DATA PROTECTION IN THE KENYAN BANKING SECTOR

A study of Publicly Available Data Policies of Commercial Banks operating in Kenya in Relation to a Set Data Protection Standard

A report by the Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University, Nairobi, Kenya

MAY 2021

IDRC · CRDI
Canada

Strathmore University
Centre for Intellectual Property and Information Technology Law

Strathmore
UNIVERSITY

Report Authors:

Mercy King'ori, Mitchel Ondili, Isaac Rutenberg, Melissa Omino, Godana Galma

Centre for Intellectual Property and Information
Technology Law, Strathmore Law School
Strathmore University, Nairobi, Kenya

CONTENTS

EXECUTIVE SUMMARY

Banking institutions, as with many other entities, are increasingly handling personal data owing to an increased use of different technologies to offer banking services. Increased handling of such personal data coupled with new statutory requirements relating to data protection have placed renewed emphasis on the efforts used by banks to create and communicate policies for handling data subjects' information. This report analyses the publicly available data policies of commercial banks in Kenya, providing an overview of the approaches taken by the studied banks with respect to data protection for existing and prospective customers.

This report compares the banks' data policy provisions against a data protection standard developed using the provisions of existing national and international data protection regimes, including the Kenya Data Protection Act 2019 (DPA) and the European General Data Protection Regulation (GDPR). This standard comprises three broad indicators: data collection, data sharing, and the rights of data subjects. Compliance with these indicators is measured using tabulated analyses showing the individual and aggregated performance of the banks.

The report's conclusions are derived from research conducted in Kenya in 2019 and 2020. A total of 32 policies were identified and analyzed, all of which were in existence prior to the enactment of the Kenya DPA. This report is therefore a baseline study of the policies; the report anticipates that there will be changes in banking policies as the DPA is put into practice. The findings in this report will be useful for comparative purposes as the DPA is implemented and enforced.

Key Findings

On average, the banks were found to be more likely to have unclear or incomplete policy provisions in all categories. Provisions relating to data collection were the most compliant while provisions relating to rights of data subjects had the lowest compliance score.

There is a notable variance in the performance of banks with regard to rights of data subjects. A large number of banks lacked any policy provisions in this category while a similarly large number of banks were clustered at the higher scores. This disparity suggests that the banks took two general approaches, i.e., to exclude policy provisions relating to data subjects' rights altogether, or to incorporate such provisions clearly and completely.

Overall, provisions relating to the purpose of processing data were the most compliant among all provisions in all categories. Provisions relating to the rights of data subjects to object to the outcome of an automated decision were the least compliant. Clarity or completeness of provisions was a problem for a large number of the policies, and the overall readability of the policies may present challenges to banking customers that are likely to have a wide range of formal education.

Although the report highlights that the banking sector falls short of what we consider internationally-recognized norms in data protection, the data also show that data protection policies are widely present in the sector, and can be modified to become compliant.

INTRODUCTION

Information is personally identifying information or personal data if it can identify a person i.e. can be reasonably linked to a natural person or if it identifies a natural person.[1] The concern of personal data protection is not novel.[2] Since time immemorial people have been concerned with how their right to information privacy is safeguarded.[3] However, there has been a recent renewed vigour in matters of data protection. This has been attributed to advanced technologies that have increased data collection capabilities.[4] Entities like banks that were once guided by the simple principle of the duty of confidentiality[5] are now required to adhere to other principles of data protection such as a purpose limitation and accuracy to ensure that customers' personal data is safeguarded. These principles of data protection require more than just maintaining the secrecy of customer information.

The new requirements of data protection emanate from the fact that banks, like many other entities that handle personal data, are categorised as both data controllers and data processors depending on the activity carried out and hence have a duty towards the data subject[6] whose information they hold.[7] Banks more than ever are handling significant amounts of personal data thanks to improved technology that has facilitated the use of alternative channels of banking such as mobile and internet banking. These alternative channels are requiring and generating new forms of personal data compared to the traditional brick and mortar form of banking, much of which is sensitive personal data. To communicate how they will handle a data subject's information, banks have resorted to developing data policies. Prior to passage of the Kenya Data Protection Act, when legal requirements for data processing in the banking industry were less comprehensive, data policies were a voluntary, self-regulatory tool. From the perspective of data subjects, it is important that such policies provide comprehensive data protection measures to ensure they adequately protect data subjects' data.

Pursuant to this, this study looks at how commercial banks in Kenya with publicly available data policies are treating customer data from the perspectives of data privacy and data protection. It also analyses whether the nature of information provided for in the policies is adequate to articulate these protection efforts. The study does so by comparing the provisions of the policies against a data protection standard developed by the authors.

First, it begins by developing the standard against which the data policies are measured to determine the adequacy of the provisions in terms of data protection. To develop the standard, this study uses national and international data protection regimes; collates what is common and identifies the non-common aspects of data protection in each of them. After developing the standard to be used, the publicly available data policies of the selected banks are measured against it and scored to determine their performance in relation to the standard. The general performance of the banks in each category is analysed. Based on this analysis, the study outlines specific areas of improvement for banks and the banking industry. The study concludes with the limitations of the study and highlights areas for future research. In an Annex to the study, the bank policies are analysed for readability.

For purposes of this initial report, the study is limited to making general findings about the performance of the studied banks. As such, the study refrains from making reference to specific banks, and anonymises bank identity in the tabulations. However, a list of the studied banks is contained in the appendix to this report. Finally of note, the reviewed data policies were those available prior to Kenya's enactment of the Data Protection Act 2019. Accordingly, this study serves as a baseline for follow-on work that will review data policies after the DPA has been in force for some time.

