The Assessment of Organizations Readiness to Comply with the Kenya Data Protection Act: A Case of a Humanitarian Arganization

Francis Ndichu
Student, Department of Computing & Informatics,
University of Nairobi,
Nairobi, Kenya
Email: ndichufrancis [AT] gmail.com

Agnes Wausi
Associate Professor, Department of Computing &
Informatics, University of Nairobi,
Nairobi, Kenya
Email: wausi [AT] uonbi.ac.ke

Abstract— **Privacy is a crucial aspect of life as it impacts on how we behave, feel and make decisions. It recognizes the dignity and inherent worth of individuals. The right to privacy as a fundamental right is recognized in our 2010 constitution under article 31 sub article c & d. Kenya enacted the Kenya Data Protection Act in 2019 (KDPA, 2019) to safeguard personal information, in accordance with a set of statutory principles.**

The act requires organizations to register with data commissioner's office (ODPC), demonstrate safeguards in place for personal data processing, carry out a data protection impact assessment (DPIA) for processes that pose a significant risk to the privileges and autonomies of its citizens and report any breach within 72 hours.

In order to evaluate an organization's compliance with the act, it is imperative to perform readiness assessment to review organizations privacy practices across different domains and identify any gaps as well as the necessary steps for achieving and maintaining compliance.

To streamline readiness evaluation therefore, this study reviewed the privacy maturity models currently in use for organizations to measure their readiness to comply with privacy laws and assessed readiness of a humanitarian organization to comply with the act.

The AICPA / CICA privacy maturity model informed the readiness assessment of the humanitarian organization to KDPA compliance. The study adopted Quantitative research methodology.

The research identified regulatory, culture and technology readiness as dimensions influencing organizations readiness to comply with KDPA and to improve the overall readiness score, organizations need to put emphasis on all the three domains (regulatory, culture and technology).

Organizations can evaluate their compliance with the provisions of the act using the study's findings, identify areas of non-compliance and prioritize remediation efforts.

Keywords: [Data protection, Data Protection and Privacy readiness assessment, Data Protection Maturity model, Data Privacy}

DEFINITIONS, ACRONYMS, ABBREVIATIONS

Abbreviations & Acronyms

AICPA	-	American Institute of Certified Public Accountants
ANOVA	-	Analysis of Variance
CICA	-	Canadian Institute of Chartered Accountants
DPA	-	Data Protection Act
DPIA-		Data Protection Impact Assessment
EU	-	European Union
GAPP	-	Generally Accepted Privacy Principles
GDPR	-	General Data Protection Regulation
HRMS	-	Human Resource Management System
ICT	-	Information and Communication Technology
KDPA	-	Kenya Data Protection Act
NACOSTI	-	National Commission for Science, Technology & Innovation
NGO	-	Non-governmental Organization
ODPC	-	Office of the Data Protection Commissioner
PII	-	Personal Identifiable Information
PMAF	-	Privacy Maturity Assessment Framework
PMM	-	Privacy Maturity Model

Definition of Terms

Privacy: The right of every person to exercise ownership over their own personal information

Data protection: A legal mechanism that guarantees privacy

Data controller: Infers a person, organization or legal entity that either on its own or in partnership determines the reason for personal data processing.

Data processor: Infers a person, organization or legal entity that processes personal data on data controller's behalf.

Data subject: Any distinct individual who can be recognized, directly or indirectly, through an identifier such as a name, an ID number, location data, or through factors specific to the individual's bodily, physiological, hereditary, mental, economic, cultural or social identity.

Personal data: Any information pertaining to a data subject

Processing: Any action taken, whether manually or digitally on personal data.

Data governance: Is the process of ensuring that business systems' data is protected, accessible and available at all times based on internal data standards & regulations.

Information Security Framework: It's a set of instructions with supportive documentation that spells out policies and guidelines for the implementation and ongoing management of information security controls.

