflecting a maturing regulatory environment. POTRAZ maintains a publicly accessible register of licensed data controllers and processors, available through its official website under the Data Protection section. In addition, the Authority publishes lists of licensed controllers in local media, enhancing transparency and public visibility of regulated entities.

As of October 2025:

- **721 licensed data controllers**
- No inactive controllers, as all licences issued remain valid initial applications
- Licence renewals are scheduled to commence in March 2026

This indicates that Zimbabwe remains in the early licensing cycle of its data protection framework, with compliance monitoring currently focused on onboarding and ecosystem formalisation rather than renewals or sanctions for lapse.

The promulgation of the **Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, S.I. 155 of 2024**, marked an important operational milestone, providing detailed procedures for controller licensing and mandatory DPO appointments.

Under Section 6 of the Cyber and Data Protection Act, data subjects have a statutory right to lodge complaints with the Authority. POTRAZ is mandated to receive, investigate, and resolve such complaints, working in collaboration with the Zimbabwe Republic Police and other sectoral regulators where necessary. To date, the Authority has received **20 formal complaints**:

- 15 investigated and resolved
- 3 under active investigation
- 2 dismissed due to jurisdictional limitations

The average complaint resolution timeframe is approximately **30 working days**, depending on case complexity.

POTRAZ has issued **11 compliance guidance notices and findings**, primarily relating to:

- Cross-border data transfers
- Personal data breaches

Enforcement remains largely corrective and advisory in nature, reflecting both the developmental stage of the regulatory regime and the absence of administrative fines within the Act.

Currently, sanctions are limited to criminal penalties (fines or imprisonment), which may reduce deterrence in certain non-compliance scenarios.

No landmark enforcement case has yet emerged, largely because implementation of the Cyber and Data Protection Act is still consolidating within the national legal system.

In 2025, POTRAZ conducted **20 proactive compliance audits**, focusing on high-risk sectors including: Financial services, Health and ICT. These audits reviewed Data Protection Impact Assessments (DPIAs), internal gap analyses, and safeguards governing cross-border data transfers. The Authority applies a risk-based monitoring model, prioritising sectors that process sensitive personal data, particularly health, education, and fintech.

The Data Protection Unit (DPU) within POTRAZ comprises **14 dedicated officials**, including legal experts, cybersecurity analysts, and compliance officers. Staff undergo continuous professional development in digital forensics, AI governance, privacy impact assessments, and international data governance standards. The Authority plans to double its data protection personnel by 2027.

Technically, the DPU operates a Computer Incident Response Team (CIRT) Laboratory equipped with:

- Automated risk assessment tools
- Forensic audit software
- Threat intelligence systems
- A Digital Financial Services monitoring system

The Authority is preparing to launch an **E-Licensing System** to streamline controller registration and compliance management.

For 2025, data protection activities are funded internally by POTRAZ, with budget allocation structured as follows:

- ✓ 60% – Public engagement and awareness
- ✓ 20% – Enforcement and compliance
- ✓ 20% – Capacity building and international cooperation

This allocation underscores a strategic emphasis on ecosystem development and awareness-building during the early phase of implementation.

To facilitate compliance, POTRAZ has issued six (6) implementation guidelines to date:

1. Cross-Border Data Transfers
2. Processing of Children's Personal Data
3. Data Breach Notification and Handling
4. Licensing and Registration of Data Controllers
5. Right to Consent
6. Appointment, Designation and Certification of Data Protection Officers

Seven (7) additional draft guidelines are undergoing public consultation and are expected to be finalised before the end of 2025. This consultative and sector-specific guidance model enhances regulatory clarity and supports gradual institutionalisation of compliance standards across industries.

No legislative amendments were made during the review period.

Public awareness and professional capacity development form a central pillar of POTRAZ's oversight strategy. Since 2023, the Authority has conducted **over 50 awareness campaigns** nationwide, covering:

- ✓ Schools and universities
- ✓ Senior citizens
- ✓ Rural communities
- ✓ Radio programmes
- ✓ Workshops for data controllers and data subjects

Through collaboration with the Harare Institute of Technology, POTRAZ established a specialised Data Protection Officer training programme, the first of its kind in the SADC region. To date:

- **829 DPOs trained**, with a target of 1,000 by end of 2025
- Participation from Malawi, Eswatini, and Zambia

The Authority has also trained boards and executive leadership of **37 data controllers** across health, education, banking, regulatory, and mining sectors.

Complaints and public queries can be submitted via email, regulatory portals, or in person. The Authority commits to responding within 14 days of receipt.

POTRAZ actively participates in regional and international privacy networks, including:

- Network of African Data Protection Authorities (NADPA-RAPDP)
- Africa CIRT and SADC CIRT

- Global Privacy Assembly
- AU Data Policy Framework initiatives
- SADC Cybersecurity and Data Protection Programme

The Authority has signed a Memorandum of Understanding with the Information Regulator of South Africa to strengthen cross-border regulatory cooperation.

Its DPO training programme received regional endorsement at a SADC forum in Madagascar in September 2025, reflecting growing regional leadership.

Despite progress, POTRAZ faces notable challenges:

- Slow uptake of licensing among data controllers due to ecosystem immaturity
- Absence of administrative fines within the Cyber and Data Protection Act
- Continued need for deterrent enforcement tools

Strategic priorities for 2026–2027 include:

- Launch of an E-Licensing system
- Launch of an online DPO training platform
- Expansion of cross-border enforcement cooperation
- Strengthened collaboration with national and international regulators

Overall, Zimbabwe's data protection regime is evolving from its foundational legislative phase into a more structured implementation and operational stage. The Postal and Telecommunications Regulatory Authority of Zimbabwe has strengthened regulatory clarity through licensing, proactive audits, issuance of sector-specific guidelines, and sustained capacity-building initiatives, while awareness campaigns and DPO certification programmes have contributed to growing compliance culture among businesses and public institutions.

The core legal framework established in 2021–2022 remains intact and functional, reflecting a solid constitutional and statutory architecture. However, enforcement continues to be largely compliance-oriented rather than punitive, and the absence of administrative fines may constrain deterrence. Greater enforcement transparency, clearer reporting of compliance outcomes, and continued institutional strengthening will be essential to consolidating public trust and advancing regulatory maturity.

If planned reforms including digital licensing systems, expanded staffing, and enhanced regional cooperation are implemented as projected, Zimbabwe's oversight capacity is likely to strengthen significantly over the next regulatory cycle, enabling the framework to move from normative robustness toward demonstrable enforcement effectiveness.

Kenya's Data Protection Regime

Context and Background

Kenya remains one of Africa's most advanced digital economies, with rapid expansion in mobile money, e-commerce, digital lending, telecommunications, and e-government services. Platforms such as **Safaricom** (through M-Pesa) continue to process transactions equivalent to over half of national GDP, embedding personal data processing into everyday economic activity.¹¹⁸ This digital acceleration has deepened since 2024, reinforcing Kenya's position as a regional technology hub while simultaneously increasing exposure to data protection risks.