[1] Section 2, Data Protection Act (2019).
[2] Barbas, S. (2012). Saving privacy from history. DePaul Law Review, 61(4), 973
[3] Daniel Solove, "Conceptualising Privacy" (2002) 90 Cal. L. Rev.
[4] Chang, C. (2015). New technology, new information privacy: Social-value-oriented information privacy theory. National Taiwan University Law Review, 10(1), 129
[5] The duty of confidentiality in banks is a common law duty that exists where there is a bank-customer relationship (the duty of confidentiality also stems from the fiduciary relationship between the bank and its customers). Under this duty a bank is obligated to maintain the secrecy of customer information with regards with customer's bank account
[6] The Data Subject is defined as an identified or identifiable natural person who is the subject of personal data. See Section 2, Data Protection Act (2019).
[7] Malta Bankers Association 'Data Protection Regulations for Banks' https://idpc.org.mt/en/Documents/Data%20Protection%20guidelines%20for%20banking.pdf

OBJECTIVE

To determine whether publicly available data policies of banks operating in Kenya adequately cover a set data protection standard.

METHODOLOGY

1. Determining the Data Protection Standard

Numerous data protection approaches currently exist, so it is necessary to select or develop a data protection standard to be applied to the data policies of Kenyan banks. The standard was developed using international and national norms of data protection, namely: the Data Protection Act, 2019 (DPA)[8], the General Data Protection Regulations (GDPR)[9] and the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and TransBorder Data Flows (OECD Guidelines)[10]. These international norms (GDPR and OECD Guidelines) were used as benchmarks since they are regarded by many as indicators of best practices for data protection at the international level. The GDPR, which became enforceable beginning 25 May 2018, has been a model and benchmark for countries that subsequently developed their data protection laws, including Kenya and its DPA, and Brazil with its General Data Protection Law.[11] Additionally, the GDPR's impact goes beyond European borders in what is known as the "Brussels Effect" – the international spread of European standards due to market harmonization or other market-based influences.[12] The OECD Guidelines were the first internationally agreed set principles of data protection.[13] They have shaped the data protection laws of countries such as Canada where they were adopted with minor modification to create the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private-sector privacy law.[14] They are principle-based and technology-neutral.[15]

The DPA is now the guiding law on data protection in Kenya, and is modelled after various aspects of the GDPR. The DPA was passed after at least a decade of efforts by the Kenyan legislature. Thus, and although the data policies reviewed in this study were available prior to the DPA, the DPA guides (in part) our development of a data protection standard.

By analysing these norms, four broad categories referred to as "indicators" were developed. The indicators were subdivided into their components known as "sub-indicators" which covered the requirements of data protection as envisioned by these norms. The broad categories include:

I. Data collection
II. Data sharing
III. Rights of data subjects

The following section gives brief explanations of the indicators, the sub-indicators and the normative basis of the sub-indicators.

i. Data Collection

For any duty to arise with regards to data protection, personal data must first be collected. Therefore, this is the first step before any data processing activities can take place. To ensure that data collection adheres to data protection requirements the following requirements must be met:

1. A data subject needs to be informed of the type of data being collected;[16] [17]

[8] Data Protection Act, 2019 http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf

[9] General Data Protection Regulation https://gdpr-info.eu/

[10] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/internet/iecO-ECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Dataonomy/oecdguidelinesontheprotection-ofprivacyandtransborderflowsofpersonaldata.htm

[11] JDSUPRA, 'Brazil's General Data Protection Law: A Comparison Between Brazil's Newly Effective Law and the GDPR' https://www.jdsupra.com/legalnews/brazil-s-general-data-protection-law-a-25950/#:~:text=Brazil%27s%20General%20Data%20Protection%20Law%20(the%20%E2%80%9CLGPD%E2%80%9D)%2C,GDPR%E2%80%9D

[12] Deloitte, 'A New Era for Privacy: GDPR Six Months On' https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

[13] OECD, 'Thirty Years After: The OECD Privacy Guidelines', 2011, 14 http://www.oecd.org/sti/ieconomy/49710223.pdf

[14] OECD, 'Thirty Years After: The OECD Privacy Guidelines', 2011, 14

[15] OECD, 'Thirty Years After: The OECD Privacy Guidelines', 2011, 14

[16] Section 29 (g) of DPA.

[17] Note that the scores on this sub indicator are contingent on the extent to which the data is defined. This means that when indicating that the bank collects personal data, it would have to provide examples of that data e.g. personal data includes: name, date of birth, phone number etc. The threshold for reaching the maximum possible score hinged on the specificity of the information provided and whether a customer/user would reasonably be expected to gain an understanding of the type of data collected from the examples and descriptions given.

2. A data subject needs to be informed of the purpose of processing;[18]
3. A description must be provided for technical and organizational security measures taken to ensure the integrity and confidentiality of the data (Principle of integrity and confidentiality);[19]
4. The data retention period/criteria to be used to determine the period must be mentioned;[20]
5. The data subject must be given a means of providing valid consent for the specified purposes of data collection;[21,22]
6. The measure to be taken in the event of data breach i.e. data breach notification provisions in the event of a security mishap;[23] and
7. The contact details and identity of the data controller/ processor must be provided.[24]

ii. Rights of Data Subjects

As owners of their personal data, data protection affords data subjects with rights that they can exercise against a data controller or processor. Data protection is ensured when the following rights are granted:

1. The right to access information about themselves, i.e. which type of data is held about them, details of the data controller, details of any recipients, data retention period etc;[25]
2. The right to rectification, which entitles data subjects to have inaccurate data about them corrected or incomplete data completed;[26]
3. The right to erasure, which entitles data subjects to have their personal data erased;[27]
4. The right to restrict processing or object to processing of all or part of their personal data, which entitles data subjects to limit how an organisation uses their data;[28]
5. The right to data portability, which entitles data subjects to transfer their personal data from one controller to another in a structured, commonly used, and machine-readable format;[29,30]
6. The right to lodge a complaint with a supervisory authority;[31] and
7. The right to know the existence of automated decision-making and object the outcome of such decision making, i.e. the logic involved, the significance, envisaged consequences of such processing and recourse.[32]

iii. Data Sharing

As part of its operations, a bank regularly shares customer information among its branches and to third parties (e.g. when giving banker's reference, initiating inter-bank funds transfers, or to credit reference agencies). Therefore, data sharing raises data protection concerns that a controller ought to be aware of and to communicate the same to data subjects. Provisions that adequately communicate a controller's data sharing practices must state:

1. Which third-party actor holds/receives the personal data;
2. The types/ categories of personal data being processed;

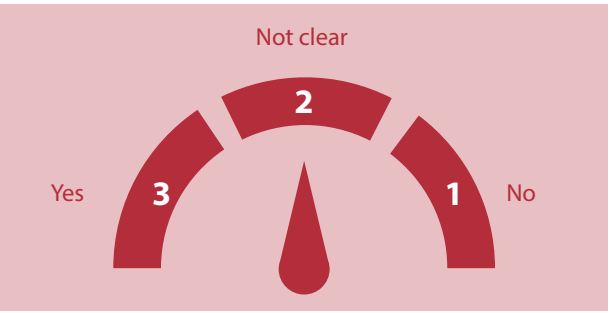
[18] As expressed under section 29 (c) of DPA and Part 2 of OECD Guidelines.
[19] This can be found in section 29 (f) of DPA and article 5(1) (f) of GDPR.
[20] Section 39 DPA and article 13(2) (a) of GDPR.
[21] Section 28(c) of DPA read together with section 32(1) and article 7 of GDPR.
[22] The authors of the study developed a threefold test to determine the adequacy of consent: first, that the customers/visitors to the site would be informed of each instance of their use of their data and be given the opportunity to opt -in/out. Secondly, the choice to opt-in/out was through a mechanism such as a check-box that would actively prompt them to indicate their consent. Lastly, that the customer/visitor to the site had the option of revoking consent in writing at a later date and the means provided for revocation of consent.
[23] This is supported under section 43(1) (b) of DPA and article 34 of GDPR.
[24] This is informed by section 29(e) of the DPA and article 7 of GDPR.
[25] This is backed by section 26 (b) of DPA and article 15 of GDPR. This is also supported by the OECD guidelines under the Individual Participation Principle.
[26] This can be found under section 26(d) and article 16 of GDPR.
[27] It is a unique feature of the GDPR and not found in the DPA.
[28] This can be found in section 26(c) of DPA and article 18 of GDPR.
[29] This can be found under section 38 of DPA and article 15(1) (f) of GDPR.
[30] The right to data portability was phrased in different ways across the different banks. The key indication in this right was: the ability to receive a copy of the data in a structured, commonly used and machine readable format as well as the transfer of that data to an institution of the customer's choosing.
[31] This can be found under section 56(1) of DPA and article 15 of GDPR.
[32] This is based on section 35 of DPA.

3. The purposes of processing; and
4. The appropriate safeguards to be maintained by a third party.

2. Measuring adequacy against the data protection standard

To determine the performance of the policies against the established standard of data protection, this study developed a scoring scale for the banks and their respective policies. The scores ranged from 1 to 3. A score of 1 represents "no", meaning that the policy does not contain the particular sub-indicator, 2 represents "not clear", meaning that the policy provision does not fully contain the particular sub-indicator (e.g., it is incomplete or missing sections), and 3 represents "yes", meaning that a data policy provision fully complies with the particular sub-indicator (i.e. the provision is clear and unambiguous).

After the policy of a particular bank was scored on the scale under each of the indicators, the score was aggregated to



give the final score of the bank under each of the indicators. Lastly, the aggregated scores under each of the indicators were used to create overall rankings of the banks.

3. Measuring the adequacy of consent

The authors of the study developed a threefold test to determine the adequacy of consent. First, the test evaluates whether customers/visitors to the site are informed of each instance of use (or intended use) of their data, and whether they are given the opportunity to opt-in/out. Second, the test evaluates whether the choice to opt-in/out was through a mechanism such as a checkbox that would actively prompt them to indicate their consent. Third, the test evaluates whether the customer/visitor to the site has the option of revoking consent at a later date, and the means provided for revocation of consent.

ANALYSIS

i. Policies evaluated on indicators pertaining to Data Collection

The adequacy of seven sub-indicators pertaining to data collection was evaluated as described above. The sub-indicators were assigned and summed, resulting in a score in the range of 7-21, with 14 as the midpoint.

eneral performance amongst the banks was fairly spread out, with 17 banks attaining aggregate scores above the midpoint score, while 15 banks attained aggregate scores below the midpoint score. The average aggregate score for all banks was also marginally lower than the midpoint, i.e., 13.66. The mean score in all the sub-indicators was 1.95, suggesting that the studied banks were generally likely to have incomplete/unclear provisions in their policies.[33]

The most frequent provision in the banks' data policies was the purpose of processing data with an average score of 2.72. This provision was clearly and completely provided in 25 policies. In fact, only two policies[34] lacked this provision altogether. This is a strong indication that this sub-indicator is not only the most common but is also the most clear/complete provision in this category.

The least frequent provision was that of data breach notification, with an average score of 1.28. This provision was present in only five policies.[35] Interestingly, in four of those five policies, the provisions were clear and unambiguous. This may suggest that, whilst this provision is generally less frequent, its clarity/completeness may not necessarily be an obstacle amongst the studied banks. However, the accuracy of this particular finding is limited by the relatively small sample size of five policies.