I. Introduction

As organizations race to digitize their operations, and become dependent on automated systems for day to day operations, data that is generated continues to increase in volumes. Against the voluminous daily transactions with customers are the ever-increasing threats of cybersecurity that organizations continue to face. In Kenya, over 1.2 billion cyber threat events were detected by the National Computer Incident Response Team in three months between October and December 2023, [25]. Strong data safety procedures must be applied to protect information against loss, theft, and breaches.

Kenya is among the 137 countries documented to have put in place legislation on data protection and privacy through the Kenya Data Protection Act, 2019 (KDPA 2019) that recognizes privacy as everyone's right, including limiting information relating to one's private life or family from being unreasonably exposed or encroachment of their communications privacy. [4]. Our 2010 constitution also recognizes the right to privacy as an essential right and its intrusion is considered as infringement and is punishable by law.

Section 18 of the KDPA and Registration of Data Controllers and Data Processors Regulations, 2021 require all individuals and organizations, both public and private, that process personal data to register with ODPC. [14] Organizations must also demonstrate the precautions, security procedures, and mechanisms they have to secure personal information and without which they risk being penalized KES. 5 Million or 1% turn over or whichever is less.

Kenya National Digital Master Plan 2022-2032 recognizes ICT as a significant contributor towards accelerating economic growth through digitization to enable data driven decision making. Digitization will allow fast processing of large volumes of data necessitating the need for adequate data handling and management practices to guarantee user's protection placing data security as a key element in fostering corporate trust and uptake of digital services.[3] Increased compliance will help our country achieve its development objectives by strengthening sectors, building a trusted brand that position us globally as an attractive investment destination which will in turn create more job opportunities as outlined in the Digital Master Plan.

Companies must consequently embrace risk based best practices in data governance to maintain a robust information security environment. Additionally, businesses should base their investments in rights-based security gaps evaluation in the way they handle personal data. Institutions in Kenya now have a legal obligation to operationalize their privacy policies, implement safeguards on personal data, respond quickly to data subject requests, manage and disclose data breaches in line with KDPA and associated regulations.

It is with this background that there is a need for a comprehensive assessment of organizations' readiness to comply with the mandatory KDPA. The developed model was applied to a case organization in Kenya that provides humanitarian services.

II. LITERATURE REVIEW

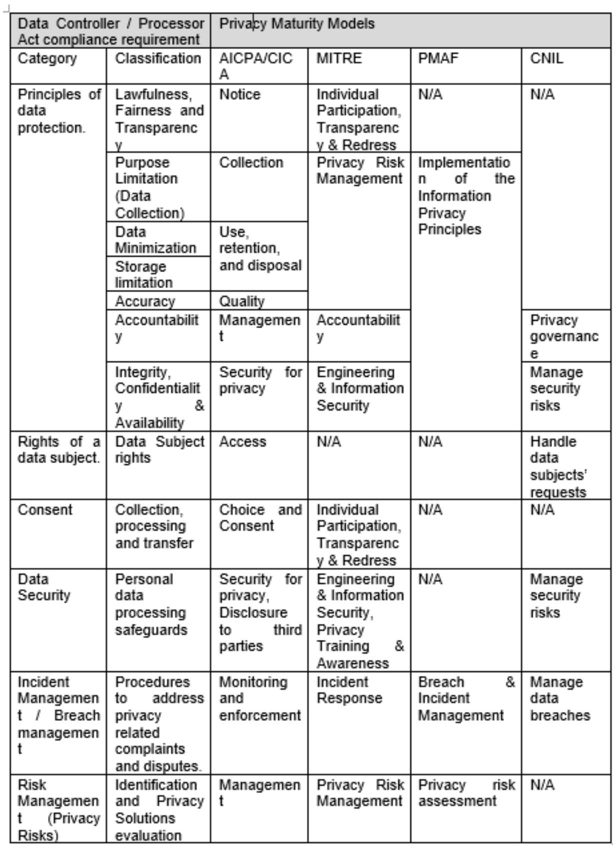
Data Protection Maturity Models

Maturity models, according to Bruin et al [10], are assessment methods used by organizations to determine their current effectiveness in a certain functional, strategic, or organizational area. The evaluation establishes a shared understanding of the kinds of changes that are most likely to help a company raise a domain's maturity level in accordance with a predetermined set of standards.