The legal foundation of this ecosystem remains Article 31 of the Constitution of Kenya (2010), which guarantees the right to privacy, and the **Data Protection Act**, enacted in 2019 and operational since 2020.¹¹⁹ As noted in the 2024 analysis, Kenya has established a comprehensive statutory regime aligned with global standards, particularly the **General Data Protection Regulation** (GDPR).¹²⁰

¹¹⁸ Central Bank of Kenya, National Payment System statistics (2024).

¹¹⁹ Data Protection Act, No. 24 of 2019 (Kenya).

¹²⁰ European Union, General Data Protection Regulation (Regulation (EU) 2016/679).

Compared to 2024, the 2025 position reflects consolidation rather than structural reform. The legal framework remains intact and largely stable, but the scale and sophistication of digital services particularly in AI systems, biometric identification (e.g., the Maisha Namba programme), and platform-based services have expanded, increasing regulatory pressure on existing safeguards.

Positive Developments and Emerging Issues

In contrast to the 2024 assessment where enforcement transparency and institutional responsiveness were flagged as concerns, 2025 reflects measurable maturation of regulatory practice. The **Office of the Data Protection Commissioner (ODPC)**¹²¹ has:

- Issued 34 determinations in 2024, with monetary penalties and compensation awards.¹²²
- Expanded regional presence beyond Nairobi, improving geographic access.
- Continued maintaining a public register of data controllers and processors, reinforcing transparency.¹²³

Enforcement has become more substantive, with financial penalties imposed across sectors including education, financial services, and digital platforms. This marks a progression from the 2024 observation of limited publicly structured enforcement reporting.

Internationally, Kenya has advanced adequacy discussions with the European Union, strengthening its global positioning and signaling regulatory credibility.

However, 2025 also reveals persistent and emerging governance tensions:

- **AI governance gaps** following the launch of the National AI Strategy,¹²⁴ with safeguards lagging deployment speed.
- Expansion of biometric and digital ID systems raising surveillance and proportionality concerns.
- Proposed social media identity verification measures that may undermine anonymity and freedom of expression.
- Continued privacy risks in digital lending and high-volume mobile financial services.

While Kenya retains regional leadership in data protection, these developments suggest that innovation continues to outpace regulatory adaptation an issue already flagged in 2024 but now more pronounced.

Legal and Institutional Framework

Kenya's data protection regime remains anchored in constitutional privacy guarantees¹²⁵ and the statutory framework established by the Data Protection Act.¹²⁶ The Act operationalises principles of lawful processing, transparency, accountability, and data subject rights consistent with international standards such as the GDPR.¹²⁷

Supporting legislation includes:

- The *Access to Information Act*, which advances transparency while requiring careful balancing with privacy protections.¹²⁸
- The *Computer Misuse and Cybercrimes Act*, addressing cyber-related offences affecting personal data security.¹²⁹
- The *Kenya Information and Communications Act*, regulating telecommunications privacy and interception safeguards.¹³⁰

¹²¹ Data Protection Act, No. 24 of 2019 (Kenya).

¹²² Office of the Data Protection Commissioner (Kenya), Enforcement Determinations and Public Decisions (2024).

¹²³ Data Protection Act, No. 24 of 2019 (Kenya).

¹²⁴ Kenya National AI Strategy (2025).

¹²⁵ Constitution of Kenya (2010), Articles 31 and 35.

¹²⁶ Data Protection Act, No. 24 of 2019 (Kenya).

¹²⁷ European Union, General Data Protection Regulation (Regulation (EU) 2016/679).

¹²⁸ Access to Information Act, No. 31 of 2016 (Kenya).

¹²⁹ Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Kenya).

¹³⁰ Kenya Information and Communications Act, Cap 411A (Kenya).

Institutionally, the ODPC operates as the designated supervisory authority under the Data Protection Act.¹³¹ As highlighted in the 2024 analysis, concerns regarding financial and operational autonomy remain relevant, given continued budgetary dependence within the executive structure. While enforcement visibility has improved since 2024, structural independence has not materially changed.

Enforcement Dynamics and Challenges

The 2024 assessment identified limited regulator engagement and incomplete visibility into enforcement patterns. During this review cycle, outreach was again directed to Kenya's **Office of the Data Protection Commissioner**, with the aim of obtaining updated and detailed information on registration statistics, enforcement activity, institutional capacity, public awareness initiatives, and compliance oversight.

While contact was initiated, the process did not yield substantive data or comprehensive updates on supervisory trends and enforcement outcomes. As a result, the analysis relies primarily on publicly available information, which constrains the depth of assessment regarding enforcement performance, regulatory priorities, and overall implementation progress within Kenya's data protection framework.

By 2025, enforcement has become more demonstrable and financially consequential.¹³² Administrative fines and compensation awards now create clearer deterrent effects, particularly in high-risk sectors. This reflects a shift from awareness-building and registration-focused oversight in the early years of implementation¹³³ to more assertive corrective enforcement under the 2021 Regulations.¹³⁴

Despite progress, structural challenges remain:

1. **Resource Constraints:** Staffing and funding remain limited relative to the scale of Kenya's digital economy.¹³⁵
2. **Reactive Compliance Patterns:** Enforcement appears largely complaint-driven rather than proactively systemic.¹³⁶
3. **Public Sector Gaps:** Concerns regarding surveillance, interception, and communications privacy persist under broader sectoral legislation.¹³⁷
4. **Regulatory Clarity:** Cross-border transfers, AI governance, and algorithmic processing require further interpretive guidance under the existing statutory framework.¹³⁸

Overall, Kenya retains regional leadership in privacy governance as of 2025. However, the status quo reflects incremental institutional strengthening rather than structural reform. Sustained investment in regulatory autonomy, clearer guidance on emerging technologies, and enhanced transparency in enforcement reporting will be essential to consolidate gains achieved since the 2024 analysis.

Uganda's Data Protection Regime

Context and Background

As of March 2025, Uganda had approximately 14.2 million internet users, representing 28% of the population,¹³⁹ marking a modest increase from 13.3 million (27%) in early 2024.¹⁴⁰ Digital services continue to expand, particularly in fintech and e-commerce, with the digital economy projected to reach US\$2.5 billion in 2025, up from US\$1 billion in 2022.¹⁴¹ Mobile money platforms now support over 27 million active accounts, reinforcing digital financial inclusion.¹⁴²

Government digitisation has also advanced, with an estimated 62% of public services accessible online through integrated systems such as the Parish Development Management Information System (PDMIS) and the Integrated Health Management Information System (IHMIS).¹⁴³ However, rural–urban disparities in broadband infrastructure and digital

¹³¹ Data Protection Act, No. 24 of 2019 (Kenya).