Only one policy[36] lacked all the sub-indicators entirely with the remaining banks (31) having at least one or more complete or incomplete provisions.

Looking at average scores for the sub-indicators, the best

[33] For this analysis, an average score between 1.75 and 2.25 was treated as being likely to contain incomplete/unclear provisions. This is because as per the adequacy standard, a score of 1 represents "no" meaning that the policy does not contain the particular sub-indicator while a score of 2 signifies that the policy provision does not fully contain the particular sub indicator i.e. it is incomplete.
[34] Bank 18 and Bank 4.
[35] Bank 23, Bank 20, Bank 16, Bank 11 and Bank 2.
[36] Bank 18

average score (2.72) was obtained for Purpose of Processing Data, while the worst average score (1.28) was obtained for Data Breach Notification Provisions.

Bank 2 was the best aggregate performer, with its policy having clear and complete provisions in each of the sub-indicators aside from the sub-indicator relating to the purpose of processing data.

ii. Policies evaluated on indicators pertaining to the Rights of Data Subjects

The adequacy of seven sub-indicators pertaining to the rights of data subjects was evaluated as described above. The sub-indicators were assigned and summed, resulting in a score in the range of 7-21, with 14 as the midpoint.

The average aggregate score amongst the banks was marginally lower than the midpoint, i.e., 13, with the banks' aggregate scores evenly distributed above 16 and below 16. In addition, the mean score in all sub-indicators was 1.85, slightly lower than the average score in the previous category (i.e., data collection). This suggests that the surveyed banks are generally likely to have incomplete/unclear provisions relating to data subjects' rights.[37]

It is however worth noting that general performance was mixed. On one hand, 10 banks[38] attained a score of 7, which means that their respective policies lacked any provisions relating to data subjects' rights. On the other hand, 11 banks[39] attained a score of 17 or above, which suggests that their policies contained a number of the sub-indicators clearly and unambiguously. Overall, a large number (21) of the banks studied took one of two approaches: clear and unambiguous provisions for the rights of data subjects, or a complete lack of such provisions.

The most frequently recited right was the right to rectification, with an average score of 2.28. This was closely followed by the right to access information, with an average of 2.25. One additional right, the right to erasure/deletion had average scores above 2. In fact, aside from the firms that completely lacked any sub-indicators, 18 out of the remaining 22 banks contained these three rights (whether clearly or unclearly provided). This suggests that these three rights were generally prominent in the policies that had some provisions relating to the rights of data subjects. In addition, 14[40] out of those 18 policies had clear and unambiguous provisions in those 3 rights. This is indicative of a high level of clarity and completeness in construing the three rights amongst the banks studied.

The right to object to the outcome of automated decision-making was the least frequent with an average score of 1.19. Only four policies[41] contained this right (whether clearly or unclearly). In addition, the right to data portability was also notably absent, with only nine policies[42] containing the right. A notable feature in this regard was that out of the nine policies that contained this right, seven policies provided the right clearly and unambiguously.

Looking at average scores for the sub-indicators, the best average score (2.28) was obtained for the Right to Rectification, while the worst average score (1.19) was obtained for the Right to Object to the outcome of automated decision-making.

Bank 1 was the best aggregate performer with its policy, fully and clearly providing all but one of the data subjects' rights, missing only the right to restrict processing.

iii. Policies evaluated on indicators pertaining to Data Sharing

The adequacy of four sub-indicators pertaining to data sharing was evaluated as described above. The sub-indicators were assigned and summed, resulting in a score in the range of 4-12, with 8 as the midpoint.

The average aggregate score of all banks was 7.47, marginally below the midpoint. The banks' aggregate scores were fairly spread out above (17) and below (15) the midpoint. The mean score of all the sub-indicators was 1.87, indicating that banks studied are on average likely to have incomplete or unclear data sharing provisions in their policies.[43]

[37] For this analysis, an average score between 1.75 and 2.25 was treated as being likely to contain incomplete/unclear provisions. This is because as per the adequacy standard, a score of 1 represents "no" meaning that the policy does not contain the particular sub indicator while a score of 2 signifies that the policy provision does not fully contain the particular sub indicator i.e. it is incomplete.

[38] Banks 3, 4, 6, 8, 10, 17, 18, 22, 24 and 29.

[39] Banks 1, 2, 7, 14, 16, 20, 21, 23, 26, 31 and 32.

[40] Banks 1, 2, 7, 13, 14, 16, 20, 21, 23, 25, 26, 27, 30 and 32.

[41] Banks 1, 16, 25 and 31.

[42] Banks 1, 2, 5, 7, 9, 16, 20, 23 and 32.

[43] For this analysis, an average score between than 1.75 and 2.25 was treated as being likely to contain incomplete/unclear provisions. This is because as per the adequacy standard, a score of

Provisions relating to the purpose of data processing by third parties were the most prominent, with 27 banks having the same in their policies and with an average score of 2.16. Provisions relating to the type or category of data received by third parties were technically the least frequent, and 11 policies[44] lacked this sub-indicator entirely. For the 21 banks with the provision, an average score of 1.69 was found, indicating that the provisions were frequently incomplete or unclear. Only one policy[45] provided the particular provision clearly. This is a strong indicator of a general lack of clarity or completeness in this particular provision in the policies of the banks studied.

Only three policies[46] lacked all the sub-indicators entirely. This suggests that most of the studied banks (29) contained at least one or more complete or incomplete provisions in their policies from this category.

Looking at average scores for the sub-indicators, the best average score (2.16) was obtained for Purpose of Processing by Third Party, while the worst average score (1.69) was obtained for Type/category of Data Received by Third Party.

Bank 6 and Bank 26 were the best performers, having clear and complete provisions in all the sub-indicators aside from the type/category of data received by third party.

