PRIVACY SCORECARD REPORT

Kenya & Uganda

NOV 2022

PRIVACY Scorecard

Written and Compiled by:

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Strathmore University
Centre for Intellectual Property and Information Technology Law

With support from:

CIVIL RIGHTS DEFENDERS

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

www.unwantedwitness.org

PRIVACY SCORECARD REPORT

2022

Authored by:
Unwanted Witness and Center for Intellectual Property and Information Technology Law (CIPIT)

TABBLE OF CONTENTS

Contents

Privacy Scorecard Report | 2022

LIST OF ACRONYMS

List of acronyms

- **CIPIT -** Centre for Intellectual Property and Information Technology Law
- **DPA -** Data Protection Act, 2019, Kenya
- **DPPA -** Data Protection and Privacy Act, 2019, Uganda
- **DPPRs -** Data Protection and Privacy Regulations, 2021, Uganda
- **NITA -** National Information Technology Authority
- **NPDPD -** National Personal Data Protection Director
- **ODPC -** Office of the Data Protection Commissioner
- **OECD -** Guidelines on Privacy OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data
- **PDPO -** Personal Data Protection Office
- **UNGPs -** The United Nations Guiding Principles on Business and Human Rights

List of respondent companies

Kenyan Companies

- Airtel
- Bank of Baroda
- Jumia
- KCB
- Mydawa
- Safaricom

Ugandan companies

- Absa
- Airtel
- Glovo
- Jumia
- MTN
- Stanbic

About Us

Unwanted Witness

The Unwanted Witness is a civil society organization (CSO) that was established to respond to the gap in effective communication using various online expression platforms.

Unwanted Witness was established in 2012 by a group of netizens, bloggers, activists, writers and human rights defenders as an independent, non-partisan and not-for-profit civil society organization.

It seeks to create secure uncensored online platforms for activists, netizens, bloggers, freelance journalists and writers to promote human rights through writing and informing, educating the citizenry who also utilize the platform for strengthening free expression and demand for accountability.

CIPIT

The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training Centre based at Strathmore University, Nairobi, Kenya.

With a mission is to study, create, and share knowledge on the development of intellectual property and information technology, especially as they contribute to African Law and Human Rights CIPIT's team is multidisciplinary, drawn from law, political science, computer science and development while using diverse methodological approaches to inform debates on ICT applications and regulation.

UNWANTED WITNESS
"Amplifying Voices, Changing lives"

Strathmore University
Centre for Intellectual Property and Information Technology Law

Introduction

World over, the right to privacy is contentious as its meaning, parameters, limitations cause controversy. In the African context, this could partly be attributed to the infancy of comprehensive legislative and policy initiatives that ensure the realization of the right. Be that as it may, over time, consensus has been built to the effect that the right to privacy is critical in many aspects of life such as in the enjoyment of other human rights and plays an essential role in 'delineating the legitimate limits of governmental power'.[1] Further, with the prominence of non-state actors in the discourse comes the conflict between the cost of 'privacy' vis-à-vis 'prying'.[2] Prying is a direct attack on personal data protection initiatives. The economic and technological trends in the world account for the recent increase in the demand for private personal data. This is reasonably expected where there is a relationship between the demander and the owner of the information. These relationships may be actual or potential, personal, or business or where the information is critical to the demander.[3] This background could partly explain the demand for the development of privacy and data protection legal and policy frameworks.

Hitherto, the American jurisprudence traced the right to privacy as a proprietary right although this has slowly changed with the current view leaning to it being recognized as part of the right to liberty.[4] The right to privacy is therefore currently viewed more as related to personal dignity which is core to the human existence.[5] 'At the root of the dignity is the autonomy of the private will and a person's freedom of choice and of action. Elsewhere, privacy has been part of the fabric of English law since at least the case of Entick v. Carington'.[6] In Africa, the development of privacy legal protection in the early 2000s was largely due to the European Directive 95/46/EC that required sufficient legal protection before any transfer of personal data to developing countries.[7]

Specific to the region, over the past three years, there has been an increase in the enactment of data protection laws,[8] particularly within East Africa. These legislations domesticate the international legal protection such as Article 12 of the Universal Declaration of Human Rights,[9] and Article 17 of the International Covenant on Civil and Political Rights.[10] Even with this progression, perhaps the most instructive framework that has shaped privacy legislations in the two countries by especially extending the protection to non-state actors is General Comment 16 and other soft law standards discussed here below. The Human Rights Committee's General Comment 16 of the ICCPR specifically expands the obligation to realize the right to privacy to both

1 Jed Rubenfeld 'The Right of Privacy' Harvard Law Review Vol. 102, No. 4 (Feb., 1989), pp. 737-807 at 737 at https://doi.org/10.2307/1341305 (accessed on 22 September 2022).

2 Richard A. Posner, "The Right of Privacy," Georgia Law Review 12, no. 3 (Spring 1978): 393-422 at 394.

3 As above.

4 See Boyd v. US, 116 US 616. See also Raddivari Revathi 'EVOLUTION OF PRIVACY JURISPRUDENCE – A CRITIQUE' Journal of the Indian Law Institute, APRIL-JUNE 2018, Vol. 60, No. 2 (APRILJUNE 2018), pp. 189-199 at 190, available at https://www.jstor.org/stable/26826635 (accessed on 4 October 2022).

5 Raddivari Revathi (n 4 above).

6 (1765) 19, Lord Chief Justice Camden, in the Court of Common Pleas, decided the case of 'seizure of papers' in favour of John Entick against Carryington, messenger to king, Raddivari Revathi (n 4 above) at 191.

7 Alex Boniface Makulilo 'Privacy and data protection in Africa: a state of the art' International Data Privacy Law, 2012, Vol. 2, No. 3 163, available at http://repository.out.ac.tz/323/1/Privacy_and_Data_Protection_in_Africa-A_state_of_the_art.pdf (accessed on 4 October 2022).

8 Daigle, B. (2021). Data Protection Laws in Africa: A Pan African Survey and Noted Trends. Journal of International Commerce and Economics. https://www.usitc.gov/journals (accessed on 4 October 2022).

9 1948.

10 1996.

state and non-state actors.[11] This is a timely clarification given the volume of private data in the hands and control of private actors. The Committee additionally notes that the obligations imposed by Article 17 ICCPR require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.[12] The other soft law standards that are relevant to this discourse are the United Nations Guiding Principles on Business and Human Rights (UNGPs).[13] Also known as the UN's protect, respect and remedy framework, the UNGPs though soft law, provide a benchmark to hold businesses accountable for the respect and protections of human rights in the territories in which these entities operate. The UNGPs are premised on the background that '...the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights;'[14] Equally relevant in this context is the access to remedy framework for victims of human rights abuses by business actors.[15] The other applicable instrument is the United Nations Internet Rights and Principles Coalition Charter of Human Rights and Principles for the Internet launched in 2011 whose principles domestic legislations in Kenya and Uganda largely mirror.[16]

It is against his backdrop that countries such as Kenya and Uganda, enacted their data protection legislations in 2019, with Uganda's operationalizing regulations adopted in 2021. The legislative efforts were to operationalize Article 27 of the Constitution of the Republic of Uganda, 1995. Similarly, personal data protection is a realization of the right to privacy and, in the Kenyan context, the right to privacy is enshrined under Article 31 of the Constitution of the Republic of Kenya, 2010. Personal data is now more than ever being utilized in different sectors for adequate delivery of services. The public and private sectors alike leverage different technologies for the provision of services, and in so doing require the constant collection and generation of personal data. The Kenyan Data Protection Act (DPA) of 2019 sets parameters by which personal data is protected and preserved. The two core elements of data protection are the principles that (i) govern the processing of personal data, and (ii) the rights of the data subjects. The DPA highlights these two elements in Sections 25 and 26, respectively.

From the Ugandan perspective, the Data Protection and Privacy Act, 2019 (DPPA) is hinged on the eight principles relevant to the processing of personal data contained in the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data (OECD Guidelines on Privacy).[17] These include: the collection limitation principle; the data quality principle; the purpose specification principle; the use limitation principle; the security safeguard principle; the openness principle; the individual participation principle; and the accountability principle. This privacy score card report assesses how well privacy policies of selected companies in the three identified sectors of telecommunication, e-commerce and financial services measure up to these principles in Kenya and Uganda.

Suffice to note that data protection impacts various sectors and in turn, the businesses within those sectors must comply with the requirements of the data protection laws. This would contribute to changing the adoption and utilization of technology and impacting service delivery and customer relations. Privacy policies as such establish the means through which compliance can be established within the non-state actors such as corporations. To this end this report focuses on evaluating the extent to which companies in selected sectors within Kenya and Uganda are compliant with the provisions of the DPA and the DPPA respectively and other relevant international and domestic legal standards. Below the report details a more context specific background to the study.

11 See Para 1 of the CCPR General Comment No. 16: Article 17 (Right to Privacy)The Right to Respect of Privacy, Family, Home and Correspondence, andProtection of Honour and Reputation, Adopted at the Thirty-second Session of the Human, Rights Committee,on 8 April 1988 available on https://www.refworld.org/docid/453883f922.html (accessed 3 October 2022).

12 Ibid.

13 Adopted in 2011, available at https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciples-businesshr_en.pdf (accessed 1 October 2022.

14 Page 1 of the UNGPs.

15 Page 1 of the UNGPs.

16 Available at https://internetrightsandprinciples.org/charter/ (accessed on 2 October 2022).

17 Updated in 2013, available at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacy-

1.1 Background of the 2022 privacy score card report

The 2022 privacy score card is a buildup on the Privacy Scorecard Report of November 2021 developed by Unwanted Witness.[18] The 2021 Privacy Scorecard was a data protection compliance monitoring tool focusing on Ugandan data collectors. The 2021 Privacy scorecard assessed the performance of the following sectors: Social Sector, e-commerce, financial, telecom, and government agencies against five indicators. The indicators were: Practicing robust data security, compliance with privacy best practices, disclosure of relevant information to data subjects, mentions third parties with whom personal data is shared and mentions the nature and quality of information shared with 3rd parties. From the assessment, a generally over all low index score of 35% was recorded, with the e-commerce sector scoring an average score of 50%, financial sector 36% and the telecom sector at 35%. The data security indicator scored highest at 66% across the sectors reviewed. Although the parameters adopted for the 2022 score card differ a little from the previous report, this is a great benchmark upon which to base an assessment of whether or not there has been progress in data protection across the selected sectors. The 2022 report therefore benchmarks with the findings of the previous scorecard.

Further, the 2022 Privacy Scorecard report develops onto the 2021 one and expands the scope to include Kenya. The methodology adopted in the 2022 report is deeper with focus on only three sectors of telecommunication, financial services and the e-commerce sectors. The 2022 report is made possible by a collaboration between Unwanted Witness and the Centre for Intellectual Property and Information Technology Law (CIPIT). The main objective of the 2022 report is to generate research that could be used to empower data collectors/processors to adopt data protection best practices; and citizens to demand for accountability in the area of personal data protection. The report could also inform legal and policy reform for the between management of personal data of data subjects by especially non state actors.

The scorecard evaluates corporate privacy policies and practices in 2022 against internationally accepted standards and national data protection laws. The 2022 report highlights the data protection performance of the three selected sectors of telecommunication, e-commerce and financial services in Kenya and Uganda. The assessment utilizes objective and quantifiable parameters for analyzing the policies and practices of the selected data collectors. The study assesses the publicly available policies of the selected companies to determine their compliance with applicable data protection legislation. Detailed below are the specific objectives this study sought to achieve.

1.2 Objectives of the 2022 Privacy scorecard

The specific objectives of the privacy scorecard were: -

To determine the legal protections of personal data and privacy in Kenya and Uganda;
To evaluate changes in compliance (and practices) of selected companies which featured in the 2021 Uganda's scorecard report;
To evaluate the compliance of data collectors in Kenya and Uganda with data protection laws;
To document the nature of abuse and violations, if any, of the rights to privacy by the assessed companies in each respective country;
To provide recommendations to improve compliance with data protection laws in Kenya and Uganda by private non-state actors;
To provide a toolkit for evaluating compliance of data collectors that citizens could replicate and rely on for better protection.

andtransborderflowsofpersonaldata.htm (accessed on 20 October 2022).

18 The Privacy Scorecard Report, 2021 is available on https://www.unwantedwitness.org/privacy-scorecard-report-2021/ (accessed 26 October 2022).

Country Insights

1.3.1 Kenya

Data privacy and protection have become crucial components in Kenya's industries. Enacted in 2019, the DPA introduced new parameters guiding and regulating the processing of personal data. The purpose of this Act is to regulate the processing of personal data, to ensure that the processing of a data subject's personal data adheres to the principles outlined in Section 25, and to protect the privacy of individuals.[19] Section 25 of the Act stipulates that every data controller or data processor, in this case, a company that processes, stores, or manages personal data, must ensure that personal data is processed in accordance with the data subject's right to privacy, in a lawful, fair, and transparent manner in relation to any data subject. In addition, the data should be collected for clear, legitimate, and specified purposes, and should not be processed in a way that is inconsistent with those purposes. The company privacy policies must clearly state this information.