Organizations are increasingly using maturity models as a standard language to describe the present condition of their privacy implementations. Since every organization is unique, many different paths may be undertaken to bring about the desired outcome after the assessment.

The study analyzed and compared four privacy maturity models against the KDPA 2019. i.e. (AICPA/CICA, MITRE, PMAF, & CNIL) all stemming from different privacy laws being used to assess and improve their privacy management practices. AICPA / CICA PMM was consistent with KDPA and therefore considered as the foundation of the readiness assessment model developed. A comparative analysis is provided in Table 1 below.

Table 1 Comparative analysis against privacy maturity models



Data Controller / Processor Act compliance requirement		Privacy Maturity Models			
Category	Classification	AICPA/CICA	MITRE	PMAF	CNIL
Principles of data protection.	Lawfulness, Fairness and Transparency	Notice	Individual Participation, Transparency & Redress	N/A	N/A
	Purpose Limitation (Data Collection)	Collection	Privacy Risk Management	Implementation of the Information Privacy Principles	
	Data Minimization	Use, retention, and disposal			
	Storage limitation				
	Accuracy	Quality			
	Accountability	Management	Accountability		Privacy governance
	Integrity, Confidentiality & Availability	Security for privacy	Engineering & Information Security		Manage security risks
Rights of a data subject.	Data Subject rights	Access	N/A	N/A	Handle data subjects' requests
Consent	Collection, processing and transfer	Choice and Consent	Individual Participation, Transparency & Redress	N/A	N/A
Data Security	Personal data processing safeguards	Security for privacy, Disclosure to third parties	Engineering & Information Security, Privacy Training & Awareness	N/A	Manage security risks
Incident Management / Breach management	Procedures to address privacy related complaints and disputes.	Monitoring and enforcement	Incident Response	Breach & Incident Management	Manage data breaches
Risk Management (Privacy Risks)	Identification and Privacy Solutions evaluation	Management	Privacy Risk Management	Privacy risk assessment	N/A

III. METHODOLOGY

PROPOSED CONCEPTUAL FRAMEWORK

The study then focused on three constructs (technological readiness, regulatory readiness and organizational cultural readiness) for the assessment of compliance readiness

Proposed model for assessing data protection compliance readiness thus developed is illustrated in figure 1.

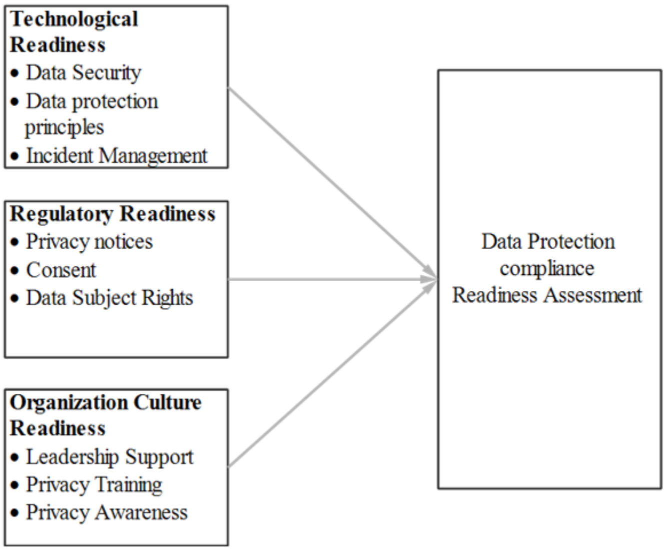


Figure 1 Conceptual framework for Data Protection Compliance Readiness Assessment

Technological Readiness

Technology is the cornerstone of adhering to the KDPA due to stringent reporting requirements, adherence to data protection principles, data breach & incident management, and DPIA for processes that put data subjects' rights and freedoms at danger. This indicator assesses the technologies in place to ensure privacy in the context of personal information.

Regulatory Readiness

The Act requires organizations to register with ODPC and to establish legal and institutional processes that secure and allow personal data to be processed in conformity with KDPA. This parameter will therefore assess privacy notices in place, consenting processes and procedures, and systems to protect data subjects' rights.