KEY FINDINGS – average and aggregate scoring

From the data above, and the tables provided in Annex 5, several observations emerge. Perhaps most importantly, the average scores in all three categories of indicators were below 2, indicating that, on average, banks are not adequately providing for any of the data protection norms in privacy policies.

Across the three categories of indicators, provisions pertaining to data collection had an average total score of 13.6 (65% of the maximum total score of 21), provisions pertaining to the rights of data subjects had an average total score of 13.0 (62% of the maximum total score of 21), and provisions pertaining to data sharing had an average total score of 7.5 (62% of the maximum total score of 12). See Tables 1-3. This shows a highly consistent treatment of the three categories, on average, indicating that the banking sector has not made substantial progress in any one category at the expense of, or while ignoring, another. Stated another way, each of the three categories of data protection principles needs roughly equal improvement to fully conform with the norms in the standard model developed for this study.

Substantial variation is present among the studied banks, as indicated by total aggregated scores (i.e., aggregations of all three categories of indicators, which value has a range of 18-54, and a midpoint of 36). See Table 4. The average total aggregated score across all banks was 34.2 (slightly below the midpoint), with a fairly high standard deviation of 8.8. The highest rated bank, Bank 2, had a total aggregated score of 49, while the lowest rated bank, Bank 18, had a total aggregated score of 18.

Looking closer at the individual sub-indicators, however, Table 1 provides the top three and the bottom three indicators by average score across all bank policies.

Table 1. Top three and bottom three rights across all policies

Right	Average Score
Right to Rectification	2.28
Right to Access Information	2.25
Right to erasure or deletion of information	2.03
…	
Right to Data Portability	1.50
Data Breach Notification Provisions	1.28
Right to object to automated decision making	1.19

Therefore, the ***data show areas that have the greatest need for improvement for the overall banking sector***. For example, the lowest average scores were obtained in the following sub-indicators:

- Data Breach Notification provisions;
- Right to Object to the outcome of automated decision-making;

1 represents "no" meaning that the policy does not contain the particular sub indicator while a score of 2 signifies that the policy provision does not fully contain the particular sub indicator i.e. it is incomplete.

[44] Banks 2, 3, 4, 8, 16, 18, 19, 22, 24, 30 and 32

[45] Bank 13

[46] Banks 8, 19 and 32.

- Right to Data Portability[47];
- Types/ categories of personal data being processed by third parties; and
- Description of the technical/ other measures taken to ensure the integrity and confidentiality of data.

KEY FINDINGS – Consent

Most banks struggle to provide a mechanism for obtaining real consent from the data subjects. For most banks, consent is implied. A data subject has no means of affirmatively providing consent, e.g., providing a statement to the effect that they consent or take part in an affirmative act. Furthermore, no bank provided a mechanism for a data subject to give partial consent – i.e., to consent to some aspects of the bank's policy but to withhold consent from other aspects.

KEY FINDINGS – Readability and completeness

Several policies made reference to policies that were not publicly available (i.e. "in-house policies"), which were mentioned as being necessary to be read together with the publicly available ones. As a result, the publicly available ones may not be a true representation of a bank's data policies. Furthermore, there is a trend by certain banks to include intellectual property provisions in the data policy. This suggests that some banks may have difficulties in differentiating between their terms of use vis-à-vis dedicated data policies.

Annex 7 provides data on readability of the data policies, as determined using the Flesch Readability Score. In summary, the average score was 35.5, and most policies scored below 40, which indicates that a significant amount of formal education (i.e., slightly above a secondary school-level of education) would be needed to understand the policies. Several policies scored below 30, meaning that the policies would be easy to understand only for individuals with a university degree.

CONCLUSIONS

Banks are custodians of the personal data of their customers which generates certain duties of data protection. Different norms have been developed to explain how custodians of personal data (i.e., data controllers or the processors) can/ must handle the personal data. The norms can be used to demonstrate the level of protection that is required. Data policies are the tools banks use to communicate their information practices with regards to personal data.

his study reveals that most banks have a data/privacy policy, yet most of these policies fall significantly short in one or more aspects when compared against the data protection standard developed herein. This study provides a baseline for future research on how the recently passed Data Protection Act, and the recently created office of the Data Protection Commissioner, will impact data protection policies in the banking sector.

[47] The right to data portability was phrased in various ways, some of which were inconsistent with the normally accepted meaning of the term.

ANNEXES

Annex 1 - List of Data Policies

KBA Banks
https://www.kba.co.ke/members.php

Absa Bank Limited
https://www.absabank.co.ke/data-privacy-statement/

African Banking Corp. Ltd
https://www.abcthebank.com/wp-content/uploads/2020/12/Privacy_Notice.pdf

Bank of Africa Kenya Ltd
https://www.boakenya.com/wp-content/uploads/2017/10/BOA-Kenya-Website-Privacy-Policy-2014.pdf

Bank of India
https://www.bankofindia.co.in/Privacypolicy

Bank of Baroda (K) Ltd
https://bankofbarodakenya.co.ke/privacy-policy/

Citibank N.A.
https://www.citigroup.com/citi/privacy.html

Co-operative Bank of Kenya
https://www.co-opbank.co.ke/info/digital-touch-points-privacy-statement-0

Credit Bank Ltd
https://creditbank.co.ke/privacy-policy/

Diamond Trust Bank (K) Ltd
https://dtbk.dtbafrica.com/privacy-policy

Dubai Islamic Bank (Kenya) Ltd
https://www.dibkenya.co.ke/privacy-policy/

Ecobank Limited
Internet Banking Privacy Notice
https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice/internet-banking
Mobile App Privacy Notice
https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice/mobile-app
Recruitment Privacy Policy
https://www.ecobank.com/privacy-centre/general-privacy-policies/recruitment-privacy-policy
Rapid Transfer
https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice/rapidtransfer
Personal Banking Privacy Notice
https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice

Equity Bank Ltd
https://online.equitybankgroup.com/Privacypolicy.html

Family Bank Ltd
https://familybank.co.ke/privacy-policy/

Faulu Micro-FinanceBank
https://www.faulukenya.com/index.php/customer-service/data-privacy

First Community Bank Ltd -
https://firstcommunitybank.co.ke/index.php/home/privacy_policy

Gulf African Bank Ltd
https://gulfafricanbank.com/privacy-policy/

Habib Bank A.G. Zurich
https://www.habibbank.com/kenya/downloads/KenyaDataPrivacyNotice.pdf

I & M Bank Ltd
https://www.imbank.com/information/information-security/privacy-notice

Middle East Bank (K) Ltd
https://mebkenya.com/privacy-policy

M Oriental Bank Ltd
https://www.moriental.co.ke/privacy/

NCBA Bank Kenya
https://ke.ncbagroup.com/privacy-policy/

Prime Bank Ltd
https://www.primebankonline.com/corp/Help_Files/Retail%20User/private.html

Sidian Bank
https://www.sidianbank.co.ke/policies/privacy-policy/

Stanbic Bank Ltd
https://www.stanbicbank.co.ke/

Standard Chartered Bank (K) Ltd
https://www.sc.com/en/privacy-policy/

SBM Bank (Kenya) Ltd
https://www.sbmbank.co.ke/search-results/privacy

UBA Bank Limited
https://www.ubagroup.com/uba-privacy-policy/

Victoria Commercial bank Ltd
https://www.victoriabank.co.ke/wp-content/uploads/2019/03/PRIVACY-STATEMENT.pdf

Annex 2 - Indicators and Sub-Indicators used in the Data Protection Framework

Main Indicators

a. Data collection
b. Rights of data subjects
c. Data sharing

Sub-indicators

a. Data collection

1. Does the data policy provide the details and identity of the data controller/processor?
2. Does the data policy state the purpose of collecting/processing
3. Does the data policy state the recipients of the personal data?
4. Does the data policy provide a description of technical and organisational security measures taken to ensure the integrity and confidentiality of the data?
5. Does the data policy state which type/category of data is collected?
6. Does the data policy state the data retention period/criteria to be used to determine the period?
7. Does the data policy provide a data subject a chance to give valid consent for the specified purpose(s) of data collection?
8. Does the data policy contain data breach notification provisions?

b. Rights of data subjects

Here we looked at whether a data policy provides for the following rights of a data subject:

1. Right to access information about themselves
2. Right to rectification
3. Right to erasure/deletion

4. Right to restrict processing/object processing of all/part of their personal data
5. Right to data portability
6. Right to withdraw consent at any time
7. Right to lodge a complaint with a supervisory authority
8. Right to know the existence of automated decision making

c. Data sharing

Here we looked at whether the data policy:

1. Reveals which third party actor holds/receives the personal data
2. Reveals the type/category of personal data being processed by a third party
3. Reveals the purpose of processing by the third party
4. Reveals the appropriate safeguards to be maintained

Annex 3 - Links to laws and Guidelines

a. Data Protection Act, 2019
http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
b. GDPR
https://gdpr-info.eu/
c. OECD Guidelines
https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Annex 4 – List of banks in the study

The study relied on a list of banks that are part of the Kenya Bankers Association. However, not all banks were featured in the study since only policies that contained provisions on data collection and usage were analysed. Therefore, the study does not include all commercial banks in Kenya that handle personal data.

Absa Bank Limited
African Banking Corporation Limited
Bank of Africa Kenya Limited
Bank of Baroda
Bank of India
Citibank N.A.
Co-operative Bank
Credit Bank
Diamond Trust Bank
Dubai Islamic Bank
Ecobank (Note: five policies were obtained for this bank, and were treated as separate "banks" in the datasets herein. Those policies were the following: Internet Banking Privacy Notice; Mobile App Privacy Notice; Recruitment Privacy Policy; Rapid Transfer; and Personal Banking Privacy Notice)
Equity Bank
Family Bank
First Community Bank
Faulu Microfinance Bank
Gulf African Bank
Habib Bank AG Zurich
Middle East Bank
NCBA
Prime Bank
Sidian Bank
Standard Chartered Bank
Victoria Commercial Bank
SBM Bank
I&M Bank
M. Oriental Bank Limited
Stanbic Bank
UBA Bank

Annex 5 - Raw rankings

a. Table 5-1 - Scoring banks based on provisions pertaining to Data Collection

Bank	Type of data collected	Purpose of processing data	Description of the technical and organisational security measures taken to ensure the integrity and confidentiality of the data	Data retention period	Means of obtaining valid consent	Data breach notification provisions	Details of the data protection officer	Total score (x/21)
Bank 1	3	3	1	2	1	1	3	14
Bank 2	3	2	3	3	3	3	3	20
Bank 3	1	2	1	1	1	1	1	8
Bank 5	3	3	2	1	1	1	2	14
Bank 4	1	1	1	1	3	1	1	9
Bank 6	2	3	2	2	2	1	2	14
Bank 7	3	3	2	3	2	1	2	16
Bank 8	2	3	1	1	1	1	2	11
Bank 9	2	3	2	2	1	1	2	13
Bank 10	2	3	2	1	1	1	1	11
Bank 11	3	3	2	2	2	2	3	17
Bank 12	3	3	2	2	1	1	1	13
Bank 13	3	2	2	1	1	1	1	11
Bank 14	3	3	2	2	2	1	3	16
Bank 15	3	3	2	2	1	1	1	13
Bank 16	3	3	2	2	2	3	3	18
Bank 17	1	3	2	2	1	1	2	12
Bank 18	1	1	1	1	1	1	1	7
Bank 19	1	2	2	1	3	1	2	12
Bank 20	3	3	2	3	3	3	2	19
Bank 21	2	3	2	3	3	1	3	17
Bank 22	1	3	1	1	2	1	1	10
Bank 23	3	3	2	3	3	3	2	19
Bank 24	1	2	3	1	1	1	1	10
Bank 25	3	3	2	3	1	1	1	14
Bank 26	2	3	2	2	3	1	3	16
Bank 27	2	3	1	1	3	1	2	13
Bank 28	2	3	2	1	3	1	2	14
Bank 29	2	3	2	2	1	1	3	14
Bank 30	1	3	1	3	1	1	1	11
Bank 31	1	3	2	2	3	1	3	15
Bank 32	3	3	2	2	2	1	3	16
Average	2.16	2.72	1.81	1.84	1.84	1.28	1.97	13.6
Std Dev	0.85	0.58	0.54	0.77	0.88	0.68	0.82	3.2

