Privacy Score Card Report (Kenya):

A Study of Data Protection Compliance of Businesses in the Telecommunication, Financial, and E – Commerce Sectors in Kenya

Strathmore University

Centre for Intellectual Property and Information Technology Law

Table of Contents

1. Introduction

Over the past three years, there has been an increase in the enactment of data protection laws,[1] particularly within the East African region. Kenya and Uganda, for example, enacted their data protection legislation in 2019. 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. 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 generation of personal data. The Kenyan Data Protection Act 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 Kenya Data Protection Act (DPA) highlights these two elements in Sections 25 and 26, respectively.

Data protection impacts various sectors and in turn, the organizations and businesses within those sectors with the requirements of the DPA changing the adoption and utilization of technology and impacting service delivery and customer relations. Privacy policies establish the means through which compliance can be established, to this effect this assessment will focus on evaluating the extent to which select sectors and companies within the Kenyan Jurisdiction are compliant with the provisions of the DPA.

[1]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

1.1. Country Insights

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.[2] 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 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).[3] 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

[2]Section 3.

[3]Section 5.

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.

> Data protection impacts various sectors and in turn, the organizations and businesses within those sectors with the requirements of the DPA changing the adoption and utilization of technology and impacting service delivery and customer relations.

2. Methodology

This report details an assessment of compliance of three private businesses (with significant market share) within three sectors: financial services, telecommunication, and e-commerce. These three sectors have the highest utilization of personal data. 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. 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 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.[4] A score of good classifies the policy as readable. 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.[5] For each of the categories listed above - publicly published, readable, noticeable - a score is awarded.

B. Informed Consent

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

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

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

c. **Types of personal data collected** - The privacy policy must mention the types of personal data collected.

d. **Data storage duration** - The privacy policy should mention the storage period for the personal data collected.

e. **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

[4] https://hemingwayapp.com/

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

companies are utilizing their data, and to verify that such use is lawful.

f. **Right to update, correct, or erase personal data** - The privacy policy should 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.

g. **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.

h. **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:

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

b. **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[6], 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.[7]

c. **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,[8] Blacklight,[9] and Exodus[10] 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.[11]

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

[6]Privacy International, https://privacyinternational.org/

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

[8] https://www.ghostery.com/

[9]https://themarkup.org/blacklight

[10] https://reports.exodus-privacy.eu.org/en/

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

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.[12] 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.[13] The categories analyzed for this indicator are,

a. 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.

b. 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.

c. 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.

E. 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.

[12]SSL Server Test <https://www.ssllabs.com/ssltest/>

[13]Security Headers <https://securityheaders.com/>

A transparency report is a public communication document that discloses key metrics and information regarding data governance and enforcement measures on a platform.

3. Company Selection Criteria

For this evaluation we reviewed two companies across three sectors i.e. 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.

Anonymization Codes for Each Sector	
Financial Services	
Company 1	F-K-1
Company 2	F –K-2
Telecommunications	
Company 1	TC-K-1
Company 2	TC-K-2
E- Commerce	
Company 1	EC-K-1
	EC-K-2

For financial services we focused on Company F-K-1 and Company F-K-2. Company F-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-K-2 is a mid-tier bank / tier 2, tier 2 banks control 41.7% of the market share. Company F-K-1 traces its history to the 19th Century and has been operational in Kenya for over a century. Company F-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-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 Company TC-K-1 with the highest market share of 67% and Company TC-K-2 with a market share of 27.2%. Company TC-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 TC-K-2 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 TC-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 EC-K-1 and Company EC-K-2. Company EC-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 EC-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-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. KCB Group also offers internet, institutional, mobile banking; and cash management, capital management, custodian services, foreign exchange, and money market services.
Company F-K-2	3%		Retail Loans. Deposits. Loans Advances. Digital Banking. International banking Personal banking

	Market shares	Subscribers/ customers	Services
Telecommunications Sector			
Company TC-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 TC-K-2	27.2%	16.2 million	Mobile Services Telemedia Services. Fixed telephony and broadband internet. Digital TV Services.
E- Commerce			
Company EC-K-1	60%	3.1 million	Marketplace service Logistics service Payment service.
Company EC-K-2	3%	80,000	Online Pharmaceutical and logistics services.

Table 1: The table above gives a bio data of the 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 company F-K-2.