¹³² Office of the Data Protection Commissioner (Kenya), Enforcement Determinations and Public Decisions (2024).

¹³³ Data Protection Act, No. 24 of 2019 (Kenya).

¹³⁴ Data Protection (General) Regulations, 2021 (Kenya).

¹³⁵ Data Protection Act, No. 24 of 2019 (Kenya).

¹³⁶ Office of the Data Protection Commissioner (Kenya), Enforcement Determinations and Public Decisions (2024).

¹³⁷ Kenya Information and Communications Act, Cap 411A (Kenya).

¹³⁸ Data Protection Act, No. 24 of 2019 (Kenya).

¹³⁹ National ICT statistics and market projections (2024–2025).

¹⁴⁰ National ICT statistics and market projections (2024–2025).

¹⁴¹ National ICT statistics and market projections (2024–2025).

¹⁴² National ICT statistics and market projections (2024–2025).

¹⁴³ National ICT statistics and market projections (2024–2025).

literacy continue to limit equitable access. Compared to the 2024 analysis, which cited a 43% internet penetration rate,¹⁴⁴ the 2025 figures suggest recalibrated measurement methodologies or updated population baselines rather than regression. What remains consistent across both assessments is Uganda's expanding digital ecosystem alongside low public awareness of privacy rights and limited access to enforcement mechanisms.¹⁴⁵

Positive Developments and Emerging Issues

Uganda retains a progressive statutory framework anchored in Article 27 of the Constitution,¹⁴⁶ which guarantees the right to privacy. The **Data Protection and Privacy Act (DPPA)** operationalises this right through principles of lawful, fair, and secure data processing, including prior consent requirements under Section 7(1).¹⁴⁷

The **Personal Data Protection Office (PDPO)** has demonstrated increased assertiveness since 2024. Notably, in 2025 it directed **Google** to register as a data controller and collector within 30 days, finding violations relating to registration and cross-border transfers under Section 19 of the DPPA and Regulation 30.¹⁴⁸ This decision represents a significant precedent in applying Uganda's data protection law extraterritorially and signals greater regulatory confidence compared to 2024.

Public awareness initiatives launched in 2023 under the "Stop, Think, Own Your Privacy" campaign remain relevant and form part of ongoing efforts to strengthen digital literacy.¹⁴⁹ Judicial engagement also continues, particularly regarding biometric data oversight linked to the National Identification Registration Authority (NIRA).

Despite progress, implementation gaps persist:

- Limited clarity regarding mechanisms for withdrawal of consent under the DPPA.¹⁵⁰
- Continued surveillance concerns under the Regulation of Interception of Communications Act.¹⁵¹
- Expanding digital ID and biometric systems under the Registration of Persons Act, raising proportionality and oversight concerns.¹⁵²
- Capacity limitations affecting proactive audits and risk-based oversight.¹⁵³

Compared to 2024, enforcement visibility has improved (notably through the Google determination), but systemic constraints remain largely unchanged.

Legal and Institutional Framework

Uganda's data protection regime is grounded in the Constitution¹⁵⁴ and principally governed by the **Data Protection and Privacy Act**.¹⁵⁵ The Act is implemented through the Data Protection and Privacy Regulations, 2021, which establish procedures for complaints, objections, and breach notification.¹⁵⁶

The DPPA applies extraterritorially, extending obligations to foreign entities processing Ugandan data subjects' information.¹⁵⁷ This approach aligns with international human rights standards, including the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights, to which Uganda subscribes.¹⁵⁸

144 2024 Privacy Scorecard Analysis – Uganda.

145 2024 Privacy Scorecard Analysis – Uganda.

146 Constitution of the Republic of Uganda, 1995, Article 27.

147 Data Protection and Privacy Act, 2019 (Uganda).

148 Data Protection and Privacy Act, 2019 (Uganda). Data Protection and Privacy Regulations, 2021 (Uganda).

149 2024 Privacy Scorecard Analysis – Uganda.

150 Data Protection and Privacy Act, 2019 (Uganda).

151 Regulation of Interception of Communications Act, 2010 (Uganda).

152 Registration of Persons Act, 2015 (Uganda).

153 2024 Privacy Scorecard Analysis – Uganda.

154 Constitution of the Republic of Uganda, 1995, Article 27.

155 Data Protection and Privacy Act, 2019 (Uganda).

156 Data Protection and Privacy Regulations, 2021 (Uganda).

157 Data Protection and Privacy Act, 2019 (Uganda).

158 International Covenant on Civil and Political Rights (1966); Universal Declaration of Human Rights (1948).

Supporting legislation includes:

- ✓ The Access to Information Act, governing public data disclosure.¹⁵⁹
- ✓ The Computer Misuse Act, addressing cyber offences and unlawful access.¹⁶⁰
- ✓ The Electronic Transactions Act, supporting secure digital transactions.¹⁶¹

Institutionally, oversight rests with the National Information Technology Authority - Uganda (NITA-U), established under the NITA-U Act, 2009, with the PDPO functioning as a semi-autonomous office within it.¹⁶²

As noted in 2024, concerns regarding regulatory independence remain.¹⁶³ The PDPO's structural placement within NITA-U continues to raise questions about autonomy and political insulation. While enforcement activity has become more visible in 2025, institutional architecture has not materially changed.

Enforcement Dynamics and Challenges

The 2024 assessment highlighted weak enforcement mechanisms, limited regulator engagement, and resource constraints.¹⁶⁴ In the current assessment period, efforts were made to engage Uganda's **Personal Data Protection Office**, to obtain updated and detailed information concerning registration data, enforcement actions, institutional capacity, public awareness initiatives, and ongoing compliance monitoring.

Although contact was established, the engagement did not result in the provision of comprehensive or updated supervisory data. Consequently, this analysis is primarily based on publicly available sources, which limits the extent to which enforcement effectiveness, regulatory priorities, and the overall status of implementation under Uganda's data protection framework can be fully evaluated.

By 2025, the PDPO's determination against Google demonstrates increased willingness to confront large multinational platforms and enforce cross-border transfer provisions.¹⁶⁵

Earlier precedents, such as the SafeBoda investigation (2023), remain important benchmarks for domestic enforcement and continue to inform regulatory practice.¹⁶⁶

However, several systemic challenges endure:

1. *Regulatory Independence*: The PDPO remains embedded within NITA-U, limiting perceived autonomy.¹⁶⁷
2. *Resource Constraints*: Financial and human capacity limitations continue to hinder proactive oversight.¹⁶⁸
3. *Limited Public Awareness*: Citizens' understanding of complaint procedures and rights remains low.¹⁶⁹
4. *Consent Ambiguities*: Withdrawal procedures remain insufficiently clarified in statute or regulatory guidance.¹⁷⁰
5. *Surveillance and Biometric Risks*: Expansion of digital ID systems and interception laws continues to generate human rights concerns.¹⁷¹

Overall, Uganda's 2025 position reflects incremental enforcement strengthening within an unchanged institutional structure. The legal framework remains robust on paper consistent with the 2024 assessment but effective protection continues to depend on enhanced independence, resource allocation, clearer regulatory guidance, and expanded public engagement.