Since its enactment, the DPA has been operationalized through different key hallmarks, beginning with the appointment of the Data Protection Commissioner and the establishment of the Office of the Data Protection Commissioner (ODPC).[20] The ODPC is the regulatory body tasked with ensuring compliance of businesses to the DPA. The ODPC's Registration of Data Controllers and Processors Regulations and the Compliance and Enforcement Regulations provide the terms and conditions under which data controllers and processors must register in adherence to the provisions of the DPA and the complaints handling procedure, respectively. Along with these regulations, the ODPC has also published guidance notes on: (i) consent, (ii) the registration of data controllers and processors, (iii) data protection impact assessment, and (iv) the complaints management manual. Early this year (2022), the office launched an online registration portal for data controllers and processors.

The registration of data controllers and processors is one of the elements of compliance with data protection legislation. Individuals and organizations cannot act in their capacity as data controllers or processors unless they are registered with the ODPC. The registration of controllers and processors ensures transparency and accountability in the processing of data. It also aids in the regulation of data processing.

Monitoring compliance through complaints is also one of the ways in which the ODPC ensures that the provisions of the DPA are adhered to. To date there have been a number of complaints filed with the Data Commissioner; the complaints range from data breaches by political parties to individual complaints on misuse of personal data by service providers. It is important to note that the DPA provides for sanctions/penalties for failure to comply with the provisions of the Act. Administrative fines are issued for non-compliance - a maximum penalty of five million Kenya shillings or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, may be issued by the Data Commissioner.

19 Section 3.

20 Section 5.

1.3.2 Uganda

Enacted in 2019, and operationalized in 2021 by the Data Protection and Privacy Regulations (DPPRs), the DPPA aims at protecting the privacy of the individual and of personal data by regulating the collection and processing of personal data; details the rights of data subjects on one hand and the obligations of data collectors, data processors and data controllers on the other hand; in addition to regulating the use and disclosure of personal data, among other related matters.[21] The hallmark of the DPPA is the respect of the right to privacy that is constitutionally guaranteed as mentioned above.[22] The DPPA applies to all entitles collecting, processing, holding or using personal data within Uganda or outside Uganda if the data relates to Ugandan citizens.[23] The entities regulated include persons, (both natural and artificial), institutions and public bodies.

The DPPA enunciates the principles that should guide any data collector, processor, controller, holder or user of personal data. These include accountability to the data subject; fairness in the collection and use of the data; ensuring that the collection, storage, processing, among others processes are limited to only relevant and necessary data; retention of data only for periods authorized by law or as long as the same is necessary; transparency and participation of the data subject in these processes; and lastly but no means the least the observance of security safeguards in respect the data.[24] The assessment of the privacy policies of the selected companies below is based on these parameters. The DPPA additionally provides for offences for breaches and noncompliance that attract a fine of UGX 4, 900, 000 or imprisonment not exceeding 10 years or both.[25]

The DPPA establishes an independent personal data protection office (PDPO) under the National Information Technology Authority (NITA) which is responsible for personal data protection.[26] Headed by the National Personal Data Protection Director (NPDPD), the PDPO oversees the implementation and enforcement of the Act; promotes the protection and observance of the right to privacy of a person and of personal data; monitors, investigates and reports on the observance of the right to privacy and of personal data; formulates, implements and oversees programmes intended to raise public awareness about the Act; and receives and investigates complaints related to infringement of the rights of the data subject, among others.[27] The Data Protection and Privacy Regulations, 2021 create additional functions on the PDPO as well as its powers

21 Long title.
22 See Section 10 of the DPPA.
23 Section 1.
24 See Section 3 of the DPPA, 2019.
25 See Part VIII of the DPPA.
26 Section 4.
27 Section 5.

such as providing guidance, supervision, monitoring and coordination of data collectors, processors and controllers and conducting data audits, among other roles.[28] The PDPO may establish a mechanism for collaborating and promotion of partnerships between various categories of players in the data protection and privacy aspects, and charging fees for services provided by the office.[29] Every data collector, data processor and data controller is mandated to register with the PDPO.[30] In June 2022, the PDPO launched the data protection and privacy portal to streamline data protection, by enabling stakeholder registration, breach and violation and complaint reporting. By the time of writing this report, sectors were yet to file compliance reports. What could however be established from an interaction with Ms. Stella Alibateesa the NPDPD, many of the complaints so far received are against telecommunication sector and relate to unlawful sharing of data by data collectors, and controllers that lead to unsolicited messages and mobile money related fraud.

In a special way, the DPPRs provide for data protection impact assessment where the collection or processing of personal data possess a high risk of human rights violation or abuses of individuals prior to the data collection or processing.[31] The data protection officer is required to publicize the list of data processing operations that require such data impact assessment.[32] This provision if implemented would go a long way in enabling data controllers and processors to project the likely impact of their data processing activities and put in place measures to ensure personal data protection of data subjects.

2. Methodology

This report details an assessment of compliance of six private companies in each country, within three sectors: financial services, telecommunication, and e-commerce. These sectors have the highest utilization of personal data given their operations and undertakings. For each of the sectors, two companies were identified for analysis. The companies were selected on the basis of their market share in Kenya; one with the highest market share, and the second with mid – tier share. In Uganda, the selected companies were all large Tier 1 financial institution, the e-commerce sector in Uganda had the largest provider with a relatively young entrant while in the telecommunication sector, both companies reviewed have a substantial market share and are the best two leading providers. The privacy policies of these companies were then evaluated on the basis of five core indicators. Each evaluation indicator has a list of categories for which a score is awarded if they are deemed to comply with privacy policy legal framework and regulations. The indicators, and their attendant categories, are as follows:

A. Existence of an accessible readable and noticeable privacy policy

A company will have fulfilled this requirement if the privacy policy is public, published, noticeable, and readable. The privacy policy is considered public and published if it is available on the company's website or mobile application. The privacy policy also needs to be noticeable; if the policy notice is in fine print, the policy is not considered noticeable. The readability of the privacy policy is assessed using the Hemingway editor. Hemingway Editor is an online tool that analyzes text for readability to determine how simple or difficult it is to comprehend a piece of writing.[33] A score of good classifies the policy as readable. An okay score on the other hand does not earn the company a credit score. The editor also assesses the length of text. In this study, a privacy policy with a word count below 200 was deemed an inadequate policy.[34] For each of the categories listed above – public, published, readable, noticeable - a score is awarded.

B. Informed Consent

In order to fulfill this requirement, users must be provided with the following information:

Company's contact details - The privacy policy should include one of the following: address, contact email, or phone number.

Purpose of data collection - The privacy policy must mention the reason for collecting data.

28 Regulation 4.

29 Regulation 5.

30 Section 29 (2).

31 Regulation 12 (1) of the DPPR.

32 Regulation 12 (3) of the DPPR.

33 https://hemingwayapp.com/

34 A word count below 200, generally would not adequately convey all the components of a privacy policy as prescribed under these evaluation criteria.

Types of personal data collected - The privacy policy must mention the types of personal data collected. Data storage duration - The privacy policy should mention the storage period for the personal data collected. Companies that simply indicated that they store the data in accordance with the law equally scored a credit.

Right to access personal data - The data subject should be informed of their right to access personal data in the privacy policy. This right enables data subjects to obtain a copy of their personal data as well as additional information. It also enables data subjects to comprehend how and why companies are utilizing their data, and to verify that such use is lawful.

Right to update, correct, or erase personal data - The privacy policy should unequivocally mention that the data subject has the right to correct, delete or erase personal data. This right can be exercised if the information in the company's database is inaccurate and needs to be updated or if the company no longer requires the data for the purpose for which it was originally collected or used.

Right to restrict or object to data processing - The data subject should be informed of his right to restrict or object to data processing in the privacy policy. This means that data subjects can limit the way their data is used. This right may be exercised when the accuracy of the data is contested, when the data is no longer required but cannot be deleted for legal reasons, or when a decision regarding their objection to processing is pending.

Right to withdraw consent at any time - The privacy policy should mention that the data subject has the right to withdraw consent at any time. Before providing consent, the data subject must be informed that they can do so verbally, as in cases involving their health, or in writing, as in financial or e-commerce. The legality of processing performed in reliance on consent prior to its withdrawal is not affected by its withdrawal.

A score is awarded for each of the categories listed above for this indicator.

C. Data collection and Third-Party Data Transfers

The privacy policy must provide users with information on (i) which parties have access to collected data, and (ii) any data transfers to external parties. In order to fulfill this requirement, the privacy policy of the company should ensure that data subjects' information is not unlawfully disclosed to third parties. The following categories were assessed for this indicator:

Data collection and privacy policy compliance - The privacy policy must mention the nature and category of personal data to be collected.

Data collection compliance – The privacy policy must provide information on the utilization and flow of information on any of their applications. For this criteria, an interception environment tool, developed by Privacy International,[35] is used to analyze how data is used by a platform's application developer and by any third parties. The interception environment tool allows one to see the flow of data in applications from a device back to a company or to third parties.[36]

Data Sharing and privacy policy compliance - The privacy policy must mention parties with access to collected data and any data transfer to external parties that may occur. Assessment of this criteria is done via technical analysis – software, Ghostery,[37] Blacklight,[38] and Exodus[39] programs are used to find trackers on the company website or mobile application. Web trackers are used to collect information about site users to monitor online activity, this practice is used to drive online services such as digital advertising and website analytics. The most common web trackers are cookies.[40]

35 Privacy International, https://privacyinternational.org/

36 'Data Interception Environment.' (Privacy International)<https://privacyinternational.org/learn/data-interception-environment>

37 https://www.ghostery.com/

38 https://themarkup.org/blacklight

39 https://reports.exodus-privacy.eu.org/en/

40 M.J Kelly, 'What is a Web Tracker.' (Mozilla , 2019) <https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/>

D. Practice Robust Data Security

Companies should make a commitment and take steps to implement robust data security measures. The data controller or processor is required to take appropriate measures to safeguard personal data from accidental access, erasure, alteration, disclosure, or destruction. To that end, the privacy policy must mention how personal data will be secured. Assessment of this criteria is done through a technical analysis of the company's website using the Qualys SSL Labs software.[41] The software grades how well a website has been set up. A security header software is also used to grade how secure the website is.[42] The categories analyzed for this indicator are,

SSL Server score for the company website. The SSL server score indicates whether the website has been accurately set up meaning, whether the website address is valid, the likelihood of errors when used, whether it is trusted and how vulnerable it is to cyber-attacks and data breaches.

Mention of how personal data is secured in the privacy policy relates to existing technical and organizational measures that have been put in place and utilized.

Security header score. This score will indicate whether the website has directives to configure security defenses in web browsers. Based on these directives, browsers can make it harder to exploit client-side vulnerabilities to cyber-attacks and data breaches.

Accountability

A score is awarded in this indicator if a company has published a transparency report in the year under review. A transparency report is a public communication document that discloses key metrics and information regarding data governance and enforcement measures on a platform. Depending on company policies and terms of service, intellectual property laws, and local laws and regulations, transparency reports may include third-party requests for users' private data, content, and platform enforcement measures.

41 SSL Server Test <https://www.ssllabs.com/ssltest/>

42 Security Headers <https://securityheaders.com/>

2. Company Selection Criteria

2.1.1 Kenya

For this evaluation in Kenya two companies across three sectors were reviewed. These were from financial services, telecommunications and e-commerce. These sectors have had the widest transition into digitization and the utilization of different technologies. Consequently, the processing of personal data is at the center of their service delivery. The companies evaluated for each sector were selected based on the market share. We selected one company with the highest market share and another with the lowest or mid-tier market share. The results and findings of the companies evaluated across the three sectors will be presented in the sections below, however the companies have been anonymized so as to reflect an unbiased analysis of the findings presented.

For financial services the report focused on Company F-S-K 1 and Company F-S-K 2. Company F-S-K 1 is a tier 1 banking institute, tier 1 are large banks with the highest cumulative assets and depositors. The banks in this tier control 49.9% of the market share. Company F-S-K 2 is a mid-tier bank / tier 2, tier 2 banks control 41.7% of the market share. Company F-S-K 1 traces its history to the 19th Century and has been operational in Kenya for over a century. Company F-S-K 1 is operational in 7 countries in the African region with 497 branches across the region with approximately 30.1 million customers and 8,877 employees across all its branches. Company F-S-K 2 originating from India, has been operational in Kenya for 68 years, having 14 branches across the country it holds a 3% market share with an overall ranking of 10th among 42 banks.

Our evaluation of the telecommunications sector focused on companies T-C-K 1with the highest market share of 67% and T-C-K 2 with a market share of 27.2%. Company T-C-K 1 has an estimated 35.6 million subscribers, with over 42 authorized outlets in the country and over 5500 staff directly and over 500,000 indirectly and operates in 10 countries across the African Region. Company T-C-K 1 is a leading provider of telecommunications and mobile money services in 14 African nations, primarily in East Africa, Central Africa, and Western Africa. It originated in India and began operations in Kenya in 2010. Company T-C-K 2 is the second largest provider of telecommunications services in Kenya. It has an estimated 16.2 million subscribers out of a total of 59.8 million on the Kenyan market, which corresponds to a 27.2% market share.

Evaluation of the e-commerce sector focused on Company E-C-K 1 and Company E-C-K 2. Company E-C-K 1 has between 201-500 employees and 6 outlets in the country. It also operates in 11 countries across the African continent and has 3.1 million active consumers. It is built around logistics, payment and marketplace services. The company is a dominant e-commerce company in Africa with a market share estimated to be over 60%. Company E-C-K 2 is Kenya's first online pharmacy with a market share of less than 3% and has a staff of about 40 employees. The company enables consumers to purchase high quality medicine and also wellness products through an app or their website. Several people use the platform since it is estimated as having over 80,000 registered users.