4. Results

1.2. 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:

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 TC-K-1 received credit for all 4 criteria, while Company TC-K-2 received credit for 3 of the 4 evaluation criteria in this section. In Company TC-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. Company EC-K-1 and Company EC-K-2 both received scores in all 4 criteria, public, published, noticeable, readable.	Company F-K-1 and Company F-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.
Data collection and Third-Party Data Transfers	Third-party data sharing is highlighted in both privacy policies. A credit score is awarded for Company TC-K-1 and Company TC-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	Company EC-K-1 and Company EC-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 Company EC-K-1 and Company EC-K-	The privacy policies for Company F-K-1 and Company F-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-K-1 and none

Indicators	Sectors		
	Telecommunications	**E-commerce**	**Financial Services**
Data collection and Third-Party Data Transfers	either website of Company TC-K-1 and Company TC-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	2 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 EC-K-1 Google, AdWorld, Criteo, Facebook, RTB house, Global Site Tag, iGodigital, Adjust, New Relic and urbanairship. The following were noted for Company EC-K-2 Adobe, Google, Facebook, Quantcast, Floodlight, DoubleClick, Criteo, Hotjar, Segment, LinkedIn , Facebook Connect, CloudFlare, LegitScript, clarity.ms, Klaviyo, and Google Analytics	for Company F-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-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 TC-K-1 notes mechanisms used to ensure security and privacy whereas the privacy policy of Company TC-K-2 does not. The SSL server score on both websites differs in scoring. Company TC-K-1 scores an A which meets the threshold for data security whereas Company TC-K-2 scores B which is below the data security threshold. Company TC-K-1 earns 3 out of 3 credit scores whereas in contrast Company TC-K-2 earns 1 out of 3 for each category in this indicator.	Company EC-K-1 and Company EC-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 EC-K-1 whereas 1 out of 3 is awarded for Company EC-K-2 for each category in this indicator.	Company F-K-1 and Company F-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-K-1 earned 2 out of 3 credit scores on the evaluation whereas Company F-K-2 earned 1 out of 3 for each category in this indicator.

Indicators	Sectors		
	Telecommunications	**E-commerce**	**Financial Services**
Accountability	No transparency report is available for the year in review on either website. Credit score on accountability is not given for either Company TC-K-1 or Company TC-K-2.	No transparency report for the year is available on either website. Credit score on accountability is not given for Company EC-K-1 and Company EC-K-2N	No transparency report for the year in review is available on either website. A credit score on accountability is not given for Company F-K-2 or Company F-K-1

*Table 2: The table above details the findings of the 6-business analyzed in the telecom*munications*, 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.*

1.3. Sectorial Compliance Scores

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: finance, telecommunications, and e-commerce sectors, 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.

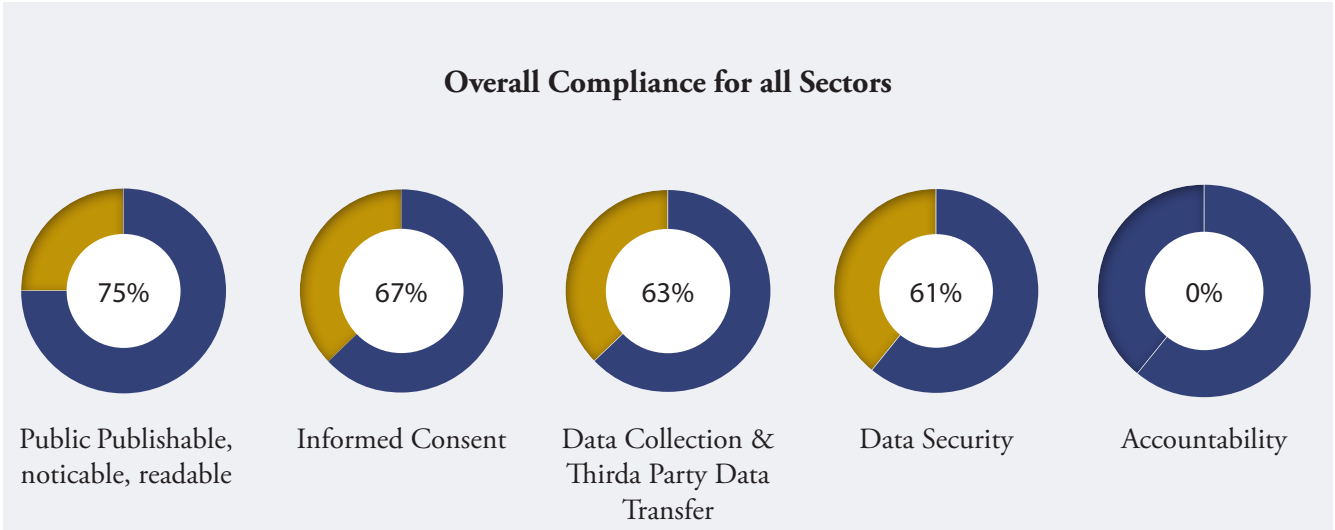

Figure 1: The figure above details the findings of the analysis on compliance of the 6 – businesses selected for study from the telecommunications, e – commerce, and financial services sectors, respectively in each of the five core indicators: existence of an accessible, readable and noticeable privacy policy; informed consent; data collection and third – party data transfers; practice robust data security, and accountability. 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%.