¹⁵⁹ Access to Information Act, 2005 (Uganda).

¹⁶⁰ Computer Misuse Act, 2011 (Uganda).

¹⁶¹ Electronic Transactions Act, 2011 (Uganda).

¹⁶² National Information Technology Authority – Uganda Act, 2009.

¹⁶³ 2024 Privacy Scorecard Analysis – Uganda.

¹⁶⁴ 2024 Privacy Scorecard Analysis – Uganda.

¹⁶⁵ Data Protection and Privacy Act, 2019 (Uganda). Data Protection and Privacy Regulations, 2021 (Uganda).

¹⁶⁶ 2024 Privacy Scorecard Analysis – Uganda.

¹⁶⁷ National Information Technology Authority – Uganda Act, 2009.

¹⁶⁸ 2024 Privacy Scorecard Analysis – Uganda.

¹⁶⁹ 2024 Privacy Scorecard Analysis – Uganda.

¹⁷⁰ Data Protection and Privacy Act, 2019 (Uganda).

¹⁷¹ Regulation of Interception of Communications Act, 2010 (Uganda). Registration of Persons Act, 2015 (Uganda).

5. Insights into Challenges, Lessons Learned, And Best Practices

Data protection regimes across Africa and the globe are evolving rapidly, yet experience shows that adoption of modern frameworks does not automatically translate into effective privacy governance. Across the continent, a recurring pattern emerges: while many countries have enacted rights-based laws often inspired by international standards such as the GDPR or regional instruments like the AU's Malabo Convention, implementation remains uneven, and compliance across sectors is frequently limited. Structural gaps, limited regulatory capacity, and low public awareness often undermine the intended protections.

At the same time, a growing body of practical experience highlights what works. Lessons drawn from organisational assessments, sectoral studies, regional harmonisation initiatives, and international regulatory models reveal recurring principles that strengthen compliance, enhance accountability, and support responsible digital innovation. Specific country experiences provide illustrative examples, yet the focus is on the underlying strategies that consistently yield results: strong institutional independence targeted capacity-building, user-centred oversight, multi-stakeholder collaboration, and integration of privacy into technological and business processes from the outset.

This chapter synthesises these insights, offering a roadmap for policymakers, regulators, industry actors, and civil society to navigate persistent challenges while building resilient, transparent, and adaptive data protection ecosystems capable of meeting the demands of a rapidly digitalising society.

5.1 Insights into Challenges

1. Uneven Compliance Across Sectors

Across African jurisdictions, compliance rates remain particularly low in sectors such as health, e-commerce, and certain government services, even where stronger performance is observed in finance and insurance. This unevenness reveals not only gaps in sectoral readiness but also the inadequacy of one-size-fits-all compliance strategies. As seen in several countries, when organizations do not register with national data protection authorities or fail to implement basic transparency requirements, it reflects systemic weaknesses in regulatory outreach, sector-specific guidance, and incentives for compliance. Regulatory regimes must therefore tailor their approaches to the maturity and risk profiles of different sectors, rather than assuming that general rules will yield uniform compliance outcomes.

2. Enforcement Deficits and Limited Institutional Capacity

Many DPAs operate with restricted budgets, insufficient staffing, and limited technical infrastructure, which weakens their ability to conduct proactive monitoring or impose meaningful sanctions. Some jurisdictions illustrate how appointment processes subject to executive influence can also compromise perceived independence, reducing public trust and deterring whistleblowing. These factors jointly demonstrate that even strong legal frameworks cannot succeed without autonomous, well-resourced institutions. Investment therefore, in institutional capacity i.e. financial, technical, and organizational, is a prerequisite for credible enforcement and for deterring violations that would otherwise persist unchecked.

3. Transparency Gaps and Weak Accountability Traditions

A significant number of organizations fail to publish clear privacy notices, detailed data-handling procedures, or transparency reports, leaving data subjects without meaningful insight into how their information is used. This opacity is compounded in countries lacking comprehensive access-to-information laws, where individuals struggle to exercise rights such as access or rectification. The pattern across jurisdictions shows that when transparency obligations remain superficial or technically inaccessible, broader accountability norms fail to take root. To that end, transparency mechanisms must be treated not merely as compliance items but as foundational tools for building institutional trustworthiness and enabling active citizen oversight.

4. Inadequate Operational and Technical Safeguards

While many organizations have adopted baseline protections like SSL encryption, numerous internal processes like breach notification pathways, data retention schedules, third-party data sharing controls, etc remain poorly defined or entirely absent. Countries where record-management systems are outdated illustrate how technical weaknesses can undermine compliance even with advanced legal frameworks. This highlights a broader lesson: effective data protection depends equally on operational maturity and technological reliability. Without investment in internal procedures, secure infrastructure, and continuous improvement, compliance remains superficial and exposes organizations to heightened breach risks.

5. Low Levels of Awareness and Limited Capacity Building

In many jurisdictions, frontline staff, public officials, and ordinary citizens remain unfamiliar with data protection rights and obligations. Studies from revenue and tax authorities in some countries show that ignorance of legal requirements directly contributes to unintentional violations. The broader implication is that legal compliance cannot be sustained without consistent education efforts and organizational cultures that prioritize privacy. Weak awareness not only facilitates violations but also reduces public pressure on institutions to adhere to the law, creating a cycle of complacency that undermines regulatory progress.

6. Biometric Data Vulnerabilities

The rapid expansion of biometric systems in national IDs, SIM registration, e-passports, and banking authentication has outpaced the development of safeguards. Real-world examples show how unclear consent mechanisms and exposure of sensitive data to frontline staff heighten risks of misuse. The lesson here is that biometrics require more stringent governance than generalized data protection frameworks often provide, owing to their permanence, sensitivity, and potential for surveillance. Strengthening oversight in this domain is essential not only to prevent abuse but also to preserve public trust in digital identity systems that are becoming central to national development strategies.

7. Tensions Between Surveillance Mandates and Privacy Protection

Legacy security laws in several countries grant broad surveillance powers that supersede newer data protection provisions. Instances where data collected for security functions is repurposed for political or administrative monitoring demonstrate how weak legal harmonization undermines fundamental rights. These experiences show that privacy rights cannot flourish where parallel legislation gives unchecked discretion to state agencies. The implication is that data protection regimes must be embedded within a broader constitutional and legislative ecosystem that imposes judicial oversight, defines proportionality, and limits executive power.