	Market shares	Subscribers/ customers	Services
Financial Services			
Company F-S-K 1	14%	30.1 million	Its banking portfolio comprises savings, transaction, and current accounts; credit, debit, and prepaid cards; home loans, mortgages, treasury bills and bonds, secured and unsecured loans, micro and corporate loans, and asset and trade financing, and personal loans, investment banking, trading, foreign exchange, financial advisory and brokerage services, and life and non-life insurances. Company F-S-K 1 also offers internet, institutional, mobile banking; and cash management, capital management, custodian services, foreign exchange, and money market services.
Company F-S-K 2	3%		Retail Loans. Deposits. Loans Advances. Digital Banking. International banking. Personal banking.
Telecommunications Sector			
Company T-C-K 1	67%	35.6 Million	Basic voice, international dialing, international roaming, short message service ("SMS"), data, voice mail, financial services such as M-Pesa.
Company T-C-K 2	27.2%	16.2 million	Mobile Services. Telemedia Services. Fixed telephony and broadband internet. Digital TV Services.
E- Commerce			
Company E-C-K 1	60%	3.1 million	Marketplace service Logistics service Payment service.
Company E-C-K 2	3%	80,000	Online Pharmaceutical and logistics services.

Table 1: The table above gives a bio data of the Kenyan companies evaluated across the three sectors, financial services, telecommunications and e-commerce. It highlights the selected companies market share, number of subscribers and customers as well as the services offered. NB: No substantive information was found on the number of customers for CompanyF-S-K 2.

2.1.2 Uganda

As was with Kenya, two companies per sector were selected for Uganda. The demographics of the companies selected from both countries differed a little as is presented below. In the financial services and telecommunication sectors, both companies selected are the biggest with a big market share. The e-commerce sector company selection included one oldest and largest company on one hand and another that has spent two years in operation in Uganda, on the other hand. For the same reasons advanced above, the companies evaluated were anonymized and the use of codes adopted.

From the telecommunication sector, the major players below were reviewed. Company T-C-U 1 which having entered into the sector in 2010 as a result of an inter country acquisition, boasts of approximately 10 million out of the 28.3 million mobile network subscribers in the Uganda. This translates into a 35.3% market share. [43]Company T-C-U 2 on the other hand is the largest telecom company in Uganda, with a customer base that has grown from 11.2 million subscribers, accounting for 55% market share, as of 30 June 2017 to 47.5% of the mobile telephone market, by the end of 2021 and with a subscriber base of 16.7 million accounts and 5.7 million active data subscribers.[44] Company T-C-U 2 operates in 22 countries in Africa and the middle East.

In the e-commerce sector, Companies E-C-U 1 and E-C-U 2 were evaluated. The government's efforts to strengthen the e-commerce sector has enabled its growth in the past decade. Company E-C-U 1 was founded in Nigeria in 2012 and launched in Uganda in 2014, and has grown to become Uganda's biggest and most popular e-commerce site with over 800,000 monthly users.[45] Company E-C-U 1 has partnerships with local and international brands which enhances their reach and service provision. Company E-C-U 2 on the other hand is a more recent player, with origins from Spain and presence in 21 countries, the company specializes in food deliveries.[46] Company E-C-U 2 commenced operations in Uganda in October 2020. This could explain why Uganda specific performance statistics such as market share, number of customers are largely scanty.

In the financial services, both companies reviewed are in the Tier 1 financial institutions category with company F-S-U 1 being the largest Tier 1 Financial Institution, with total assets of approximately UGX 8.71 trillion in 2021 and a market share of 21%.[47] Company F-S-U 2 on the other hand is the 3rd largest Tier 1 Financial Institution by assets with a total of approximately 4 trillion and a market share of 9.7% by 2021.[48] Company F-S-U 1 is the oldest commercial bank in Uganda tracing its history as far back as 1906 with the defunct National Bank of India. The bank evolved with several bank take overs until 2002 when Standard Bank acquired 90% of the shares in the Uganda Commercial Bank and rebranded to the current company name. Company F-S-U 2 on the other hand commenced operations in Uganda in 1927 and has equally gone through several management and name changes to date, with the most current rebranding having happened in 2019. Both companies reviewed are largely foreign owned with one being majorly South African owned and the other with its roots from Great Britain.[49]

43 The Independent Uganda (6 October 2021). "Fears over MTN, Airtel dominance in Uganda's telecom sector". The Independent (Uganda). Kampala, Uganda.

44 Esiara Kabona (2 July 2022). "Tough times in telecom sector as new MTN boss Sylvia Mulinge takes office". The EastAfrican. Nairobi, Kenya.

45 See https://ictguy.com/ecommerce-websites-in-uganda/ accessed on 30 September 2022. See also https://www.pmldaily.com/business/2022/06/jumia-celebrates-decade-of-e-commerce-in-uganda.html accessed 30 September 2022.

46 https://techpointmag.com/glovo-in-uganda-to-dis-rupt-food-delivery-services/ accessed on 3 October 2022.

47 See https://www.watchdoguganda.com/news/20220717/139829/list-top-10-powerful-and-richest-bankers-in-uganda-2022.html accessed on 20 October 2022.

48 Ibid.

49 https://african.business/2012/01/finance-services/uganda-foreign-banks-dominate/ accessed on 20 October 2022.

	Market shares	Subscribers/ customers	Services
Financial Services			
Company F-S-U 1	21%	572,168 customers by Dec 2021	Largest Tier 1 banking financial institutions services with agency banking and banc assurance.
Company F-S-U 2	9.7%	- (Information not readily available publically) Only indicates that customer deposits have grown to UGX 2.4 trillion.	Third largest Tier 1 banking financial institutions services with agency banking and banc assurance.
Telecommunications Sector			
T-C-U 1	35.3%	10 million	Telecommunications, Fintech, Mobile Money, Airtel Money Pay, Mobile Payments, Communities, Culture, Education, and People.
T-C-U 2	47.5%	16.7 million accounts and 5.7 million active data subscribers	Voice, bundles, data, international bundles, roaming, SMS bundles, and mobile money.
E- Commerce			
Company E-C-U 1	- (Information not readily available publically)	Over 800,000 monthly users	Online shopping mall for electronics, fashion, and groceries among others.
Company E-C-U 2	- (Information not readily available publically)	- (Information not readily available publically)	Food deliveries.

Table 2: The table above gives a bio data of the Uganda companies evaluated across the three sectors. Not much information was readily available for company E-C-U 2. This could partly be due to the fact that it has only been in operation in Uganda for only two years.

Results

3.1 Overall Results

This section details the extent to which the privacy policies of the analyzed companies meet regulatory thresholds on privacy and data protection as evaluated against the five core indicators detailed in earlier sections of this report. The study findings are as follows:

3.1.1 Kenya

Indicators	Sectors		
	Telecommunications	E-commerce	Financial Services
Existence of an accessible readable and noticeable privacy policy	The criteria in this section is if the privacy policy is public, published, noticeable, and readable. In the 2 telecommunication companies published, Company T-C-K 1 received credit for all 4 criteria, while Company T-C-K 2 received credit for 3 of the 4 evaluation criteria in this section. For Company T-C-K 2, a score was not awarded for the 'noticeable' criteria as its privacy policy was not easily noticeable.	Both companies evaluated in this sector had privacy policies with high readability scores. Both companies' privacy policies were visible on their respective website landing pages. Companies E-C-K 1 and E-C-K 2 both received scores in all 4 criteria, public, published, noticeable, readable.	Companies F-S-K 1 and F-S-K 2 both earned 3 scores for privacy policies that were publicly available, published, and readable. However, both companies had privacy policies that were not easily noticeable.
Informed Consent	A Credit score was earned for each of the categories for this indicator for both Companies T-C-K 1 and T-C-K 2. However, the privacy policy for Company T-C-K 2 did not have information on the kind of data being collected, data storage period, contact details, and rights of the data subject. Of the evaluated companies, Company T-C-K 2 earned only 4 out of 8 credit scores whereas Company T-C-K 1earned all 8 credit scores for each category.	Companies E-C-K 1 and E-C-K 2 Privacy policies scored a credit each on the categories under this indicator, however, credit score was not given on availability of contact details, data storage duration, and description of personal data being collected. 6 out of 8 and 7 out of 8 credit scores were earned respectively.	A credit score was earned for each category in this criterion for the privacy policies of Companies F-S-K 1 and F-S-K 2 with the exception of the category on data storage duration for Company F-S-K 2 the same was not highlighted. Company F-S-K 2 earned 7 out of 8, whereas Company F-S-K 1 the earned all 8 credit scores for each category.

Data collection and Third-Party Data Transfers	Third-party data sharing is highlighted in both privacy policies. A credit score is awarded for companies T-C-K 1 and T-C-K 2. One of the privacy policies indicates a list of third parties by industrial sectors whereas the other does not list third parties. Tech analysis does not show third-party listings on either website of companies T-C-K 1 and T-C-K 2. Tech analysis reveals for both that the most common third parties with whom data is shared are Google, Facebook, LinkedIn, twitter, Amplitude, Clever tap.	Companies E-C-K 1 and E-C-K 2 both mention data sharing with third parties, however, there is no indication of the type of data that will be shared nor a list of the third party companies. The tech analysis showed 22 and 30 third parties respectively for companies E-C-K 1and E-C-K 2 for each of the companies, that have not been publicly listed. The credit scores awarded for each indicator are 3 out of 4 and 2 out of 4 respectively. Technical analysis from ad trackers shows the following third parties for Company E-C-K 1 Google, AdWorld, Criteo, Facebook, RTB house, Global Site Tag, iGodigital, Adjust, New Relic and urbanairship. The following were noted for Company E-C-K 2 Adobe, Google, Facebook, Quantcast, Floodlight, DoubleClick, Criteo, Hotjar, Segment, LinkedIn , Facebook Connect, CloudFlare, LegitScript, clarity.ms, Klaviyo, and Google Analytics.	The privacy policies for companies F-S-K 1 and F-S-K 2 provide for third-party data sharing, each respectively lists third parties by service provided, sector, and/ or institution. For this, a credit score is earned. Tech analysis lists 3 third parties for Company F-S-K 1 and none for Company F-S-K 2. Credit score of 2 out of 4 is earned for both evaluated polices for each category in this indicator. Technical analysis indicated the following third party ad trackers for Company F-S-K 1 Google AdWords Conversion, Twitter Advertising, Customer Interaction (Smartlook), Google Tag Manager, Facebook Connect, Google Analytics, Huawei Mobile Services (HMS) Core.
Practice Robust Data Security	Privacy policies highlight maintaining the privacy of their customers, a credit score is earned for this. The privacy policy of Company T-C-K 1 notes mechanisms used to ensure security and privacy whereas the privacy policy of Company T-C-K 2 does not. The SSL server score on both websites differs in scoring. Company T-C-K 1 scores an A which meets the threshold for data security whereas Company T-C-K 2 scores B which is below the data security threshold. Company T-C-K 1 earns 3 out of 3 credit scores whereas in contrast Company T-C-K 2 earns 1 out of 3 for each category in this indicator.	Companies E-C-K 1 and E-C-K 2 both highlight public commitment to ensure that necessary measures are taken to ensure privacy and security, a credit is earned for this however, the measures to be taken are not prescribed. In addition, The Tech analysis shows a low SSL Server score for both websites the grade on each respectively indicating B and D which is below the required threshold of A to meet the provisions for data security. 3 out of 3 credit scores is awarded on the evaluation of Company E-C-K 1 whereas 1 out of 3 is awarded for Company E-C-K 2 for each category in this indicator.	Companies F-S-K 1 and F-S-K 2 privacy policies make a public declaration to take all necessary measures to ensure privacy and security of their customer's information, for which a credit score is earned. SSL Server scores are respectively graded as A and A+ which meets the website data security threshold. Company F-S-K 1 earned 2 out of 3 credit scores on the evaluation whereas Company F-S-K 2 earned 1 out of 3 for each category in this indicator.
Accountability	No transparency report is available for the year in review on either website. Credit score on accountability is not given for either Company T-C-K 1 or Company T-C-K 2.	No transparency report for the year is available on either website. Credit score on accountability is not given for Company E-C-K 1and Company E-C-K 2.	No transparency report for the year in review is available on either website. A credit score on accountability is not given for Company F-S-K 2 or Company F-S-K 1.

Table 3: The table above details the findings of the 6 Kenyan businesses analyzed in the telecommunications, e – commerce, and financial services sectors, respectively in each of the five core indicators: existence of an accessible, readable and noticeable privacy policy; informed consent; data collection and third – party data transfers; practice robust data security, and accountability.

Sectorial Compliance Scores for Kenya

The overall percentage compliance scores in the five core indicators (detailed in prior sections of this report) for the businesses analyzed in all three sectors of interest is shown in Figure 1. The highest scores observed were in indicator of public, publishable, and readable privacy policy, 75%, and the lowest across the board were observed on the accountability, 0%, indicator. The informed consent indicator had an overall compliance score of 67%; the data collection and third-party data transfer indicator, 63%, and the data security indicator, 61% compliance.