Organizational Culture Readiness

A shared knowledge of how personal data can and should be used to support more general strategic goals can be found in an organization with a strong privacy culture. This indicator will evaluate perceptions that are established within the organization by privacy practices, privacy awareness training conducted and the approach taken by the senior leadership and how that affects compliance maintenance.

IV. RESEARCH INSTRUMENTS

The study adopted a survey design for the case organization, which involved developing a survey questionnaire in line with the assessment conceptual framework. The questionnaire adopted a five-point Likert scale structured questionnaire. The rationale to adopting this design include the ability to alludes to an empirical analysis helpful for determining whether scientific theories and models actually function in the real world. [22]

V. DATA COLLECTION

The case organization in the study was an international humanitarian organization that has been operational in Kenya for over thirty years. The study used a quantitative method of data collection. The population for the study were participants from the humanitarian organization's 6 directorates with a total of 812 staff. The staff were sampled using stratified random sampling proportional to the directorate size, thus the directorate serving as the stratum. The participants to be interviewed in each stratum were selected through random sampling from the sampling frame obtained from the organization's HRMs System. Everybody in the stratum had an equal opportunity to be picked as a respondent.

Hypergeometric distribution formula was used to calculate the sample size of 268 participants [14]. A 95% confidence level with a 5% significance level was utilized, where N represented the total population size, n the sample size studied, and e represented the margin of error that was calculated at 5% [27].

To accomplish the research objectives, a questionnaire was used to collect primary data. A self-administered approach was used where a google form link was sent to all staff through email requesting staff to fill the questionnaire online and submit. Collected data from 268 participants was cleaned and quality assured before the analysis was done. Cleaning procedures included completeness checks, validity and consistency of the responses. Cleaned data was then summarized with descriptive statistics: that is, mean and standard deviation for continuous variables and frequency counts and proportions for categorical variables.

Culture, regulatory and technology readiness composite scores were generated by summing the responses from each individual question asked under each of the domains and converting to a percent score of the total expected sum. Overall percent score was obtained by summing all the responses from all the questions across the three domains and converted to a percent score of the total expected sum. The score was interpreted on a scale of 0-100 where the closer the score is to 100 the readier the organization is to conform with KDPA.

To examine factors associated with readiness to comply with KDPA which is a continuous variable, ANOVA technique was used. For a significance level of 0.05, all estimates whose p-value were less than 0.05 were considered significant. Cronbach alpha was used to assess reliability of the survey instrument. A Cronbach Alpha coefficient of 0.7 and above is considered acceptable [22].

To examine the relationship between the dependent variable (organizational readiness score) and the independent variables (technology score, culture score and regulatory score), multiple linear regression was estimated. The general linear regression equation used is;

$$y=\beta_0+\beta_1 x_1+\beta_2 x_2+\beta_3 x_3+e$$

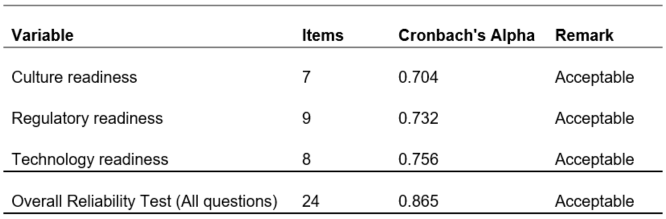
where
y=Organizational readiness score, x_1=Culture score, x_2=Technology score and x_3=Regulatory score,
e=error term, β_0 is the model intercept (constant), β_1 is the coefficient for culture score, β_2 is the coefficient for technology score, β_3 is the coefficient for regulatory score. Linear regression was used because the dependent variable is continuous. Data analysis was done using Stata v17.

VI. FINDINGS

The study targeted to interview a minimum of 268 participants. The questionnaire was sent to all staff with anticipated response rate above 50% to be considered satisfactory. However, the response rate was higher than anticipated with 350 participants submitting the questionnaire and answering every question. This equates to a 130% response rate, which is an acceptable representation of the research sample and increases the statistical power of the sample.