8. Unclear Criteria for Cross-Border Data Transfers

Many jurisdictions restrict international data transfers to countries with “adequate safeguards,” yet fail to define adequacy criteria or set transparent assessment procedures. This creates ambiguity for organizations and exposes both regulators and companies to inconsistent decision-making. The broader lesson is that clarity in cross-border governance is indispensable for business continuity, digital trade, and protection of data subjects. Countries seeking to expand their digital economies must establish predictable and transparent adequacy and transfer mechanisms to avoid regulatory bottlenecks and arbitrary enforcement.

9. Systemic Technical Barriers to Policy Accessibility

In some digital ecosystems, technical barriers like broken links, malfunctioning websites, inaccessible documents, make privacy policies difficult or impossible for users to access. This problem extends beyond mere inconvenience; it reflects systemic issues in digital infrastructure and undermines a core principle of transparency. The implication is that accessibility must be recognized as an essential component of compliance. Without reliable, user-friendly communication channels, legal rights remain theoretical and organizational accountability deteriorates.

10. Policy Localization Gaps and Overreliance on Generic Templates

Numerous organizations, including multinational firms, rely on generic global templates that omit references to national law, local contact mechanisms, and context-specific processing activities. Country experiences demonstrate that such policies fail to meet legal standards and obscure real data flows. This reflects a broader challenge: privacy governance cannot be meaningfully outsourced or standardized across jurisdictions without careful customization. To avoid superficial compliance, organizations must invest in locally grounded, operationally accurate privacy documentation that reflects actual practices.

11. Fragmented Multi-Agency Regulation and Coordination Challenges

Where multiple authorities hold overlapping mandates such as telecommunications regulators, cyber agencies, central banks, digital innovation boards, organizations often receive inconsistent instructions. In some contexts, this has led to regulatory gaps where no authority takes ownership of critical data protection issues. These experiences reveal that fragmentation threatens both compliance and enforcement, underscoring the need for harmonized standards and co-ordinated oversight mechanisms. Effective data governance ultimately depends on institutional coherence, not merely statutory mandates.

12. Technological Innovation Outpacing Regulatory Frameworks

Artificial intelligence, IoT ecosystems, algorithmic profiling, and blockchain services are expanding faster than DPAs can adapt. In several countries, national AI strategies and digital identity rollouts lack comprehensive privacy safeguards, exposing individuals to risks and regulators to capacity gaps. The implication is that data protection must evolve alongside innovation, not after it. Regulators require new technical skills, agile rule-making processes, and precautionary frameworks particularly, around automated decision-making to govern emerging technologies effectively.

13. Rights Enforcement Gaps and Persistent Opacity in Third-Party Sharing

Across jurisdictions, organizations often fail to articulate data-sharing practices or provide clear mechanisms for exercising user rights. Even when laws require breach notifications or the publication of transparency reports, compliance rates remain low. This pattern illustrates how transparency and user rights can erode when regulators lack capacity to monitor or compel disclosures. The broader implication is that rights-based frameworks depend heavily on active enforcement and public-facing accountability. Without rigorous reporting standards and user empowerment measures, data protection regimes risk becoming symbolic rather than functional.

5.2 Insights into Lessons learned, and Best Practices

A. Best Practices and Lessons Emerging from Organisational Assessments

▪ Comprehensive and Accessible Privacy Policies Build User Trust

Clear, well-structured, and easily accessible privacy policies consistently strengthen transparency and consumer confidence. The principle is demonstrated by organisations in several African markets such as leading telecom operators and financial institutions, which maintain detailed disclosures on data collection, lawful bases, user rights, and third-party transfers. Their example illustrates a broader lesson: meaningful transparency is a foundational element of trust, compliance, and ethical data governance.

▪ Strong Security Controls, Including SSL, Are Foundational to Compliance

Across sectors, entities that pair SSL encryption with explicit statements on technical and organisational safeguards tend to exhibit stronger overall data protection maturity. The broader principle is that robust baseline security like encryption standards, access controls, and secure development practices, is not optional but a prerequisite for lawful and responsible processing. Countries and sectors that have emphasised secure-by-default standards show measurably better outcomes in breach prevention and incident containment.

▪ Active Registration and Regulatory Visibility Promote Accountability

Organisations that maintain active registration with national data protection authorities typically exhibit better governance practices and clearer documentation. The pattern illustrates a core principle: regulatory visibility fosters accountability. Where regulators require up-to-date filings and periodic renewals, organisations are more likely to internalise compliance obligations and invest in sustainable privacy programmes.

▪ Defined and Documented Breach Response Mechanisms Improve Resilience

Entities that articulate internal breach procedures including detection pathways, reporting channels, and user notification protocols, set the benchmark for effective risk management. This reflects a broader truth: data breach readiness must be operationalised, not implied. Countries where organisations implement detailed response playbooks demonstrate faster containment, clearer communications, and reduced harm to affected individuals.

▪ Sectoral Leaders Serve as Models for Broader Governance Maturity

Financial services, telecommunications, and certain digital lending companies frequently demonstrate more advanced practices, reflecting a combination of higher regulatory expectations and stronger internal governance cultures. These

sectors illustrate the principle that robust compliance ecosystems emerge when clear standards, supervisory pressure, and industry-driven initiatives align. Their progress provides templates that other sectors can adapt.

B. International Best Practices and Adaptable Governance Lessons

▪ Drawing from Global and Regional Leadership Examples

Countries developing or strengthening their data protection regimes benefit significantly from analysing global experience and adapting successful approaches in line with local realities.

- **The EU's GDPR framework** highlights the value of comprehensive rights protections, risk-based obligations, and strong enforcement powers. However, developing economies must tailor these concepts to domestic institutional capacities, market structures, and cultural contexts rather than replicate them wholesale.
- **South Africa's POPIA experience** offers particularly relevant lessons for balancing privacy with economic development. Its multi-stakeholder consultations, sectoral guidance, and capacity-building initiatives exemplify how resource-constrained jurisdictions can build resilient regulatory ecosystems.
- **Singapore's pragmatic approach** emphasising targeted regulation, industry collaboration, and innovation-friendly compliance tools, illustrates how smaller economies can support technological growth while maintaining strong privacy safeguards.
- **African Union and sub-regional harmonisation efforts** show how cooperation enables shared learning, consistent standards, and coordinated responses to cross-border challenges. Such platforms create opportunities for mutual support, regulatory peer review, and collective capacity building.

C. Sectoral Engagement and Collaborative Governance Models

▪ Broad Stakeholder Coalitions Strengthen Privacy Outcomes

Experience across multiple jurisdictions shows that privacy protection is most effective when regulators work alongside industry, civil society, academia, and international partners. Regulatory enforcement alone cannot drive systemic compliance; a culture of privacy requires societal participation.