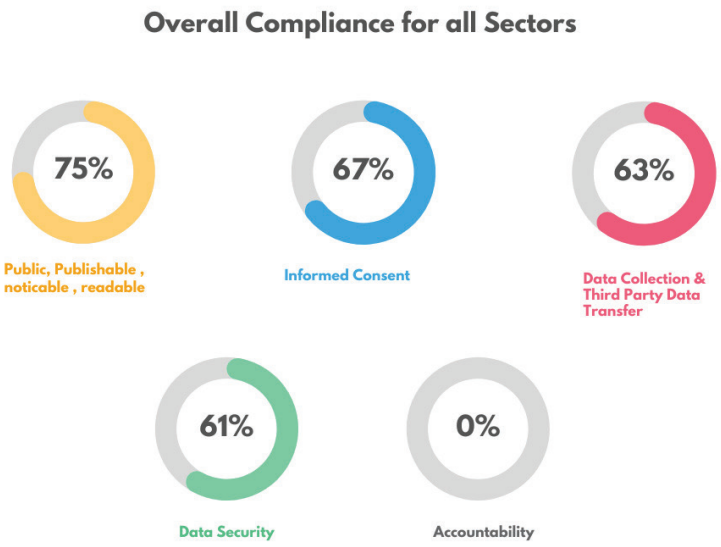


Figure 1: The figure above details the findings of the analysis on compliance of the 6 – businesses selected for the study. The highest scores observed were on criterion of public, publishable, and readable privacy policy (75%) and the lowest across the board were observed on the accountability (0%) criteria.

On a sectoral level, the compliance scores of the businesses in the financial services sector mirrored the trend from the overall scores with the highest average percentage score observed for the existence of a public, publishable, noticeable, and readable privacy policy indicator (75%) and the lowest average percentage for accountability (0%). Data collection and third-party transfer as well as data security indicators had compliance scores of 50%. The informed consent indicator had a compliance score of 70%.

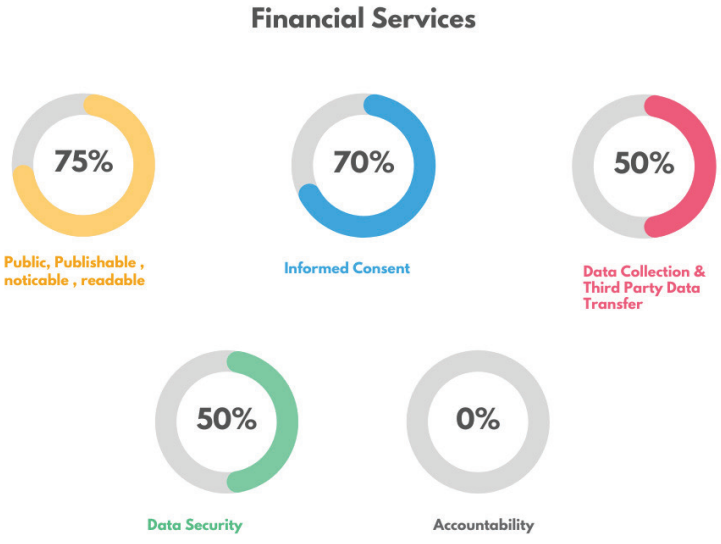


Figure 2: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the financial services sector in each of the five core indicators. The scores in the financial services sector mirrored the trend of the overall compliance scores with the highest scores observed in the existence of public, publishable, and readable privacy policy (75%) indicator and the lowest in the businesses analyzed observed on the accountability (0%) indicator.

In the e-commerce sector, the highest average compliance, was observed for the informed consent indicator scoring at 81%, followed by the existence of a public, publishable, noticeable, and readable privacy policy indicator (75%), and the lowest for the accountability indicator (0%). Compliance scores for the data security indicator, 50%, and the data collection and third – party data transfer indicator, 63%.

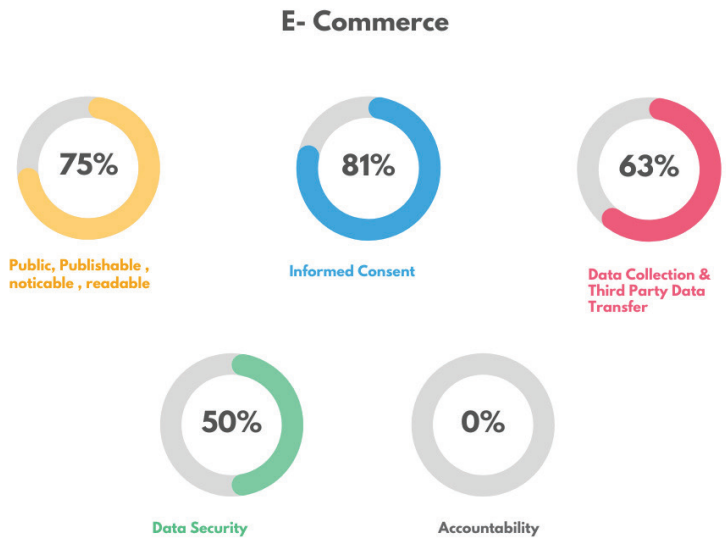


Figure 3: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the e – commerce sector. The scores in the e - commerce sector mirrored the trend of the overall compliance scores and the scores observed in the financial sector in that the highest scores observed were for Informed consent (81%) indicator and the lowest in the businesses analyzed observed on the accountability (0%) indicator.

Deviating from the common trend, the businesses analyzed from the telecommunications sector had the highest compliance score for the indicator for data collection and third-party data transfer (75%). The scores for the other four indicators are as follows: existence of an accessible, readable, and noticeable privacy policy, 70%; informed consent, 30%; data security, 22%, and accountability, 0%.

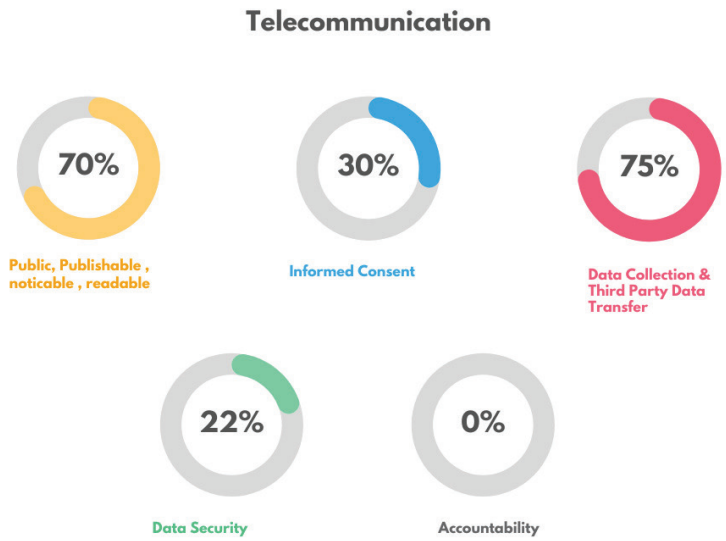


Figure 4: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the telecommunications sector. The analyzed businesses in the telecommunications sector had the highest compliance score for the indicator for data collection and third-party data transfer (75%). The scores for the other four indicators are as follows: existence of an accessible, readable, and noticeable privacy policy, 70%; informed consent, 30%; data security, 22%, and accountability, 0%.

3.2 Analysis of Findings for Kenya

3.2.1 Overall Analysis

Overall, each sector scored highest in a different indicator.The financial services sector scored highest (75%) in the existence of public, publishable, noticeable and readable privacy policies, the e-commerce sector in the informed consent indicator (81%), and the telecommunication sector in data collection and third party data sharing (75%). This suggests that the companies analyzed understand the importance of protecting their customers' personal data and that they have some data protection practices in place. Comparatively, the compliance score for the informed consent varies from sector to sector, with the highest score recorded in the e-commerce sector (81%) and the lowest in telecommunication (30%). This may indicate the need for standardized national guidelines for privacy policy statements for companies in the private and public sectors. These guidelines would clearly outline which parameters must be included in every privacy policy created by an organization. Sector specific data protection guidelines would also significantly influence the information required in a privacy policy. This would be in line with the provisions of section 26 and 27 of the DPA. Further, section 71 mandates the cabinet secretary for the ministry of ICT to develop guidelines or codes of practice that give effect to the Act.

Compliance scores for the data collection and third-party data transfer indicator also vary from sector to sector. This is due to a lack of clarity of the information provided by the privacy policies of the companies analyzed on the type of personal data shared. Only one of the analyzed companies, from all three sectors, provides information on data storage limitations. Two of the six companies provide information on the type of personal data that will be collected, and five of the six companies state the purpose for which data is to be collected.

Notably, all of the companies analyzed across the three sectors received a compliance score of 0% for the accountability indicator. Clearly, the practice of publishing a transparency report is not common to any of the sectors. A transparency report serves the purpose of highlighting digital and data governance enforcement measures. This document, shared with the public, builds trust and openness between businesses and their customer base. From the assessment, the need for transparency reports needs to be better championed by the ODPC.

Across the three sectors reviewed, the percentage scores as indicated in figure 1 are above 50% for all four indicators with the exception of the accountability indicator. This is indicative of a trend in trying to comply with existing data protection regulations, specifically the DPA. However, it is also indicative of the gaps that exist in terms of compliance and implementation of data protection rights particularly as they relate to ensuring the exercise of the rights of the data subjects, data processing practices as relates to storage, and third party data transfer. These key areas must be re-evaluated across all three sectors in order to strengthen implementation and compliance processes within the sectors developing best practices.

3.2.2 Sectoral Analysis.

Financial Services

High compliance scores were recorded for both companies analyzed in this sector. 75% is recorded for the existence of a privacy policy indicator and 70% for the informed consent indicators respectively. The high scores for these indicators suggests the development of some data protection practices by the sector and adherence to data protection laws and regulations by the companies analyzed, particularly in ensuring data subject rights are protected in the processing of personal data. Clarity is however, required with respect to data storage and the kind of personal data being collected, as this information is either not provided or is not substantively elaborated in the companies' privacy policies.

For the financial services sector personal data is not only collected for access to services, personal data is also utilized as a means of authentication. It is therefore important for the financial sector to ensure that data subjects i.e. customers and subscribers are able to adequately exercise their rights, for example the right to update, correct, delete or erase personal data.[50] Contact information is required on how best data subjects can get in touch with the company to enable exercise of these rights. Clear protocols on access to information, updating, correction, deletion and erasure requests must also be clearly communicated within the privacy policy. This could involve creating links on the website landing page to facilitate the exercise of these rights and or direct communication with customer care, or the development of a data protection call desk to facilitate exercise of the respective rights.

The lowest compliance scores were recorded for data collection and third-party transfer (50%), data security (50%), and accountability (0%). Of the two companies assessed, the privacy policies clearly indicate that data collected will be shared with third-parties. However, the data subjects are not notified of the third parties with whom their data will be shared. Technical analysis of the companies' website and applications indicates the presence of ad trackers and third-party cookies from online advertising companies with whom data is shared – most commonly Google and Facebook. Other ad trackers indicative of this party data sharing include, CleverTap, MixPanel of the two companies assessed in this category, both companies i.e. Company F-S-K 1 and Company F-S-K 2 reflected good security header results, both were respectively graded A. An A score and above is an indication that the website has been properly set up, i.e. the website is less susceptible to cyber-attacks because the web server is correctly installed, trusted and cannot give the users any errors. The SSL server test is primarily designed to confirm validity of a web address. Accountability holds the lowest score (0%) due to the lack of a transparency report.

This is indicative of how laws and policies affect privacy and security. Currently there are no national regulations make a privacy policy a legal requirement. The same applies to transparency reports. Where regulatory requirements are made for compliance through a Privacy Policy or Accountability report, it is more likely that the laws will be adhered to and a practice of well drafted privacy policies and transparency reports will be developed, not only in the financial sector but across all sectors. Compliance with data protection laws i.e. the DPA requires further operationalization through ensuring that relevant guidelines on privacy policies and transparency reports are developed not only to strengthen compliance with the Act but to also ensure data protection rights for users are upheld, and keeping sector players accountable though out their data processing operations.

50 These rights are provided for under section 26 of the DPA.

ii) Telecommunications

For companies T-C-K 1 and T-C-K 2, from the telecommunications sector, the data collection and third-party data transfer indicator have the highest compliance score (75%), closely followed by the indicator for the existence of a privacy policy that is noticeable, public, published, and readable (70%). The high compliance score on data collection and third-party data transfer is primarily attributed to Company T-C-K 1. Whereas Company T-C-K 1 demonstrated a high regard for data collection and third-party data transfer protection protocols, meeting the majority of the requirements of the category, Company T-C-K 2 failed to provide adequate information on data transfer, e.g., the type of data collected, the third parties with access to this data, etc., which may be indicative of poor data protection practices within this company. The poor practice further likely indicates that the subscribers and customers of Company T-C-K 2 are likely to be easily exposed to data breaches and cyber security threats, further, the customers and subscribers are not aware of their rights as indicated in the DPA and have no means of exercising their data protection rights or their right to privacy and security as prescribed in the constitution of Kenya. Company T-C-K 1 holds twice the number of subscribers as Company T-C-K 2 and operates in approximately 10 countries, this exposure could also be indicative of why they are more compliant with data protection regulations not only in Kenya but in the respective countries within which they operate as they are bound by the data protection laws of those countries. In contrast however, Company T-C-K 2 operates in 18 countries across Asia and Africa yet lacks a privacy policy indicative of good data protection practices per the indicators of the evaluation.