Reliability test was conducted before actual analysis was conducted. The Cronbach's alpha coefficient of 0.865 in table below indicated that the results were reliable. This was deemed acceptable [22].

Reliability Statistics table



Variable	Items	Cronbach's Alpha	Remark
Culture readiness	7	0.704	Acceptable
Regulatory readiness	9	0.732	Acceptable
Technology readiness	8	0.756	Acceptable
Overall Reliability Test (All questions)	24	0.865	Acceptable

The descriptive findings were as follows:

Majority of the survey participants were male (63%) followed by female at 36% of the sample while a small percentage (1%) preferred not to disclose their gender. The age distribution revealed that the largest group (41% of the population) was between the ages of 30 and 39, followed by those between the ages of 40 and 49 (36%) while those 18-29 years accounted for 17%. In terms of education, most respondents held undergraduate degrees (48%) or postgraduate degrees (37%) while a small percentage held a diploma (10%) or certificate (5%). Majority of participants were staff members (86%), with 12% representing departmental heads and 2% senior leadership. Additionally, a larger portion of the staff was field-based (64%) compared to those based in the head quarter (36%). Most participants had been working in the organization for more than 5 years (47%), followed by those with 0-2 years of experience (38%).

Organization Culture readiness

The majority of respondents (96%), had heard of KDPA. However, the majority of participants (52%), perceived their understanding of the KDPA to be moderate. 91% reported that the organization facilitates staff awareness sessions. 75% of respondents agreed that their organization has an internal regulatory framework in place to handle privacy and data protection issues but only 39% reported to have been trained on this framework. This finding is in line with a study on End User Behavior and Corporate Culture, that affirms that firms require more than an annual awareness training to improve their staff behavior. [21]. This is an opportunity for organizations to expand the scope of their awareness program to foster a culture of privacy by design and default.

Analysis further details that 77% of participants perceived the organization’s board / Executive support the compliance process. This finding is consistent with the findings of an intervention study [2] that information security culture is dependent on senior leadership, focus, actions, and attitudes.

Regulatory Readiness

The KDPA requires organizations to provide consent forms that are simple, clear and in an understandable language [13]. Respondents generally perceived the consenting process / procedures to be clear (77%). Consenting processes and procedures need to be reviewed based on the score responses. With the advancement in technology being witnessed in the 21st century, Medine and Murthy, 2020 [17] suggests that for consenting processes and procedures to be more effective, organizations must adopt new approaches that goes beyond data subjects consenting and impose a reasonable burden on data processors and controllers to act on data subjects' interest by subjecting processing to KDPA principles to offer sufficient protections of personal data.

Technological Readiness

A significant majority of the respondents (83%) agreed that their organization ensures personal data is only used for the intended purpose after being collected. Respondents (78%) reported awareness of the organization's policy on information security backed by appropriate security measures with an almost similar percentage (74%) reporting awareness of policies and procedures to manage incidents and breaches of personal data. From this study findings, there is a proactive approach to data security and privacy within the organization as the respondents demonstrated measures their organization has put in place to safeguard against personal information.

Factors associated with the readiness to comply with DPA, 2019

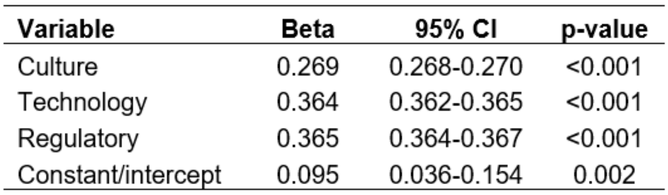
This was examined using bivariate analysis of variance between readiness scores and the socio-demographic characteristics. Results show that there were some significant differences in readiness scores by sex, education level, directorate respondents served and the number of years in the organization. Specifically, Technology readiness scores were higher among those with lower education levels (certificate=75% and diploma=77%) compared to those with higher education (undergraduate degree=66% and post graduate degree 67%). This finding contradicts (Rogers, 2003)'s [21] research findings on the relationship between higher levels of education and adoption of an innovation.