▪ Industry Associations as Vehicles for Sector-Specific Capacity Building

Sectors with strong self-regulatory traditions like banking and telecommunications, often demonstrate higher compliance maturity. Their associations facilitate shared learning, harmonised best practices, and cost-effective training initiatives. This illustrates the broader principle that industry cooperation complements public oversight.

▪ Civil Society as a Critical Accountability and Public Awareness Actor

Civil society groups enhance transparency, public education, and independent monitoring. In several countries, they have documented violations, pursued strategic litigation, and advocated for reform. This demonstrates that civil society engagement is indispensable for strengthening rights enforcement and democratic oversight.

▪ Academic Institutions as Engines of Research and Long-Term Capacity

Universities and research bodies support regulatory and industry maturity through training, empirical studies, and policy analysis. Their role is critical for cultivating the next generation of privacy professionals and embedding privacy in national digital development strategies.

D. Public-Private Partnership Models and Co-Regulation

▪ Constructive Government-Industry Collaboration Enhances Compliance

Experience shows that organisations treating privacy as a business enabler rather than merely a regulatory burden, achieve stronger compliance and innovation outcomes. Co-regulatory models foster shared responsibility without compromising regulatory independence.

▪ Technology Partnerships Support Oversight and Build Capacity

Carefully structured collaborations between regulators and technology providers enhance supervisory capabilities (e.g., automated compliance monitoring, data-flow mapping tools). Such partnerships must be governed by clear safeguards to preserve independence.

- **International Partnerships Expand Expertise and Promote Convergence**

Cross-border regulatory cooperation provides access to technical resources, training, and best practices that no single country can develop alone. These partnerships facilitate mutual learning and alignment with global standards.

- **Multi-Stakeholder Governance Mechanisms Address Complex Challenges**

Initiatives that bring together government, industry, academia, and civil society can resolve nuanced issues such as AI fairness, biometric governance, and cross-border transfers. Their effectiveness depends on meaningful participation, transparent processes, and measurable outcomes.

E. Privacy-by-Design, Innovation, and Technology Governance

- **Embedding Privacy into System and Product Design Improves Outcomes**

Organisations that integrate privacy by design at the outset, not after deployment show stronger compliance, improved operational efficiency, and greater user trust. This underscores the principle that privacy must be an architectural requirement, not a retrofit.

- **Privacy-Enhancing Technologies (PETs) Provide Sustainable Advantages**

Techniques such as encryption-at-rest, differential privacy, and secure computation strengthen protection while supporting innovation. Their adoption requires investment and expertise but yields long-term resilience and competitive benefit.

- **Aligning Business Models with Privacy Protection Ensures Sustainability**

Firms that identify commercial value in privacy through trusted services, secure digital products, ethical data monetization, demonstrate deeper, more durable compliance cultures than those driven solely by regulatory pressure.

- **Regulatory Innovation Encourages Responsible experimentation**

Models such as regulatory sandboxes, safe-harbour mechanisms, and tiered compliance obligations allow controlled testing of new technologies (e.g., fintech or AI) while safeguarding rights. These approaches show how oversight can be adaptive rather than restrictive.

F. Regional Regulatory Cooperation and Harmonisation Lessons

- **Strengthening Independence and Institutional Autonomy**

Some African jurisdictions have improved regulatory credibility by establishing independent data protection authorities with secured funding and transparent appointment processes. These reforms demonstrate how independence enhances enforcement effectiveness and reduces political interference risks.

- **Integrating Constitutional Rights with Statutory Privacy Frameworks**

Countries that embed privacy rights in constitutional structures supported by active judicial oversight, create strong foundations for enforcement. Strategic litigation in such jurisdictions shows how courts can reinforce accountability even against state actors.

- **Leveraging Regional Harmonisation for Capacity Building and Coherent Standards**

Regional initiatives such as those under the EAC, ECOWAS, and the African Union provide opportunities for shared expertise, aligned regulations, and coordinated enforcement against cross-border violations. Countries serving as regional leaders illustrate how cooperative frameworks can generate economies of scale and strengthen digital market integration.

G. Enforcement Strategy Development and Penalty Calibration

- **Graduated Enforcement Models Maximise Compliance Impact**

International practice shows that blended approaches such as warnings, corrective orders, negotiated remediation, and proportionate penalties, balance deterrence with constructive compliance support. This model is especially effective in resource-constrained contexts.

- **Guidance-Driven Enforcement Enhances Voluntary Compliance**

Regulators that invest in clear guidelines, consultation processes, and capacity-building programmes see higher voluntary compliance. Singapore's experience illustrates how education and collaborative enforcement can achieve broad, sustainable improvements.

- **Democratic Accountability Strengthens Public Sector Compliance**

Countries using parliamentary oversight, privacy impact assessments, and structured public consultations provide examples of how transparency enhances government compliance and public trust.

- **Sector-Specific Enforcement Improves Precision and Reduces Burdens**

Targeted regulatory approaches, e.g., tailored rules for health, credit reporting, or telecoms demonstrate how sectoral specialisation improves effectiveness while reducing unnecessary compliance costs.

H. Technology Governance and the Innovation-Protection Balance

- **AI Governance Frameworks Must Align Rights Protection with Economic Priorities**

International AI regulation illustrates the need for context-sensitive models. The EU AI Act provides a valuable template, but developing economies must adapt its provisions to local priorities and technological maturity.

- **Regulated Experimentation Supports Innovation with Safeguards**

Fintech and AI regulatory sandboxes in several jurisdictions demonstrate how controlled pilots can support new business models while managing risks. Evidence-driven policymaking results in more robust long-term frameworks.

- **Guidance and Engagement Help Promote Responsible Digital Markets**

Regulators that publish clear guidance on emerging technologies like biometrics, automated decision-making, cross-border transfers, enable innovation while maintaining strong rights protections.

I. Civil Society Engagement and Capacity Building

- **Civil Society Strengthens Oversight and Democratic Accountability**

Internationally, civil society organisations have shaped privacy reform, pursued strategic litigation, and held both governments and corporations accountable. This demonstrates that regulatory institutions alone cannot safeguard rights.

- **Strategic Litigation as a Tool for Advancing Privacy Rights**

Litigation experiences in countries with active constitutional courts illustrate how judicial review can reinforce privacy protections, especially in surveillance and government data-processing contexts.

- **Public Education Expands the Reach and Impact of Privacy Frameworks**

Advocacy groups in various jurisdictions have increased public understanding of rights, enabling individuals to hold organisations accountable. This reinforces the principle that privacy frameworks are effective only when the public can activate them.