Informed consent and data security had low compliance scores, 30% and 22%, respectively. The low scores are an indicator of the companies' practices, and perhaps priorities, when it comes to protecting their customers' personal data and informing them of their data rights. Of the two companies assessed, Company T-C-K 2, failed to provide for the rights of the data subject, meaning, the privacy policy had no provisions on the subscribers and customer's rights to access their data, update, and delete data and the right to object data processing and withdraw consent. Consequently, there is no indication of how data subject's rights could be exercised. This is an indication of a need to review the privacy policy to reflect the provisions of the DPA especially as they speak to data subjects' rights and third party data sharing. The telecommunications sector holds a wider repository of personal data owing to the services provided that a majority of the population rely on, not only in terms of communication, but in association with financial services. Because of this interlink, privacy policies must reflect the provisions of data protection laws.

The technical analysis relating to the SSL server tests graded companies T-C-K 1 and T-C-K 2 respectively, indicating that that the websites were less likely to be vulnerable to cyber-attacks and data breaches through web address errors as the website was adequate set up. When looking at data collected Company T-C-K 1 provided information on the kind of data being collected i.e. unique device details which was similar to that revealed in the technical analysis. Company T-C-K 2 failed the test as the technical analysis did not reveal personal information collected, however the privacy policy indicated it did not give information collected, further the privacy policy did not highlight the kind of data being collected. Knowledge of the type of data collected informs consent to data processing and also informs how data subjects can exercise their rights. Where these parameters are not met, companies are likely to be exposed to sanctions by the office of the ODPC, the regulatory authority. Further, it leaves the subscribers open to data breach and cyber security threats that could result to cases of fraud, identity theft, phishing, malware and password attacks. Similar to the financial service sector and e-commerce, accountability holds zero percentage as neither of the assessed companies published a transparency report. A transparency report especially for the telecommunications sector would be beneficial in addressing areas where compliance to data protection laws has been strengthened. In the event of any data breaches the report would give an opportunity to elaborate of mitigating measures and reinforced security measures put in place to avoid future breaches. This would further build trust with its subscribers and provide ways in which they could participate in reinforcing their rights as data subjects. Across the sector, transparency reports ought to be established as common practice.

E-Commerce

In the companies analyzed in the study, the highest compliance scores were observed for Informed consent (81%), the existence of a privacy policy (75%), followed by the data collection and third-party data transfer indicator, (63%). These scores indicate good data protection practices as it pertains to data transfer and informing users of their data rights. However, both companies could increase accessibility to the privacy policy on their website by ensuring that the privacy policy is clearly labeled as a privacy policy and is reflected on the top tab of the landing page as opposed to the bottom of the landing page where it is in fine print and often hard to find as was the case for both Companies E-C-K 1 and E-C-K 2. Data security holds a 50% average and accountability holds 0 % indicative of the need for better practice in ensuring the security of their platforms from possible breaches and cyber-attacks. Notably of the two companies assessed, Company E-C-K 2 did not indicate the purpose for which the data is collected. E-C-K-1 and E-C-K-2 both provided for data subject rights however these rights are given under certain circumstances which have not been clarified in the respective privacy policies. The lack of clarity in these provisions in the privacy policy is indicative of a need to improve and revise data protection practices for the company. Data subjects' rights influence consent of its consumers as they are not fully aware of how their data is being used, noting that it is the responsibility of the data collector to ensure

that the data subject is well informed of existing rights and any underlying caveats before consenting to the processing as provided under section 29 of the DPA.

On data security, both of the companies analyzed in the study mention their commitment to protect and secure client data. However, neither company gives information on the measures and steps that will be taken to protect and secure client data. Indicating measures not only shows compliance but also demonstrates accountability and transparency on the part of the company in its data processing activities. This is also applicable to third-party data transfer; highlighting the third parties who will have access to the data enables the data subjects to exercise their rights.

The low percentage score on data security is also informed by the low SSL Server grade for both websites, the grade on Companies E-C-K 1 and E-C-K 2 respectively indicating B and D which is below the required threshold of A to meet the provisions for data security. This means that the company's websites are more vulnerable to cyber-attacks and data breaches and also showing that the requirement on data security as provided under section 29(f) and the principle of security on ensuring security and confidentiality have not been met. These further exposes consumers to data breaches, instances of fraud, identity theft and other arising cyber security threats.

The accountability score in this sector also remains at 0% as there is no published transparency report by either of the companies assessed. Developing standard practice in publishing transparency reports remains relevant not only for this sector but for all the sectors evaluated. For this particular sector, the accountability reports would improve and strengthen compliance with the data protection laws, keeping the companies accountable not only to the relevant regulatory authorities but also to its consumers.

3.1.2 Uganda

Indicators	Sectors		
	Telecommunications	**E-commerce**	**Financial Services**
Existence of an accessible readable and noticeable privacy policy	Under this indicator, both companies T-C-U 1 and T-C-U 2 earned credit scores for their policies being public and publicized. None of companies T-C-U 1 and T-C-U 2 scored a credit for the readability parameter as they both were rated at 'okay'. Whereas Company T-C-U 1 earned a credit score for having a noticeable policy, Company T-C-U 2 did not as its policy was printed in fine print. Conclusively, Company T-C-U 1 earned three out of the four parameters assessed while Company T-C-U 2 earned two out of the four.	Both companies E-C-U 1 and E-C-U 2 earned credit in the evaluation criteria of noticeability, and having published and publically available privacy policies. Again both companies E-C-U 1 and E-C-U 2 failed on the readability parameter with an 'Okay' evaluation. Both companies in this sector earned three out of the four parameters assessed.	Whereas both companies F-S-U 1 and F-S-U 2 in this sector had noticeable, public and published privacy policies and earned a credit score for the same, both failed on the readability evaluation criteria like other Ugandan companies assessed for this report. Both companies F-S-U 1 and F-S-U 2 earned three out of the four parameters assessed.

Informed Consent	Both companies T-C-U 1 and T-C-U 2 earned only two credit out of the eight parameters assessed. These were for their privacy policies indicating the purpose of the data collected from the data subjects and type of data collected. Companies T-C-U 1 and T-C-U 2 did not indicate their contact addresses, the duration for which data is retained, as the well as the rights to: access the data held on the data subject, erase or update the data, restrict data usage and to withdraw consent to data usage. There is need to establish whether this is a sector specific challenge, especially in the telecommunication sector.	Under this assessment, Company E-C-U 2 earned all the eight credits, while Company E-C-U 1 earned seven out of eight scores as its policy did not indicate the duration for which data was retained.	Whereas Company F-S-U 2 indicates the nature of personal data collected, this includes information of a private and irrelevant nature that is expressly prohibited under Section 9 of the DPPA. The same may not fall under any exceptions including the one on informed consent. Company F-S-U 1 on the other hand did not earn credit for the failure of its privacy policy to mention the nature of personal data collected or processed or specifically provide the right to update or erase personal data. Whereas Company F-S-U 2 performed fairly well in the areas of evaluation, it did not score a credit for failure to include the duration of data storage in its privacy policy. Company F-S-U 1 in total earned six out of the eight assessed parameters while Company T-S-U 2 earned seven out of the eight.

Data collection and Third-Party Data Transfers	Third-party data sharing is highlighted in both privacy policies. A credit score is awarded for companies T-C-U 1 and T-C-U 2. The privacy policy for Company T-C-U 2 indicates that personal data shall be shared within its group of companies whereas Company T-C-U 1 does not list third parties with whom they share the personal data. Even then, both companies fail on the assessment of whether the list of third parties given aligns with the trackers. Both companies do not indicate the nature of personal data they share with third parties. Tech analysis reveals for both that the most common third parties with whom data is shared are Google, twitter, Amplitude, Facebook and Appsflyer. Conclusively, Company T-C-U 1 scores one out of the four areas of evaluation while T-C-U 2 scores two out of four.	Both companies E-C-U 1 and E-C-U 2 mention data sharing with third parties in their policies. There is however no indication by Company E-C-U 1 as to the type of data that will be shared nor a list of the third party companies they share the data with, however, Company E-C-U 2 indicates the type of data that will be shared and the industries with whom your data will be shared. The tech analysis showed 16 and 21 third parties respectively for Company E-C-U 1 and Company E-C-U 2 respectively for each of the companies that have not been publicly listed. The credit scores awarded for this indicator are two out of four and three out of four for companies E-C-U 1 and E-C-U 2 respectively. Technical analysis from ad trackers shows the following third parties for Company E-C-U 1; Google, New Relic, cedexis, iGoDigital, Adjust, Facebook Login, Facebook Share, Google Admob, Google Analytics, Google Crashlytics, Google Firebase Analytics, Google Tag Manager, Urbanairship, Google Analytics, Facebook Domain Insights, Global Site Tag, and Google Conversion Linker. The following were noted for Company E-C-U 2 ; Google Beacons, Google Tag Manager, Hotjar, Facebook Connect, Google Analytics, unidentified tracker, mParticle, Adjust, Branch, AB Tasty, Amplitude, Pinterest Conversion Tracking, Facebook Signal, Adjust, Branch, Braze (formerly Appboy), Facebook Analytics, Facebook Login, Facebook Share, Google CrashLytics, Google Firebase Analytics, Instabug, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes, mParticle.	Whereas as the privacy policy for Company F-S-U 1 does not provide for third-party data sharing, Company F-S-U 2's policy provides for the same. Company F-S-U 2 provides a list of third parties they share the personal data with. While company F-S-U 1 fails on all the four assessed parameters under this indicator, Company F-S-U 2 scores two out of the four evaluated criteria. Technical analysis indicated the following third party ad trackers for Company F-S-U 1; Adobe Audience Manager, Google Adwords Conversion, SalesForce Live agent, Adobe Dynamic Tag Manager, Google Tag Manager, Adobe Experience Cloud, Adobe Dynamic Tag Management, Adobe Marketing Cloud, Omniture SiteCatalyst, Global Site Tag, Adobe Experience Cloud, AltBeacon, Appdynamics, Audience Studio (Krux), Google AdMob, Google CrashLytics, Google Firebase Analytics, Huawei Mobile Services (HMS) Core, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes, OpenTelemetry (OpenCensus, OpenTracing), Salesforce Marketing Cloud. Technical analysis indicated the following third party ad trackers for Company F-S-U 2; Adobe

Practice Robust Data Security	Under this indicator, both Companies T-C-U 1 and T-C-U 2 do not indicate the means of securing personal data and as such no credit is earned for both. The SSL server score on both websites differs in scoring. Company T-C-U 2 scores an A which meets the threshold for data security whereas Company T-C-U 1 scores B which is below the data security threshold. Both companies fail on the security header threshold. Company T-C-U 2 earns 1 out of 3 credit scores whereas in contrast Company T-C-U 1 earns no credit in this indicator.	Company E-C-U 1 and Company E-C-U 2 do not earn a credit for failing to mention the measures taken to ensure data security. In addition, The Tech analysis shows a low SSL Server score of B for websites of Company E-C-U 1 which is below the threshold to meet the provisions for data security. Company E-C-U 2 on the other hand earns a score for the same. Both companies fail on the security header parameter. Company E-C-U 1 therefore earns no credit in this indicator while Company E-C-U 2 earns one out of three indicators in this part.	Company F-S-U 1 scores three out of three credits in the areas of assessment for earning an A on the security header parameter, detailing the means of ensuring data security and scoring an A in the Tech analysis in the SSL Score. On the other hand, Company F-S-U 2 only scores two out of the three credits for compliant SSL server and security header score, while failing on one parameter for not indicating the measures adopted to ensure personal data protection. This is a great performance given the generally low assessment of other sectors in this indicator.
Accountability	No transparency report is available for the year in review on either website. As such no Credit score on accountability is not given for either Company T-C-U 1 or T-C-U 2.	No transparency report is available for the year in review on either website. As such no Credit score on accountability is not given for either Company E-C-U 1 or Company E-C-U 2 .	No transparency report is available for the year in review on either website. As such no Credit score on accountability is not given for either Company F-S-U 1 or Company F-S-U 2.

Table 4: The table above summarizes Uganda's performance per company, per sector in the five indicators of assessment as indicated above.

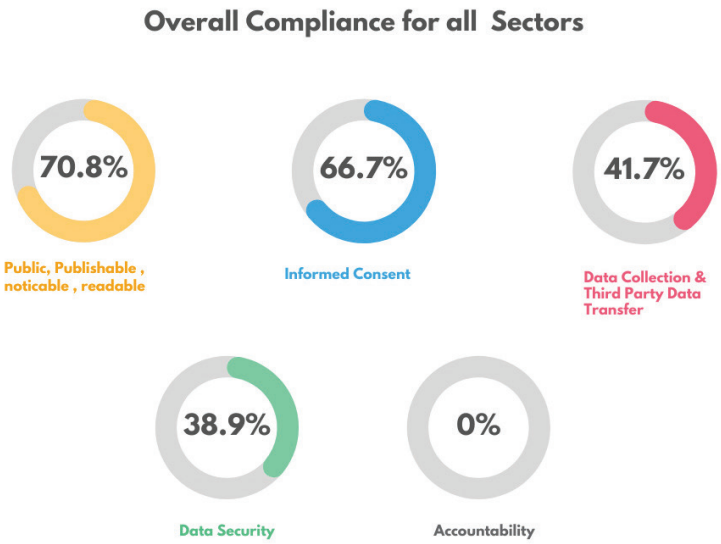


Figure 5: The chart above indicates the general sectoral performance on each of the five indicators in Uganda. It indicates the highest score of 70.8% in presence of public, noticeable and readable privacy policies, with a lowest score of 0% on the accountability indicator. The overall compliance indicator for all sectors on the informed consent indicator was 66.7% and 38.9% on data security. The companies whose privacy policies were reviewed scored below average in three areas of evaluation.