Overall readiness score also increased by the years one had worked with those who had worked over 5 years having higher scores of 72% compared to those who had worked 3-5 years with a score of 68% and those who had worked for 0-2 years with a score of 66% (p=0.008). The same trend was also observed in the technology readiness score with those who had worked over 5 years having higher technology readiness score of 73% compared to those who had worked 3-5 years with a score of 70%. Incorporating more awareness training during onboarding is deemed to improve the percentage score.

Regression Model

The study sought to establish the effect of culture, regulatory and technology readiness score on the overall organization readiness. Multiple linear regression was estimated to examine the effect of culture, regulatory and technology scores on the overall readiness of the organization. The overall model diagnostics showed that the variables fit the model adequately (p<0.001). The coefficient of determination (R2= 0.91) shows that the model explained 91% of the variability in the dependent variable (organization readiness).

Regression model examining effect of culture, regulatory and technology readiness scores on the overall readiness of the organization.



Variable	Beta	95% CI	p-value
Culture	0.269	0.268-0.270	<0.001
Technology	0.364	0.362-0.365	<0.001
Regulatory	0.365	0.364-0.367	<0.001
Constant/intercept	0.095	0.036-0.154	0.002

From the model results, for every one unit increase in culture score, organization readiness would increase by 0.27 units (p<0.001) and for every one unit increase in technology score, the organization readiness would increase by 0.36 units. Further, for every one unit increase in regulatory score, the overall organization score would increase by 0.365 units.

The model summary is therefore given as

y=0.095+0.269x_1+0.364x_2+0.365x_3

where y=Organizational readiness score, x_1=Culture score, x_1=Technology score and x_1=Regulatory score

From the analysis, the results show that there was a direct positive relationship between the scores (technology, culture & regulatory) and the overall readiness. This means an increase in technology score, culture score and regulatory score would result in increase in the overall readiness to comply with KDPA. The three factors are therefore important and organizations need to consider them to be fully compliant with KDPA and in doing so demonstrate safeguards in place to protect personal data. These findings are similar to a study by Da Veiga and Eloff (2010) [6], who argued that external factors to an organization, such as legal and regulatory systems, as well as internal factors like the information security policy, are critical components of an information security culture.

VII. CONCLUSION

The research identified regulatory, culture and technology readiness as dimensions influencing organizations readiness to comply with KDPA and to improve the overall readiness score, organizations need to put emphasis on all the three domains (regulatory, culture and technology).

The organization shows a willingness to sustain compliance with KDPA and has implemented measures across the three domains according to the study outcomes.

The finding of this study can therefore be used by organizations to evaluate their compliance with KDPA requirements, identify areas of non-compliance and prioritize remediation efforts.

The study compliance readiness score demonstrates organization's commitment to sustain compliance status across all three domains. More awareness training needs to be conducted for staff to be fully oriented on their obligations under the act. Consenting processes and procedures need to be reviewed based on the score responses. Organizations should assess their compliance score on a regular basis in an effort to reach the highest compliance score of 100%.

VIII. LIMITATIONS OF THE STUDY AND FURTHER RECOMMENDATION

More case studies should be done to test the privacy maturity model in order to offer a standard for automating the tool for organizations to comply with the KDPA.

IX. COMPETING INTERESTS

Authors have declared that no competing interests exist.

X. AUTHORS' CONTRIBUTIONS

All authors read and approved the final manuscript.

XI. ACKNOWLEDGMENT

I would like to express my gratitude to the God Almighty for His grace during the study. I appreciate the support & guidance of the School of computing through my supervisor Professor Agnes Wausi for her invaluable support, insightful feedback and encouragement throughout this journey. Grateful to, Mr. Christopher Moturi, Dr. Ruhiu, Dr. Almaz, & Dr. Muchemi for the candid feedback that enhanced the project work. Grateful to my circle of friends and family for the support and prayers to push the project to this far. I acknowledge the respondents who filled out the survey questionnaire for their participation and being instrumental in enriching this research.

REFERENCES

[1] AICPA/CICA. (2011). Privacy Maturity Model. Retrieved February 4, 2023, from https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf

[2] Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29, 432-445.