J. Cross-Cutting Lessons from Rwanda's Sectoral Findings (Illustrative Example)

- **A Comprehensive Law Is Not Self-Executing**

Rights-based legislation creates a strong foundation, but implementation gaps persist when organisational practices lag. Rwanda's experience illustrates how transparency, user rights, and breach-readiness remain weak unless supported through sustained capacity building and oversight.

- **Multi-Agency Models Require Structured Coordination**

Where data protection responsibilities are distributed across specialised regulators, deliberate coordination is essential. Rwanda's experience underscores the need for harmonised enforcement to avoid regulatory gaps or overlaps.

- **Public Awareness Is a Critical Pillar of Effective Enforcement**

Low public understanding of data rights diminishes bottom-up accountability. Without broad awareness, enforcement relies solely on regulators an unsustainable model, especially in resource-constrained contexts.

- **High-Risk Sectors Require Prioritised Oversight**

Sectors handling sensitive or high-volume data such as health, digital lending, and betting—demand heightened scrutiny. Rwanda's assessments show how limited transparency in these sectors increases systemic risk.

- **Transparency Reporting Is a Key Indicator of Governance Maturity**

Only a few organisations publish transparency reports, revealing a broader structural weakness. Mandatory transparency requirements could significantly enhance accountability and public trust.

Synthesised Best-Practice Principles Across Jurisdictions

Strong regulatory independence supported by secure funding and depoliticised appointments.

Sector-specific guidance reflecting distinct risk profiles and operational realities.

Mandatory capacity-building programmes for regulators, organisations, and the public.

Clear, accessible, and locally grounded privacy documentation aligned with real processing activities.

Robust biometric governance, including special safeguards for sensitive identifiers.

Regularised technical audits focusing on security, access management, and third-party oversight.

Predictable cross-border transfer regimes with transparent adequacy criteria and standardised instruments.

Integrated multi-agency coordination structures anchored by a central harmonising authority.

User-centric oversight, prioritising transparency reporting and effective rights-exercise mechanisms.

6. Recommendations

Based on the findings of this report, it is clear that while notable progress has been made across jurisdictions including Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya and Uganda, gaps persist in legal clarity, institutional independence, enforcement capacity, public awareness, and cross border coordination. The following recommendations provide practical, actionable steps for key stakeholders to strengthen privacy and data protection ecosystems across Africa.

Recommendations for Governments

1. *Ensure Financial and Operational Autonomy:* Establish or strengthen independent Data Protection Authorities (DPAs) with secure, ring-fenced budgets and transparent appointment processes to guarantee impartial oversight.
2. *Strengthen Legal Frameworks:* Amend existing laws to include clear breach notification timelines, mandatory audits, and defined data retention limits, ensuring consistency with international standards (e.g., GDPR, Malabo Convention).
3. *Enhance Oversight of Surveillance Practices:* Introduce judicial authorization and periodic public reporting for state surveillance activities to prevent abuse and reinforce public trust.
4. *Ratify and Domestic Regional Treaties:* Countries yet to do so should ratify and implement the Malabo Convention and actively engage in EAC, SADC, and AU data governance initiatives.
5. *Promote Responsible Innovation:* Develop national AI and emerging technology frameworks requiring Data Protection Impact Assessments (DPIAs) for high-risk digital systems, particularly in e-government, digital ID, and health data platforms.

Recommendations for Policy Makers

1. *Benchmark against Global Best Practices:* Align sectoral legislation with international models such as GDPR, OECD Guidelines, and AU Model Laws, ensuring consistency across national policies.
2. *Clarify Penalty and Enforcement Provisions:* Introduce graduated, percentage-based penalties to promote accountability while maintaining a fair investment climate.
3. *Integrate Data Rights in Broader Policy Agendas:* Mainstream data protection into national digital transformation, e-commerce, and AI policies to promote holistic governance.
4. *Facilitate International and Regional Cooperation:* Promote cross-border data flow agreements, joint investigations, and harmonised standards across African states to ease digital trade and enforcement collaboration.

3. Recommendations for Data Protection Regulators

1. *Enhance Institutional Capacity:* Secure sustainable funding, expand staffing, and invest in digital tools for compliance monitoring, case management, and audit automation.
2. *Develop and Enforce Regulations:* Issue sector-specific guidance, especially for high-risk sectors like healthcare, fintech, betting, and digital lending, while clarifying dispute resolution and appellate mechanisms.
3. *Expand Public Awareness and Education:* Lead nationwide campaigns targeting youth, SMEs, and rural communities, integrating data protection into school curricula and professional training.
4. *Conduct Routine Compliance Audits:* Undertake random and risk-based audits, publish annual enforcement and transparency reports, and maintain a public register of compliant controllers.
5. *Collaborate Across Borders:* Establish regional regulator networks under AU or EAC frameworks to enable knowledge sharing, peer learning, and coordinated responses to transnational data issues.

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

1. *Strengthen Internal Governance:* Adopt privacy-by-design principles, appoint Data Protection Officers (DPOs), and conduct annual privacy audits.
2. *Implement Data Minimization and Security Practices:* Collect only necessary data, ensure secure storage and timely deletion, and adopt encryption and pseudonymization technologies.
3. *Establish Breach Notification and Transparency Protocols:* Publish annual privacy and breach reports and promptly notify both regulators and affected individuals of data incidents.
4. *Localize Privacy Policies:* Ensure privacy policies reflect domestic legal requirements and are accessible in local languages for transparency and compliance.
5. *Foster Innovation for Compliance:* Invest in privacy-enhancing technologies (PETs), secure-by-design products, and participate in regulatory sandboxes for ethical data innovation.

Recommendations for Data Subjects (Individuals)

1. *Exercise Legal Rights:* Use legal channels to demand access, rectification, erasure, portability, and objection under national data protection laws.
2. *Stay Informed and Vigilant:* Engage with awareness campaigns, verify consent conditions, and report suspected data misuse to regulators.
3. *Demand Transparency and Accountability:* Request clear information from organizations on how personal data is collected, stored, shared, and protected.

Recommendations for Civil Society and the Media

1. *Advocate for Enhanced Privacy Protections:* Campaign for expanded data subject rights (e.g., algorithmic transparency, right to be forgotten) and for stronger oversight of surveillance and biometric systems.
2. *Monitor, Report, and Educate:* Investigate privacy violations, publish findings, and translate technical issues into accessible language for public understanding.
3. *Foster Citizen Empowerment:* Promote digital literacy, encryption tools, and civic engagement to enhance privacy resilience.
4. *Convene Multi-Stakeholder Platforms:* Collaborate with regulators, academia, and private sector actors to create annual privacy observatories or national data protection forums for dialogue and reform tracking.