Below the report presents the illustrative performance of Ugandan evaluated companies in the different sectors; clearly marked as such.

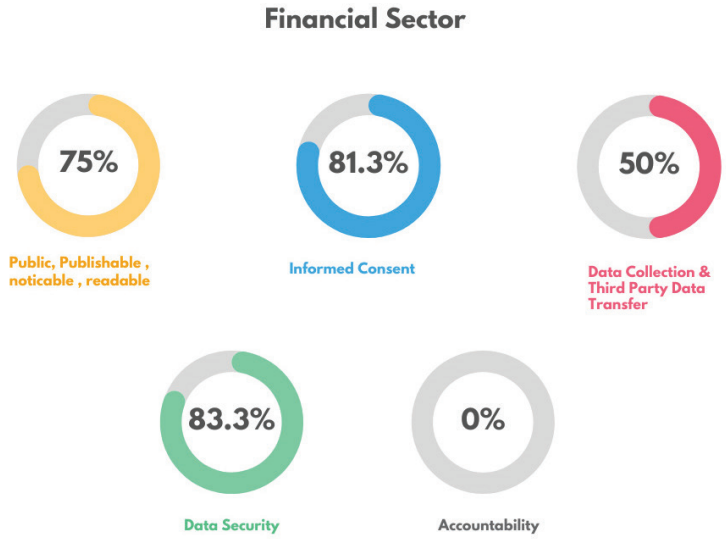


Figure 6: The chart above presents the overall performance in the financial sector. The best performance in the was recorded in the data security indicator, standing at 83.3% and the lowest in the accountability parameter at 0%. The sector scored 81.3% on the informed consent indicator, 75% on the existence of public, publishable, noticeable and readable policies and 50% on data collection and third party data transfer.

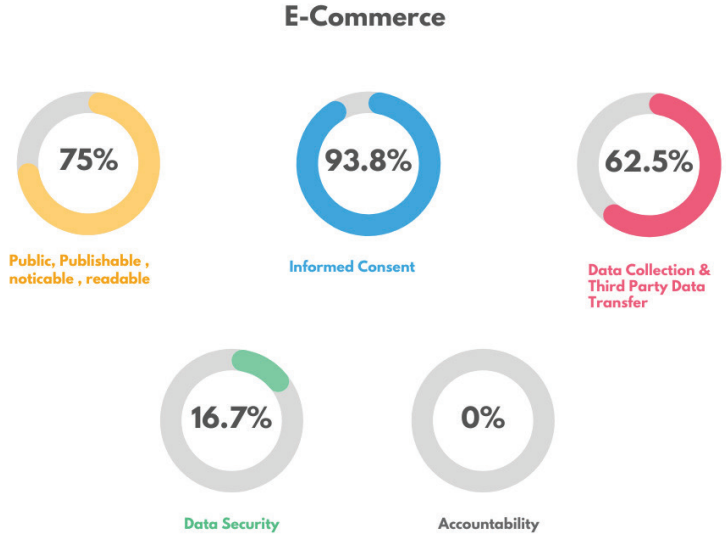


Figure 7: The chart above indicates the privacy assessment performance in the e-commerce sector. The best performance in the e-commerce sector was recorded in the informed consent indicator at 93.8%, and the lowest in the accountability parameter at 0%. The score of the existence of readable, public and publicized privacy policies stood at 75% while a below average score of 16.7% was recorded in the data security parameter.

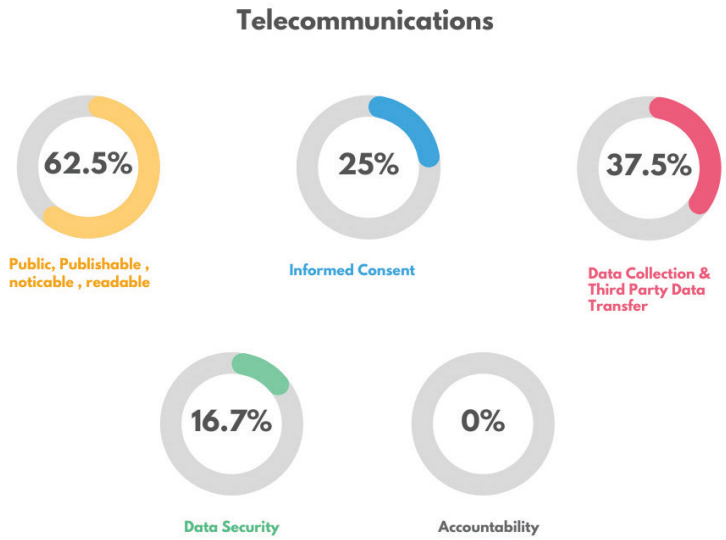


Figure 8: The chart above presents the overall performance in the telecommunication sector. The telecommunication sector generally performed poorly with a below average score in four out of five indicators. The best performance was recorded in the existence of public, readable, published and noticeable policies, at 62.5% and the lowest in the accountability parameter at 0%. The informed consent indicator scored 25%, data collection and third party data transfer had a 37.5% score.

3.3 Analysis of Findings for Uganda

3.3.1 Overall Analysis

Overall, all two sectors had the highest compliance score in the existence of a privacy policy indicator, while the financial sector scored best in the data security indicator and e-commerce in informed consent. This suggests that the different companies analyzed appreciated and implemented the various indicators assessed differently. Comparatively, the compliance score for the informed consent indicator had surprises too. Whereas very high percentages were recorded in the financial services and e-commerce sectors, telecommunication services scored as low as 25%. The low compliance score for the informed consent in the telecommunications sector is characterized by the non-compliance with most of the assessed parameters by both companies T-C-U 1 and T-C-U 2. This may call for the need to mandate companies to come up with privacy policies that reflect their legal obligations as a matter of law and not discretion. These polies should be in line with the legal protections of data subjects contained in Part V of the DPPA.

Compliance scores for the data collection and third-party data transfer indicator also vary from sector to sector with two sectors with an average and slightly good performance and one scoring below average. This is due to a lack of clarity of the information provided by the privacy policies of the companies analyzed on the type of personal data shared. Only one of the analyzed companies, from all three sectors, provides information on data storage durations. Further, companies generally did not exhaustively indicate the third parties with whom they share personal data. This lack of transparency affected the performance on this indicator.

Notably, all of the companies analyzed across the three sectors received a compliance score of 0% for the accountability indicator. Clearly, the practice of publishing a transparency report is not common to any of the sectors. This could be as a result of lack of a clear legal mandate on companies to do so. To address this, the law may need to include this indicator as part of the express obligations on data collectors, controllers, and processors.

From the overall performance of the three sectors reviewed as seen in figure 5, only two out of five indicators scored above the average score. This is concerning and is indicative of a country that is struggling to ensure adequate protection of personal data and the right to privacy. This calls for relevant stakeholders to pay keen interest on the different indicators and devise means of holding private actors accountable for the realization of the right to privacy.

3.2.2 Sectoral Analysis for Uganda

I) Financial Services

The sector generally performed well in many indicators. Except for the accountability indicator, the rest of the scores were above average. The best performance was recorded in data security, followed by the informed consent and the existence of noticeable, public and readable privacy policies respectively. There is however need to strengthen the data collection and third party transfers of data to confirm to international and domestically recognized standards.

The high levels of compliance in the financial sector in Uganda could be explained by the fact that long before the enactment of data protection legislations, financial institutions have traditionally been bound by the confidentiality principle both contractually and by the banking legal framework. The excellent performance in the informed consent and data security indicators would as such not be a surprise, especially given the profile of both companies F-S-U 1 and F-S-U 2.

One of the greatest undoing in the sector though is that company F-S-U 1 does not indicate the nature and category of personal data collected and both companies F-S-U 1 and F-S-U 2 do not indicate in the privacy policies the third parties they share personal data with. This largely contributed to the average performance in the data collection and third party sharing indicator.

Further, Technical analysis of the companies' website and applications indicates the presence of ad trackers and third-party cookies from online advertising

companies with whom data is shared as listed below: Company F-S-U 1; Adobe Audience Manager, Google Adwords Conversion, SalesForce Live agent, Adobe Dynamic Tag Manager, Google Tag Manager, Adobe Experience Cloud, Adobe Dynamic Tag Management, Adobe Marketing Cloud, Omniture SiteCatalyst, Global Site Tag, Adobe Experience Cloud, AltBeacon, Appdynamics, Audience Studio (Krux), Google AdMob, Google CrashLytics, Google Firebase Analytics, Huawei Mobile Services (HMS) Core, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes, OpenTelemetry (OpenCensus, OpenTracing), Salesforce Marketing Cloud. For Company F-S-U 2; Adobe Audience Manager, Google Adwords Conversion, DoubleClick Spotlight, Twitter Advertising, IPG MediaBrands, Adobe Dynamic Tag Manager, Adobe Experience Cloud, Google Tag Manager, Linkedin Analytics, Facebook Connect, New Relic, Omniture SiteCatalyst, Adobe Dynamic Tag Management, Adobe Experience Platform Identity Service, Adobe Analytics, LinkedIn Insights, Facebook Pixel, Appdynamics. These many trackers that are not expressly known to the data subjects water down the legal protection of the privacy of the data subject.

Both Company F-S-U 1 and Company F-S-U 2 reflected good security header results of 'A'. This is an indication a secure website that is less susceptible to cyber-attacks. Of the three parameters of data security, Company F-S-U 2 did not earn a credit for the failure to indicate the means employed to secure personal data. Otherwise, both companies earned a credit for all the other parameters. That could explain why data security was its highest percentage score of all indicators in this sector.
As discussed above, the accountability score of 0% in the sector is not surprising given the lack of a legal obligation on companies to enact privacy policies that reflect the current legal framework. It is thus possible that companies could still be relying on voluntary initiatives in the form of policies adopted before the coming into force of the DPPA and the DPPRs. There is therefore the need for companies to legally be obliged to take initiatives that ensure the observance and respect of the core tenets of the right to privacy and personal data protection.

II) Telecommunications

Given the large volume of personal data that telecommunications Companies T-C-U 1 and T-C-U 2 hold given their profiles and market share, the performance of this sector is particularly concerning. As indicated above, the sector scored below average in four out of 5 indicators. The country analysis profiles both Companies T-C-U 1 and T-C-U 2 as big multinational companies with big market shares and should be expected to take issues of legal compliance especially with data protection and the right to privacy seriously.

The sector scored 62.5% on the indicator of existence of public, published, readable and noticeable privacy policies. This was the highest score in the five indicators assessed. Like other sectors, the lowest score of 0% was recorded in the accountability indicator. Companies T-C-U 1 and T-C-U 1 both recorded 25% on the informed consent indicator, 37.5% on the data collection and third party transfers, and 16.7% on the data security indicator. Company T-C-U 2 did not earn a credit score in many evaluated parameters. Its policy was for example not noticeable as it is printed in fine print, and like Company T-C-U 1 had an okay score on readability of the privacy policy which did not earn a credit score. In addition, Company T-C-U 2 did not indicate their contact details in the privacy policy and only scored one credit for indicating the purpose of data collection out of the eight parameters assessed under the informed consent indicator. The performance of Company T-C-U 1 in the informed consent indicator was also generally poor with credit earned only for mentioning the nature of personal data collected and the purpose for which it is collected. On the data security indicator, Company T-C-U 1 failed all the three areas of assessment while Company T-C-U 2 earned one credit for an A SSL assessment. The sector however did not have as many trackers as the financial services and e-commerce sectors.

The above performance is indicative of a sector whose privacy policies do not align with the legal provisions in the DPPA and the DPPRs to the detriment of the data subjects. As indicated in the market share and number of subscribers above, telecommunication services offer a wide range of services as indicated above and as such key players should urgently reflect on the need for compliance with the legal framework on data protection. This would involve the NPDPD's office taking a keener interest in the privacy policies and practices of private actors to ensure that they reflect the legal obligations of the state.

III) E-Commerce

The e-commerce sector performed well in tree out of five indicators evaluated. The highest score was recorded in the informed consent indicator (93.8%), followed by the existence of noticeable, public, published and readable privacy policies (75%), the data collection and third party data transfer indicator scored 62.5%, data security at 16.7% and accountability at 0%. The rather good performance of the e-commerce sector compared to the other sectors was largely attributed to the excellent performance of Company E-C-U 2 in many of the parameters evaluated. Company E-C-U 2 failed on few parameters such as readability of its privacy policy, failing the security header score, the SSL server grade score and not mentioning the data protection measures in its privacy policy. Of all companies assessed in Uganda and Kenya, company E-C-U 2 had the longest policy with approximately 6037 words. This could point to the same being comprehensive. Company E-C-U 2 which has only been operating in Uganda for two years scores highly many indicators as compared to companies across the sectors that have been operating in Uganda for a longer period of time.