a. Table 5-2 - Scoring banks based on provisions pertaining to the Rights of Data Subjects

Bank	Right to access information	Right to rectification	Right to erasure/ deletion	Right to restrict processing	Right to data portability	Right to lodge a complaint with a supervisory authority	Right to object the outcome of automated decision-making	Total score (x/21)
Bank 1	3	3	3	2	3	3	3	20
Bank 2	3	3	3	3	3	3	1	19
Bank 3	1	1	1	1	1	1	1	7
Bank 4	1	1	1	1	1	1	1	7
Bank 5	2	2	2	2	2	2	1	13
Bank 6	1	1	1	1	1	1	1	7
Bank 7	3	3	3	3	3	3	1	19
Bank 8	1	1	1	1	1	1	1	7
Bank 9	2	2	2	2	2	2	1	13
Bank 10	1	1	1	1	1	1	1	7
Bank 11	2	2	2	2	1	2	1	12
Bank 12	3	3	1	1	1	3	1	13
Bank 13	3	3	3	1	1	3	1	15
Bank 14	3	3	3	3	1	3	1	17
Bank 15	3	3	1	1	1	2	1	12
Bank 16	3	3	3	3	3	1	2	18
Bank 17	1	1	1	1	1	1	1	7
Bank 18	1	1	1	1	1	1	1	7
Bank 19	2	3	3	3	1	1	1	14
Bank 20	3	3	3	3	3	1	1	17
Bank 21	3	3	3	3	1	3	1	17
Bank 22	1	1	1	1	1	1	1	7
Bank 23	3	3	3	3	3	3	1	19
Bank 24	1	1	1	1	1	1	1	7
Bank 25	3	3	3	1	1	1	2	14
Bank 26	3	3	3	3	1	3	1	17
Bank 27	3	3	3	3	1	1	1	15
Bank 28	3	3	1	1	1	1	1	11
Bank 29	1	1	1	1	1	1	1	7
Bank 30	3	3	3	1	1	1	1	15
Bank 31	3	3	1	3	1	3	3	17
Bank 32	3	3	3	3	3	3	1	19
Average	2.25	2.28	2.03	1.88	1.50	1.81	1.19	13.0
Std Dev	0.92	0.92	0.97	0.94	0.84	0.93	0.54	4.7

b. Table 5-3 - Scoring banks based on provisions pertaining to Data Sharing

Bank	Identity of third party	Type/category of data received by third party	Purpose of processing by third party	Appropriate safeguards to be maintained by third party	Total score (x/12)
Bank 1	2	2	2	2	8
Bank 2	3	1	3	3	10
Bank 3	1	1	2	1	5
Bank 4	1	1	2	1	5
Bank 5	2	2	2	2	8
Bank 6	3	2	3	3	11
Bank 7	2	2	3	2	9
Bank 8	1	1	1	1	4
Bank 9	1	2	2	1	6
Bank 10	2	2	2	1	7
Bank 11	2	2	3	3	10
Bank 12	2	2	2	2	8
Bank 13	1	3	3	2	9
Bank 14	2	2	3	2	9
Bank 15	2	2	3	2	9
Bank 16	2	1	2	3	8
Bank 17	2	2	2	2	8
Bank 19	1	1	1	2	5
Bank 18	1	1	1	1	4
Bank 20	3	2	3	1	9
Bank 21	2	2	2	1	7
Bank 22	1	1	2	2	6
Bank 23	3	2	2	3	10
Bank 24	1	1	2	2	6
Bank 25	2	2	3	1	8
Bank 26	3	2	3	3	11
Bank 27	1	2	2	1	6
Bank 28	1	2	2	1	6
Bank 29	2	2	2	1	7
Bank 30	3	1	1	2	7
Bank 31	2	2	2	3	9
Bank 32	1	1	1	1	4
Average	1.81	1.69	2.16	1.81	Average = 7.5
Std Dev	0.74	0.54	0.68	0.78	Std Dev = 2.0

c. Table 5-4 - Overall aggregated ranking[48]

Bank	Data Collection (Rank)	Rights of data subjects (Rank)	Data sharing (Rank)	Total Aggregated Score	Overall Rank
Bank 2	1	2	2	49	1
Bank 23	2	2	2	48	2
Bank 20	2	4	3	45	3
Bank 26	5	4	1	44	4T
Bank 7	5	2	3	44	4T
Bank 16	3	3	4	44	4T
Bank 14	5	4	3	42	7T
Bank 1	7	1	4	42	7T
Bank 31	6	4	3	41	9T
Bank 21	4	4	5	41	9T
Bank 32	5	2	8	39	11T
Bank 11	4	8	2	39	11T
Bank 25	7	6	4	36	13
Bank 13	10	5	3	35	14T
Bank 5	7	7	4	35	14T
Bank 12	8	7	4	34	16T
Bank 15	8	8	3	34	16T
Bank 27	8	5	6	34	16T
Bank 30	10	5	5	33	19
Bank 6	7	10	1	32	20T
Bank 9	8	7	6	32	20T
Bank 28	7	9	6	31	23
Bank 29	7	10	5	28	24
Bank 17	9	10	4	27	25
Bank 10	10	10	5	25	26
Bank 24	11	10	6	23	27T
Bank 22	12	10	6	23	27T
Bank 8	10	10	8	22	29
Bank 4	12	10	7	21	30
Bank 3	13	10	7	20	31
Bank 18	14	10	7	18	32
				Average = 34.2	
				Std. Dev. = 8.8	

[48] For the order of ranking in the table, a score of 1 indicates the best performing bank.