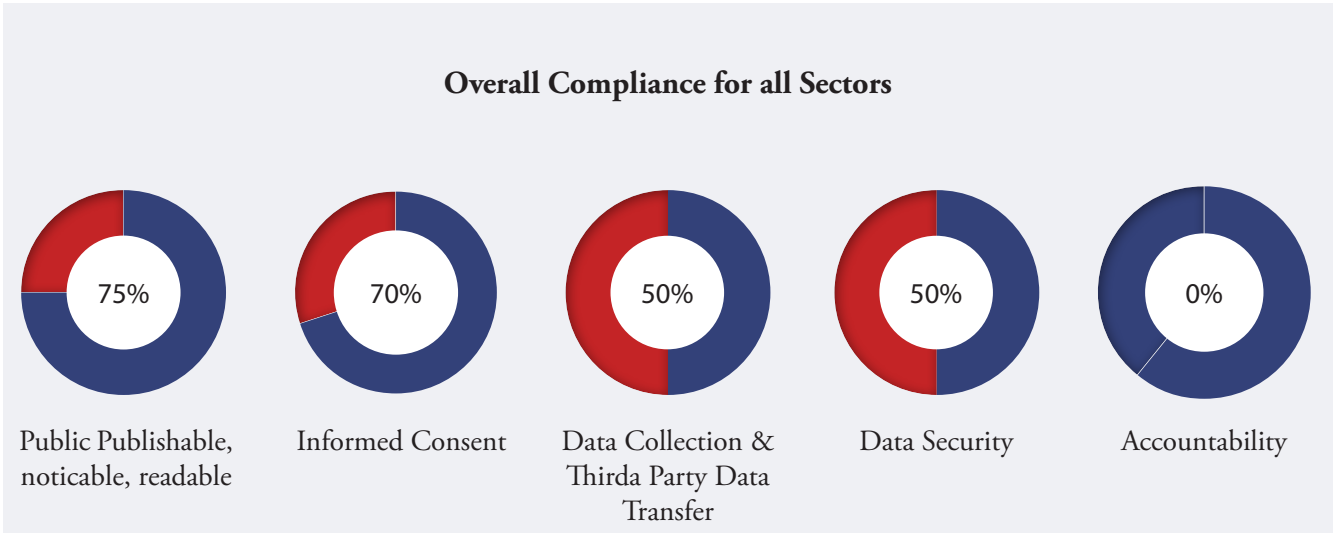

Figure 2: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the financial services sector in each of the five core indicators: existence of an accessible, readable and noticeable privacy policy; informed consent; data collection and third – party data transfers; practice robust data security, and accountability. 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, yet again, was observed for 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 informed consent indicator was 25%, the data security indicator, 23%, and the data collection and third – party data transfer indicator, 63%.

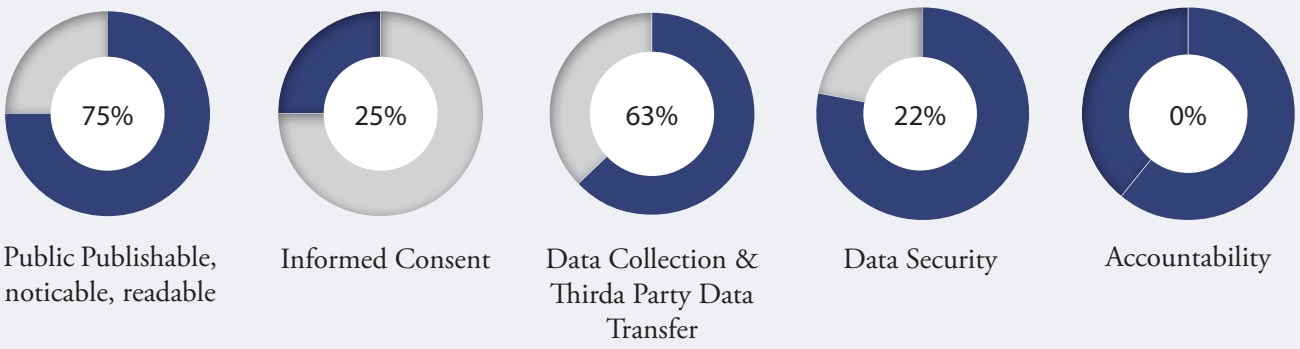

Figure 3: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the e – commerce sector in each of the five core indicators: existence of an accessible, readable and noticeable privacy policy; informed consent; data collection and third – party data transfers; practice robust data security, and accountability. 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 the existence of public, publishable, and readable privacy policy (75%) 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%.