Technical analysis from ad trackers shows the following third parties for Company E-C-U 1; Google, New Relic, cedexis, iGoDigital, Adjust, Facebook Login, Facebook Share, Google Admob, Google Analytics, Google Crashlytics, Google Firebase Analytics, Google Tag Manager, Urbanairship, Google Analytics, Facebook Domain Insights, Global Site Tag, and Google Conversion Linker. The following trackers were noted for Company E-C-U 2: Google Beacons, Google Tag Manager, Hotjar, Facebook Connect, Google Analytics, unidentified tracker, mParticle, Adjust, Branch, AB Tasty, Amplitude, Pinterest Conversion Tracking, Facebook Signal, Adjust, Branch, Braze (formerly Appboy), Facebook Analytics, Facebook Login, Facebook Share, Google CrashLytics, Google Firebase Analytics, Instabug, Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes, mParticle. These as discussed above water down the realization of the right to privacy for data subjects.

Like with the other sectors discussed above, there is need for more conformity with the law on accountability, data security, data protection and data sharing with third parties as well as other indicators.

As mentioned in the background of this report, Uganda had in 2021 launched a similar study; in the section below, this report highlights the emerging trends by comparing the previous findings with the current ones.

4.0 The 2021 vis-à-vis the 2022 Privacy Scorecard for Uganda: A comparative analysis

In 2021, Unwanted Witness launched a Privacy Scorecard report that presented findings from seven sectors including insurance, telecommunication, banking, finance, government, health, and e-commerce. A total of 33 entities were evaluated. The 2022 study narrowed down the scope to three sectors and a total of six companies were evaluated in Uganda. This introduction highlights some of the methodological differences between the two privacy score cards. Because of this, the comparison considered only findings from similar sectors that were assessed in both years.

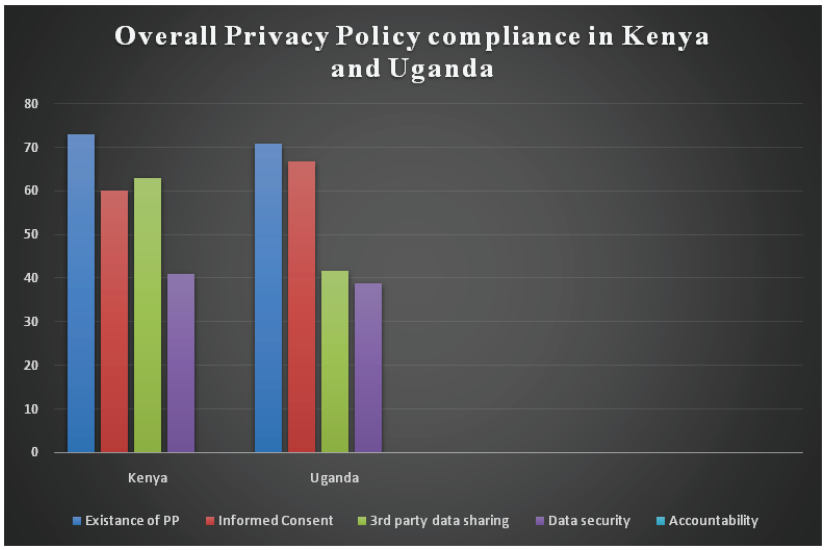
Furthermore, but connected to the methodological differences, the indicators assessed in the two reports also varied in some respects. The 2021 report was based on the following indicators: practice robust data security, complies with privacy best practices, gives information to data subjects, mentions 3rd party to share personal data with, mention quantity of information shared and with whom, which broadly represents in some respects the informed consent, data security and data collection and third party sharing. The 2022 report builds onto this but in addition to the three indicators mentioned above, assesses compliance with existence of noticeable, public, published and readable privacy policies and the accountability indicator. These are also assessed in more details with more parameters evaluated under each indicator per sector. These methodological differences make it difficult to have an objective assessment of progress or lack from the two reports. However, this report indicates a few conclusions, below, bearing in mind these limitations.
In the 2021 Privacy Scorecard report, the leading parameter was the existence of Robust data security at 66%; followed by compliance with privacy best practices at 54%; whether information was given to data subjects at 35%; whether entities mentioned the third-parties with whom they shared personal data at 19%; and lastly, whether they mentioned the quantity of information shared and with third-parties at 0%.

According to the 2022 Privacy Scorecard, the leading parameter was the existence of public, publishable, readable and noticeable privacy policy at 70.8%. This was followed by the informed consent indicator at 66.7%; data collection and third party sharing at 41.7%; data security at 38.9%; and lastly the accountability indicator at 0%. As mentioned above, again due to methodological differences, not many conclusions can be drawn from these figures at this stage.

From the sectoral performance analysis, three of the sectors evaluated last year have been assessed in this 2022 Privacy Scorecard report. These are the telecommunication sector, the e-commerce and the financial services sector. According to the 2021 Privacy scorecard report, the most compliant sector was social security which scored 80%. This was followed by the e-commerce sector at 50%; the financial sector at 36%; and the telecommunication sector at 35%. In 2022, the most compliant sector is the financial sector at 57.9%; followed by e-commerce at 49.6%; and the least complaint is the telecommunication sector at 28.3%. These figures indicate that nothing much has changed in one year, even with the differences in methodology. This could make sense given the fact that the policies reviewed may not have changed within a year, and therefore the practices too could not be expected to be different. The performance rank aside, the e-commerce sector maintains almost the same performance score, of approximately 50%, with the telecommunication sector being the least complaint in both years. Below the report considers the comparison between Kenya and Uganda in the 2022 Privacy scorecard.

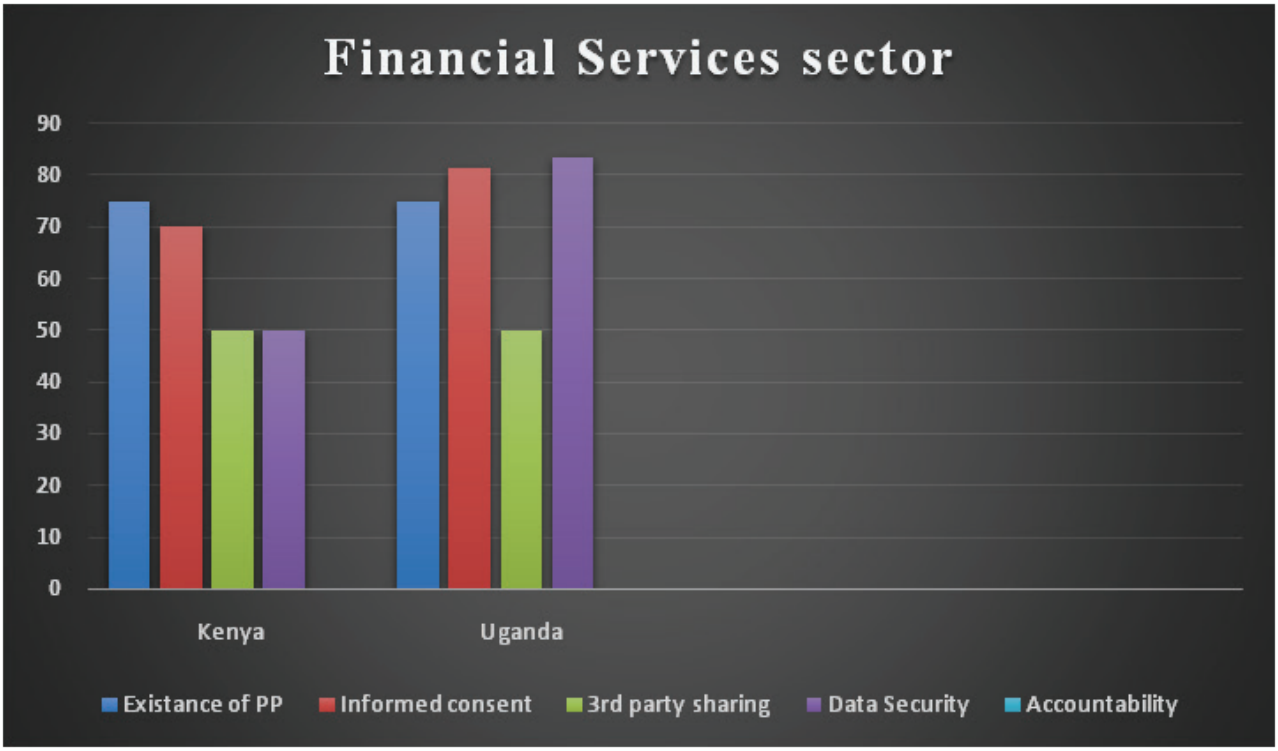
5.0 The 2022 Privacy Scorecard: A comparative analysis between Kenya and Uganda

Before the conclusion and recommendations, the 2022 Privacy Scorecard for Kenya and Uganda makes a comparison between the findings regarding personal data protection in both countries. This is done by comparing the overall compliance assessment and the sector specific performances. The chart below presents the overall compliance assessment evaluation for all sectors reviewed in Kenya and Uganda.



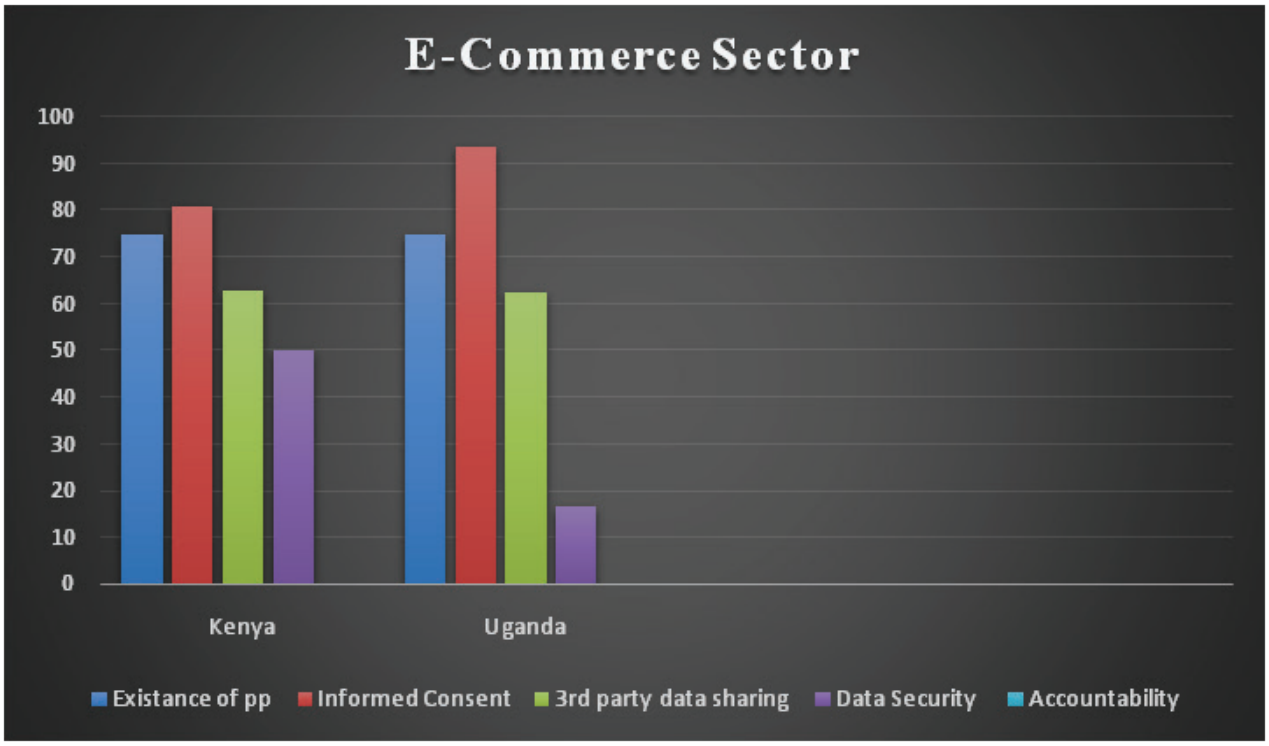
As indicated in the chart above, although Kenya (73%) performed slightly better in the existence of public, published, readable and noticeable privacy policies, as compared to Uganda (70.8), the difference is negligible. Uganda scored a higher percentage score (66.7) on the informed consent indicator, with Kenya (60%). There was a big difference on the data collection and third party data sharing with Kenya (63%) scoring higher than Uganda (41.7) whose score was below average. Both Kenya and Uganda scored below average on the data security indicator at 41% and 38.9% respectively. Lastly both countries scored a 0% on the accountability indicator.

The overall compliance of Kenya stood at 47.4% with Uganda closely following at 43.6%. This is an indication that a lot has to be done to ensure privacy policies adhere to the legally acceptable parameters of personal data protection. This could be achieved if this is taken as a legal obligation rather than a matter of charity. Below the report reviews the sector specific performances in both countries.