Recommendations for the Technical Community

1. *Provide Technical Expertise in Policy Development:* Support legislators and regulators in crafting evidence-based, technology-informed data laws.
2. *Develop Privacy-Enhancing Technologies (PETs):* Innovate tools for secure data storage, consent management, and breach monitoring accessible to SMEs and public entities.
3. *Conduct Cybersecurity and Compliance Training:* Offer capacity-building for data officers, IT staff, and entrepreneurs to strengthen practical implementation of privacy safeguards.
4. *Participate in Standards Development:* Collaborate with regional and international standards bodies to align local technical practices with global privacy and cybersecurity benchmarks.

Recommendations for Regional and International Mechanisms

1. *Advance Regional Harmonization:* The AU, EAC, ECOWAS, and SADC should coordinate convergence of legal standards and develop regional data protection benchmarks.
2. *Strengthen Regulatory Cooperation:* Build regional data protection taskforces and peer-review systems for enforcement and mutual recognition of adequacy.

3. *Facilitate Cross-Border Data Governance Frameworks:* Develop model laws and standard contractual clauses to guide secure data transfers within and outside Africa.
4. *Promote Knowledge Exchange:* Host annual continental data protection dialogues and capacity-building exchanges among national DPAs.

Recommendations for Development Partners

1. **Support Institutional Strengthening:** Fund training, infrastructure, and digital tools for DPAs, CSOs, and judiciaries.
2. **Invest in Research and Benchmarking:** Back regional comparative studies and indexing of data protection maturity to measure progress and guide reforms.
3. **Promote Inclusive and Rights-Based Digital Development:** Ensure all development and digitalization projects integrate data protection and human rights safeguards.
4. **Encourage South–South Cooperation:** Facilitate technical assistance and peer learning among African countries to accelerate regional data governance harmonization.

Cross-Cutting Priority Actions

- Establish national data breach response frameworks with clear timelines, responsibilities, and reporting procedures.
- Mandate public transparency reporting across all sectors handling personal data.
- Institutionalize data protection education across schools, universities, and professional certification programs.
- Embed privacy, security, and ethical AI principles in all digital transformation strategies.

Implementing these measures will build institutional independence, public trust, and continental coherence in data governance positioning African nations to balance innovation, security, and human rights in the evolving digital ecosystem.

7. Conclusion

Africa's accelerating digital transformation continues to redefine governance, commerce, and social interaction, making robust data protection a fundamental pillar of trust, inclusion, and sustainable digital growth. The collective experiences of Nigeria, Ghana, Botswana, Rwanda, Tanzania, Mauritius, Zimbabwe, Kenya and Uganda, demonstrate steady legislative progress toward safeguarding personal data, even as countries contend with persistent enforcement, compliance, and capacity challenges that test the depth and resilience of these reforms.

Across the region, a clear trend has emerged where legal and institutional foundations are largely in place, but the effectiveness of these frameworks depends on consistent application, institutional maturity, and public trust.

Ghana and Botswana have advanced their legal architectures, introducing or strengthening statutory frameworks to address previously identified gaps in oversight, breach management, and institutional authority. Yet, underfunded regulators, uneven sectoral compliance, and limited public engagement continue to constrain impact. Sustained capacity building and the integration of global standards, such as the GDPR and the Malabo Convention on Cyber Security and Personal Data Protection will be essential to deepen operational effectiveness.

Mauritius, an early pioneer, continues to align closely with international norms through its Data Protection Act 2017 and institutional mechanisms. However, translating a sophisticated legal framework into consistent enforcement and transparency remains a pressing challenge. A stronger national data governance strategy, underpinned by enhanced breach response, corporate accountability, and regional cooperation, can help Mauritius consolidate its leadership role.

In Nigeria, the enactment of the Nigeria Data Protection Act 2023 and establishment of the independent Data Protection Commission have positioned the country among Africa's most ambitious data governance jurisdictions. However, stark disparities persist across sectors ranging from strong compliance in financial services to gaps in government and telecommunications. Nigeria's next frontier lies in strengthening institutional enforcement, promoting citizen awareness, and ensuring that the protection of over 200 million individuals is not just a statutory goal but an operational reality.

Kenya's dynamic data protection ecosystem continues to shape regional norms. Its proactive Office of the Data Protection Commissioner (ODPC) and a vibrant digital economy exemplify both progress and complexity. Yet, regulatory gaps, resource limitations, and new technological frontiers such as AI, block chain, and the Internet of Things demand agile, future-ready governance that preserves privacy while fostering innovation. Maintaining institutional independence and embedding ethical technology practices will be central to Kenya's continued leadership.

Rwanda has adopted a principled approach to ethical data governance, integrating privacy and security into its broader digital transformation agenda. However, operationalizing compliance across sectors remains uneven. Targeted enforcement, enhanced regulator coordination, and greater citizen awareness will be vital to convert strong legislation into measurable protection outcomes.

Uganda, Zimbabwe, and Tanzania illustrate the growing depth of regional participation in Africa's data protection movement. Uganda's 2019 Data Protection and Privacy Act provides a solid base but requires enhanced enforcement and sectoral audits to ensure effective compliance. Zimbabwe's 2021 framework reflects growing recognition of privacy as a right, yet transparency, reporting, and accountability mechanisms remain limited. Tanzania's 2022 Data Protection Act signals commitment to reform but still needs institutional strengthening and alignment with continental and international norms to realize its potential.

Taken together, these national trajectories reveal an Africa in transition, from establishing data protection laws to embedding a culture of privacy and accountability. Yet, the enduring "implementation gap" remains the region's greatest challenge: limited institutional resources, fragmented oversight, and low public awareness continue to impede full realization of privacy as a lived right rather than a legal aspiration.

Looking ahead, three strategic imperatives will shape the next phase of Africa's data protection evolution:

- **Institutional Empowerment and Sustainability:** Data protection authorities must be adequately resourced, autonomous, and equipped with technical expertise to enforce compliance across complex, data-driven sectors.
- **Harmonization and Cross-Border Cooperation:** Regional alignment through the Malabo Convention, AU digital frameworks, and GDPR-informed best practices can strengthen interoperability, facilitate lawful data flows, and enhance Africa's global digital competitiveness.
- **Citizen-Centered Data Governance:** Governments, businesses, and civil society must foster a culture of data ethics, transparency, and user empowerment through public education, accessible privacy tools, and open accountability mechanisms.

Ultimately, data protection is not merely a regulatory requirement, it is a human right and an enabler of digital trust, innovation, and democratic resilience. Africa's success will depend on transforming legal frameworks into living systems of accountability, inclusivity, and respect for personal dignity. By embedding privacy at the heart of digital policy, the continent can build a future where technological advancement and fundamental rights progress together anchoring Africa's position as a responsible and rights-driven participant in the global digital economy.

The Unwanted Witness

Bulange Mengo, Block 381, Plot 26, Nsibambi Village, Sentema Road,
P.O.BOX 71314 Clock Tower Kampala - Uganda