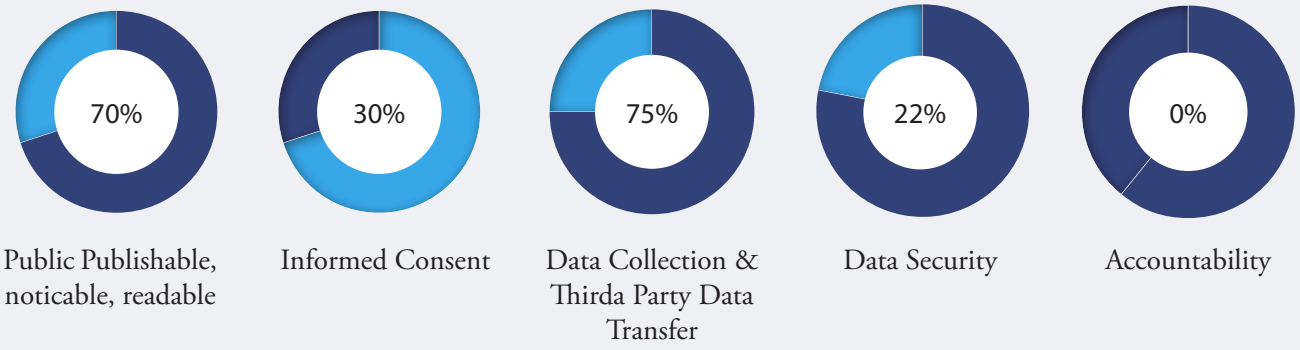

*Figure 4: The figure above details the findings of the analysis on compliance of the 2 – businesses selected for study from the telecommunications sector in each of the five core indicators: existence of an accessible, readable and noticeable privacy policy; informed consent; data collection and third – party data transfers; practice robust data security, and accountability. 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%.***Overall Analysis.**

5. Analysis of Findings

5.1 Overall Analysis.

Overall, all three sectors had the highest compliance score in the existence of a privacy policy indicator. 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 financial services and the lowest in telecommunications. The low compliance score for the informed consent in the telecommunications sector is characterized by the lack of a well-drafted privacy policy on providing for the rights of data subjects in Company TC-K-2. 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 protection 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 analysed on the type of personal data shared. Only one of the analysed companies, from all three sectors, provides information on data storage limitations. 2 of the 6 companies provide information on the type of personal data that will be collected, and 5 of the 6 companies state the purpose for which data is to be collected.

Notably, all of the companies analyzed across the 3 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 i.e. financial services, telecommunications and e-commerce, 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 reevaluated across all three sectors in order to strengthen implementation and compliance processes within the sectors developing best practices.

5.2 Sectoral Analysis.

5.2.1 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 indicator which assessed whether the privacy policy is published, noticeable, readable and accessible, and the rights of data subjects respectively. The high scores for these indicators suggests the development of some data protection practices by 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.[14] Contact information is required on how best data subjects i.e. subscribers and customers can reach 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-K-1 and Company F-K-2 reflected good security header results, both were respectively graded A. A 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.

5.2.2 Telecommunications

For the companies analyzed in this sector, Company TC-K-1 and TC-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 TC-K-1. Whereas Company TC-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 TC-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

[14]These rights are provided for under section 26 of the DPA.

Company TC-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 TC-K-1 holds twice the number of subscribers as Company TC-K-2 and is available 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 TC-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 TC-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 regulations.

The technical analysis relating to the SSL server tests graded Company TC-K-1 and Company TC-K-2 A 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 TC-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 TC-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.

5.2.3 E-Commerce

In the companies analyzed in the study, the highest compliance scores were observed for the existence of a privacy policy indicator, (75%), and 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 Company EC-K-1 and Company EC-K-2. Informed consent and data security hold the lowest percentages, 25% and 22%, respectively, indicative of practices in dealing with data protection rights and ensuring the security of their platforms from possible breaches and cyber-attacks. Notably of the two companies, Company EC-K-1 and Company EC-K-2, assessed, Company EC-K-2 did not indicate the purpose for which the data is collected nor

did it provide for any of the rights of the data subject. The lack of these provisions in the privacy policy is indicative of poor data protection practices for the company. It influences 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 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 Company EC-K-1 and Company EC-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 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 sector more specifically as it will speak not only to improved and strengthened compliance with the data protection laws keeping the companies accountable not only to the relevant regulatory authorities but also to its consumers.