Annex 6 – Selected provisions and further discussion

The privacy policy of one bank attempts to give a detailed explanation of the types of data collected and the uses of the personal data collected. Interestingly, the bank states that it collects certain sensitive personal data such as race/ethnicity, religious or philosophical beliefs, political opinions, trade union membership, health, criminal convictions and offences. The policy states that the bank collects certain technical information such as internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices that a user uses to access the bank's systems. This raises certain questions; are there limits to the type of data to be collected by banks especially in this era as banks heavily leverage on technology? How is certain data relevant to the core of banking business?

The data policy of another bank is the first to expressly limit itself to collection and use of personal information to the bank's online banking services. Therefore, it would be interesting to see whether there is another policy that regulates collection and use of non-online banking services. The bank has several online banking services that would benefit from the data policy. They include online account opening, mobile banking services and internet banking services.

The bank performs poorly at articulating the rights of data subjects as it does not provide the data subjects with any information on the rights towards their own data. The policy begins with a statement to the effect that it aims to inform customers on how the bank uses their personal data. It also makes statements that allude to the fact that the bank shares information with third parties. However, the provisions on data sharing are still wanting. For example, the policy does not reveal which 3rd party actor receives the personal information, it does not state the type of data that they receive, and it does not clearly state the appropriate safeguards to be maintained. On the part of appropriate safeguards, the policy states that the Bank *"requires all third parties with a business need to access this information to adhere to similar and equally stringent privacy policies"*. This statement does not mention what safeguards should be maintained.

The policy of another bank has a section titled 'Adherence,' which reads as follows:

> *"Your use of the Services signifies that you agree to waive your material privacy rights. You also agree not to hold [the bank] liable for use of your personal data from the Services as envisaged herein. Your use of the Services signifies your consent to allowing [the bank] to disclose personal data as envisaged herein. You agree not to hold [the bank] liable for any disclosure of such information."*

The section negates the spirit of the data policy by waiving the material privacy rights of the customers and additionally for presuming their consent.

Interestingly, some policies grant certain rights to customers from certain regions. The most common region was the European Economic Area, where banks accord citizens from this area certain rights based on the General Data Protection Regulation. This is interesting because the protections under GDPR are not based on citizenship or residency, but rather the location of the origin of the data.

Annex 7 – Readability Test

To effectively communicate to customers how data is collected and used, it is reasonably expected that the text of the policy can be comprehensible. The ease of understanding the privacy policies affects other factors such as a customer's ability to give valid consent. To determine the ease of comprehension we calculated the readability of the policies using the Flesch reading ease test.[49]

The Flesch reading ease test is a measure of the complexity of a task developed in 1948 by Rudolf Flesch. This text scoring method as well as others emerged from a desire to advocate for the use of plain English for everybody. According to this test, the lower the score is, the more difficult the text is to read. The test uses the average length of your sentences (measured by the number of words) and the average number of syllables per word in an equation to calculate the reading ease from a sample text.

The formula[50] used for the Readability Ease Score (RES) is:

RES = 206.835 – (1.015 * ASL) – (84.6 * ASW)

where:

ASL = Average Sentence Length (i.e., number of words / number of sentences)

ASW = Average number of syllables per word (i.e., number of syllables / number of words).

The RES is then a number in the range of 0 to 100. The range is a continuum, with the following providing guidance:

- scores above 90 represent a document easily understood by someone educated no further than Form 5 in the Kenyan education system;
- scores between 60-70 represent a document easily understood by someone educated through the first year of secondary school;
- scores below 30 represent a document that is easily understood by a college graduate.

[49]See Flesch, R. (1948) "A Readability Formula in Practice," Elementary English, 25(6), 344-351.
[50]See https://readabilityformulas.com/flesch-reading-ease-readability-formula.php

Table 7-1 – Readability scores

Bank	Readability Ease Score (RES)
32	53
28	48.7
7	48.7
19	45
11	43.9
14	43.9
5	43.6
18	43.1
13	40.4
9	39.9
2	39.7
1	39.3
19	37.8
17	37.1
26	36.5
15	36.4
8	35.9
12	34.9
22	33.9
21	32.5
6	32.5
29	31.5
25	31.4
30	30.9
27	30
20	29
23	28.3
16	26.9
31	26.7
3	18.4
4	18.1
24	16.9
Average	35.5
Std Dev	8.8

Annex 8 – List of Images on this Report

a. Skyscrapers on page IV
Image by Jason Goh from Pixabay

https://pixabay.com/photos/skyscraper-singapore-sky-blue-3184798/

b. Personal Banking Sign on page 8
Photo by Jonathan Cooper on Unsplash
https://unsplash.com/photos/0O2Pp6-mOkY

c. Coins on page 9
Image by Olya Adamovich from Pixabay
https://pixabay.com/photos/coins-pennies-money-currency-cash-912719/

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada

Strathmore University
Centre for Intellectual Property and Information Technology Law

Strathmore
UNIVERSITY