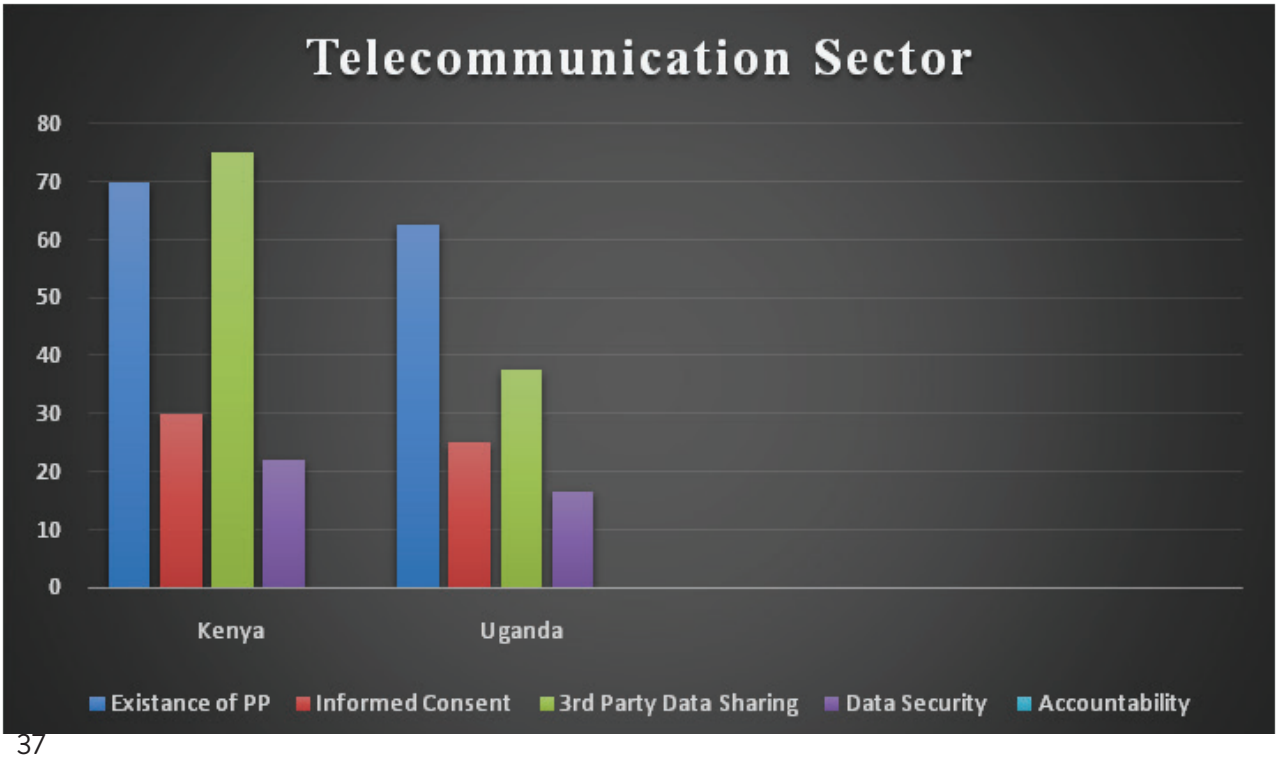
In the Financial services sector, both Kenya and Uganda scored 75% and 50% on the existence of public, publishable, noticeable and readable privacy policies and data collection and sharing indicators respectively. On the other indicators, both countries had high scores for the informed consent at 70% and 81.3% for Kenya and Uganda respectively. On the data security indicator, Kenya scored an average performance of 50% while Uganda scored an 83.3%. Both countries scored 0% on the accountability indicator.

Overall, Kenya scored 49% in the financial services sector with Uganda scoring 57.9%. The slightly better performance by Uganda could partly be explained by methodological difference since Uganda's sample space included only Tier 1 biggest banking financial institutions with regional and international presence and have been in the sector for many decades. This is as compared to Kenya which had one company from Tier 1 and another from mid-Tier 2.



In the e-commerce sector, both Kenya and Uganda scored 75% in the existence of public, published, noticeable and readable policies. On the informed consent indicator, Kenya had an 81% score as compared to the 93.8% Ugandan rating. On the data collection and third party sharing indicator, Kenya had a 63% score compared to Uganda's 62.5% performance. The greatest difference was in the data security indicator with Kenya 50% against Uganda's 16.7%. Both countries scored 0% on the accountability indicator.

In the overall performance for the e-commerce sector, Kenya stood at 53.8% while Uganda stood at a 49.6%. This is performance is indicative of a situation that is not much different in the two countries.



In the telecommunication sector, Kenya scored higher scores in the four parameters of assessment, with the exception of the accountability indicator where both countries scored 0%. Kenya scored 70% on the existence of public, publishable, noticeable and readable privacy policies, against Uganda's 62.5%, 30% on the informed consent indicator, against Uganda's 25%, 75% on the data collection and third party sharing indicator, against Uganda's 37.5% and 22% on the data security indicator, against Uganda's 16.7%.

The telecommunication sector had the lowest scores in both Kenya (39.4%) and Uganda (29.2%). This is concerning given the large volume of data that telecommunication companies hold in both countries. The second lowest parameter score, after the accountability indicator where all sectors and countries stood at 0%, being in data security for both countries is equally a cause for alarm. The regulators in both countries need to devise means of making private actors accountable for the realization of the right to privacy for personal data in their possession.

Conclusion

For data controllers or processors to be entrusted with handling personal data they must illustrate capacity to comply with the applicable laws in the countries. The rights of a data subject should be adequately provided for in the companies' privacy policies so that they can feel comfortable when sharing their personal data. This should not be taken as a matter of charity but a legal obligation. Privacy policies play a vital role in illustrating to data subjects that the platforms that they share their information with can be trusted and that the procedures put in place by these companies will protect their personal data, in accordance with the law.

It is also important that although, Kenya performed slightly better than Uganda, the abuses relating to personal data protection in both countries are largely the same. As a matter of fact, the performance difference was small. There is thus a call on both countries to benchmark best practices internationally and in the region to ensure better personal data compliance by companies through appropriate privacy policies.

This study's findings indicate that there is an understanding by business entities on the importance of protecting users' data. All the companies analyzed had at least some measures in place to protect the personal data of its users. Across all the sectors analyzed, our findings showed that data processors need to put greater effort to ensure all appropriate measures are employed to protect personal data from misuse, loss, theft, or unauthorized action. Failure to do so can result in malicious interference of users' personal data by cybercriminals. One way of achieving this could be by the legal framework making it imperative for all undertakings that collect or control personal data to have in place privacy policies that conform with the legal framework. Similar obligations have been seen in other legislations in Uganda such as the Employment Act, 2006 and the Persons with Disabilities Act, 2019.

Recommendations

a. General Recommendations

Based on the study findings from the evaluation of the privacy policies of the six selected companies in Kenya and Uganda, the following recommendations are made to strengthen data protection practices in business across all sectors:

- Companies should be mandated by law to adopt privacy policies that conform to the data protection legal frameworks. This could call for amendment of existing privacy policies to ensure compliance.
- Companies that process users' personal data should be transparent about their practices and inform users about how they handle their personal data through a prominently displayed and sufficiently noticeable privacy policy.
- Companies should include in their privacy policies a detailed and easily understood information that specifies the type of data being collected, the duration of data storage, contact information, and the rights of the data subject. This not only informs the data subject about the processing of personal data but also allows them to decide whether or not to consent. The data collected should also relate to only that that is legally allowable.
- Data transfers to third parties must be mentioned in the privacy policy to ensure that the data transferred between the company and a third party, where the transfer is necessary, is secure, the data subjects are fully informed, and the purpose and parameters are adequately explained.
- The inclusion of security measures in the company's privacy policy demonstrates its commitment to protecting sensitive information. The privacy policy should outline the physical, technical, and procedural safeguards that comply with applicable legal and technical standards. The robust security measures outlined should correspond with actual security procedures.
- Businesses across all sectors should be sensitized to the importance of a transparency report as it is not only indicative of their compliance with data protection regulations, but also of their transparency and accountability in demonstrating measures that have been implemented for securing

data and mitigating any security breaches.
- Companies with qualifications on data protection rights should ensure that the same are compliant with the laws.

b. Sectoral Recommendations

The recommendations below are tailored to each of the evaluated sectors, in line with the identified gaps from the analysis described in prior sections in this report:

i. The Financial Services

The following recommendations should be implemented to ensure that businesses in the financial services are fully compliant with laws pertaining to the protection of their customers' data:
- Companies should regularly update their privacy policies and Standard Operating Procedures (SOPs) to align with the provisions in the laws in both countries and data protection regulations, especially those that relate to the processing of personal data.
- Companies in the financial sector should make it standard practice to conduct regular internal privacy impact assessments to evaluate the vulnerability of operating systems to cyber-attacks and data breaches. A transparency report should then be published highlighting security measures that have been taken and implemented to ensure the privacy and security of its consumers' personal data.
- Companies should provide clarity in their privacy policy on the purpose for data collected, data processing, data held, data used and data that will be disclosed to third parties.
- Companies should appoint a data protection officer who will not only ensure compliance with the relevant data protection regulations but will also ensure that internally the company fully operates and deals with personal data in alignment with the company's internal data protection guidelines and will also be able to pre-empt and mitigate any data protection breaches.
- Security mechanisms must not only be stated in the privacy policy but should also be visibly implemented as this builds consumer trust and ensures accountability and transparency within the sector.
- The financial sector should strengthen financial literacy and awareness around personal data not only within the sector but also for its consumers so that they are aware of how and when they can exercise their data protection rights as prescribed in the regulations.

ii. E-commerce

The following recommendations are given for companies in the e – commerce sector to ensure full compliance with data protection laws and regulations:
- The privacy policies need to be reviewed to ensure that minute details such as the effective date are not left out. This enables data subjects to see how recent the privacy policy is and whether regular updates need to be done.
- To ensure compliance with the legal framework, the companies need to incorporate provisions essential to fulfil the criteria for achieving informed consent. This will entail the inclusion of the data storage duration and providing the data subjects with all rights as provided in the laws without any limitation.
- The privacy policies should clearly indicate the parties with access to personal data and third-party data transfer. This enables the data subjects to know how their personal data is being handled and which parties have access to the data to prevent unlawful disclosure to unauthorized third parties.
- Data security measures that will be used to protect personal data are an essential component of the privacy policy and should be clearly indicated by describing in detail the technical or organizational security measures that will be used to protect personal information.
- A clause mentioning and describing that the privacy policies will be regularly updated needs to be incorporated in the privacy policies so that users can keep checking and get updated on the measures the companies are taking to continuously protect personal data.
- The e-commerce companies have no percentage on the accountability indicator and to achieve a high percentage, they need to conduct regular assessment of their privacy practices and publish comprehensive transparency reports that will boost trust from the general public.

iii. Telecommunications

The following recommendations are made for business in the telecommunications sector to ensure full compliance with data protection laws and regulations:
- Companies should be transparent about their practices and inform users about how they handle their personal data via an easily noticeable privacy policy. The outdated ones need to equally be amended.
- Companies should include in their privacy policies a section on informed consent describing the type of data being collected, the duration of data storage, contact information, and the rights of the data subject.
- Data security measures are an essential component of the company's privacy policy. This should be clearly communicated by describing the technical or organizational security measures that will be utilized to protect personal data.
- To ensure that the data subjects are fully informed of their data processing, management, and access, the data transferred between the companies and a third party must be disclosed and the parameters must be clearly outlined in the companies' privacy policies.
- Companies must conduct regular audits of their privacy policies and practices and publish comprehensive reports on their transparency, which will increase public trust and confidence.

List of Legislations

International Instruments and soft law standards

- The Human Rights Committee's General Comment 16 of the ICCPR, 1988
- The International Covenant on Civil and Political Rights, 1966,
- The United Nations Guiding Principles on Business and Human Rights, 2011
- The United Nations Internet Rights and Principles Coalition Charter of Human Rights and Principles for the Internet, 2011
- The Universal Declaration of Human Rights, 1948

Domestic legislation

- Data Privacy and Protection Act, 2019 at https://media.ulii.org/files/legislation/akn-ug-act-2019-9-eng-2019-05-03.pdf
- Data Privacy and Protection Regulations, 2021 S.I No. 10 available at https://pdpo.go.ug/media//2022/03/Data_Protection_and_Privacy_Regulations-2021.pdf
- Data Protection Act, 2019 at http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%200f%202019
- The Constitution of the Republic of Kenya, 2010
- The Constitution of the Republic of Uganda, 1995

List of References

- Boyd v. US, 116 US 616
- Daigle, B. (2021). Data Protection Laws in Africa: A Pan African Survey and Noted Trends. Journal of International Commerce and Economics. https://www.usitc.gov/journals (accessed on 4 October 2022)
- Kabona, Esiara (2 July 2022). "Tough times in telecom sector as new MTN boss Sylvia Mulinge takes office". The EastAfrican. Nairobi, Kenya
- Kelly, M.J 'What is a Web Tracker.' (Mozilla , 2019) <https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/>
- Makulilo, Alex Boniface 'Privacy and data protection in Africa: a state of the art' International Data Privacy Law, 2012, Vol. 2, No. 3, available at http://repository.out.ac.tz/323/1/Privacy_and_Data_Protection_in_Africa-A_state_of_the_art.pdf (accessed on 4 October 2022)
- Posner, Richard A. "The Right of Privacy," Georgia Law Review 12, no. 3 (Spring 1978): 393-422
- Revathi, Raddivari 'EVOLUTION OF PRIVACY JURISPRUDENCE – A CRITIQUE' Journal of the Indian Law Institute, APRIL-JUNE 2018, Vol. 60, No. 2 (APRILJUNE 2018), pp. 189-199, available at https://www.jstor.org/stable/26826635 (accessed on 4 October 2022)
- Rubenfeld, Jed 'The Right of Privacy' Harvard Law Review Vol. 102, No. 4 (Feb., 1989), pp. 737-807 at https://doi.org/10.2307/1341305 (accessed on 22 September 2022)
- The Independent Uganda (6 October 2021). "Fears over MTN, Airtel dominance in Uganda's telecom sector". The Independent (Uganda). Kampala, Uganda

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