> A transparency report especially for the telecommunications sector would be beneficial in addressing areas where compliance to data protection laws has been strengthened.

6. Recommendations

6.1 General Recommendations

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

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

6.2 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:

6.2.1 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:

i. Companies should regularly update their privacy policies and Standard Operating Procedures (SOPs) to align with the provisions in the DPA and data protection regulations set forth by the ODPC, especially those that relate to the processing of personal data.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

6.2.2 E-commerce

The following recommendations are given for companies in the e – commerce sector to ensure full compliance with data protection laws and regulations:

i. 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.

ii. To ensure compliance with the Data Protection Act, 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 Data Protection Act without any limitation.

iii. 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.

iv. 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.

v. 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.

vi. 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.

6.2.3 Telecommunications

The following recommendations are made for business in the telecommunications sector to ensure full compliance with data protection laws and regulations:

i. Companies should be transparent about their practices and inform users about how they handle their personal data via an easily noticeable privacy policy.

ii. 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.

iii. 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.

iv. 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.

v. 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.

7. Conclusion

For data controllers or processors to be entrusted with handling personal data they must illustrate that they have complied with the principles of data protection as enshrined in section 25 of the Data Protection Act. The rights of a data subject should be adequately provided for so that they can feel comfortable when sharing their personal data. 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.

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.

All the companies analyzed had at least some measures in place to protect the personal data of its users.

Appendix

Appendix 1

List of Companies in the Evaluation

This evaluation relied on select companies in three different sectors i.e. Financial services, Telecommunications and E-Commerce. However, not all companies were featured in the evaluation as the only privacy policies. Therefore, the evaluation does not include all the companies in the three sectors that handle personal data and have privacy policies.

- Absa
- Aliexpress
- Bank of Baroda
- Jumia
- Kenya Commercial Bank (KCB)
- Safaricom
- Stanbic Bank
- Airtel
- Avechi
- Jambo Shop
- Kilimall
- MyDawa
- Standard Chartered
- Telkom

Appendix 2

Privacy Policy Assessment Matrix

The Data Protection Act 2019 governs the processing of personal data, including the name, postal address, e-mail address, telephone number, and other personal details of a data subject. As a result, companies are required to inform the public of the nature, scope, and purpose of the personal data they collect, use, and process, and to inform data subjects of their rights. Following the Data Protection Act, the assessment matrix below evaluates the components of the privacy policies of the selected companies.

	Component of the privacy policy	Yes/No
1.	Is there an effective date?	
2.	Does the privacy policy mention that personal data is being collected?	
3.	Does the privacy policy explain why the data is collected?	
4.	Does the privacy policy mention the applicable law?	
5,	Does it mention how you, as the data subject, can withdraw consent at any time?	
6.	Can you access and correct your information?	
7.	Can you request the deletion of your personal information?	
8.	Can you restrict or object to the processing of your personal information?	
9.	Does the privacy policy specify how long the data is retained?	
10.	Does the privacy policy mention data sharing with third parties?	
11.	Does the entity's contact information appear in the privacy policy?	
12.	Does the privacy policy state whether you will be notified if there are any changes to it?	
13.	Is the privacy policy in simple, understandable language?	

There is also an interactive version of the matrix which is available here:

https://privacypolicytool.cipit.org/

For the interactive version, the results will appear in colour codes which have been explained below:

Scoring & Colour Code

The evaluation criteria were based on the indicators in the privacy policy assessment matrix.

Range (based on a number of yeses)	Colour code & Meaning
10-13	Green
6-9	Yellow
0-5	Red

Colour code meaning

Green: This means that the privacy policy is generally good as it meets more than three quarters (75%) of the criteria outlined in the privacy policy assessment matrix.

Yellow: This means that the privacy policy is average as it meets between half (50%) to slightly more than half of the criteria outlined in the privacy policy assessment matrix. There are missing components that should be added and/or the existing ones should be improved to meet the criteria.

Red: The privacy policy meets less than half (49% and below) of the criteria outlined in the privacy policy assessment matrix. There are missing components of the privacy policy that have not been included at all, and/or the ones that are present require additional clarification so that they are clear and understandable.

This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.