[3] Authority, I.C.T (2022). The Kenya National Digital Master Plan. https://cms.icta.go.ke/sites/default/files/2022-04/Kenya%20Digital%20Masterplan%202022-2032%20Online%20Version.pdf

[4] Constitution of Kenya (2010).https://kenyalaw.org/lex/actview.xql?actid=Const2010#sec_31

[5] Creswell, J. W. (2013). Research design: qualitative, quantitative, and mixed methods approaches. Los Angelis: SAGE Publications Ltd.

[6] Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture," Computers & Security, Vol. 2010, No. 29, pp. 196-207

[7] Data Protection (Complaints Handling and Enforcement Procedures) Regulations, (2021). (Data Protection (Compliance and Enforcement) Regulations, 2021 – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke))

[8] Data Protection (General) Regulations, (2021) (Data Protection (General) Regulations, 2021 – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke))

[9] Data Protection (Registration of Data Controllers and Data Processors) Regulations, (2021). (Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke))

[10] De Bruin, T.; Rosemann, M.; Freeze, R.; Kulkarni, U. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model.ACIS 2005 Proceedings. Australasian Chapter of the Association for Information Systems.

[11] France/CNIL: Privacy maturity model, Web: https://www.privacydesign.ch/2021/09/10/france-cnil-privacy-maturity-model-with-self-assessment/ (2021)

[12] General Data Protection Regulation (GDPR) (EU) 2016/679. (REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) (europa.eu))

[13] International Network of Privacy Law Professionals (INPLP). Accessed on 06 May 2023 https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/

[14] KDPA. (2019). https://www.odpc.go.ke/download/kenya-gazette-data-protection-act-2019/?wpdmdl=3235&refresh=64d810be383e81691881662

[15] Kothari, C.R. (2004) Research Methodology: Methods and Techniques. 2nd Edition

[16] Mena Financial Crime Compliance Group (MENA FCCG 2021): A Practical Guide: Establishing a Privacy and Data Protection Framework (https://menafccg.com/wp-content/uploads/2021/03/Privacy-and-Data-Protection-Guide.pdf)

[17] Mugenda, O.M., & Mugenda, A.G. (2003). Research methods.(3rd Ed.). Nairobi: Act Press publication.

[18] Murthy, G. and Medine, D. (2020). New Approaches to Data Protection and Privacy

[19] NGOs Co-ordination Board. (2023). Annual NGO Sector Report Year 2021/2022.https://ngobureau.go.ke/wp-content/uploads/2023/06/AR-Booklet.pdf

[20] ODPC. (2023). Register of Data Controllers and Data Processors. https://www.odpc.go.ke/registered-data-processors-and-controllers/?

[21] Ponemon Institute data breach 2022. Accessed on 08 July 2023

[22] Robert K. Yin. (2014). Case Study Research Design and Methods (5th ed.)

[23] Rogers, E.M. (2003). Diffusion of innovations (5th ed.). New York: Free Press.

[24] S. Woodhouse. (2007) Information Security: End User Behavior and Corporate Culture. Proceedings of the Seventh International Conference on Computer and Information Technology. IEEE.DOI 10.1109/CIT.2007.186.

[25] Taber, K.S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Res Sci Educ 48, 1273–1296. https://doi.org/10.1007/s11165-016-9602-2

[26] THE MITRE CORPORATION: Privacy Maturity Model, Web: https://www.mitre.org/publications, (2019)

[27] The National KE-CIRT/CC (2023). The National KE-CIRT/CC 2023-24-Q2-Cyber-Security-Report.https://ke-cirt.go.ke/wp-content/uploads/2024/01/2023-24-Q2-Cyber-Security-Report_compressed-1.pdf

[28] United Nations Conference on Trade and Development (UNCTAD). 2021. Data Protection and Privacy Legislation Worldwide? Accessed on 16 July 2023 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[29] Warren, S. and Brandeis, L.D. (1890). “The right to privacy”, Harvard Law Review, Vol. 4 No. 5, pp. 193-220.

[30] Yamane, T. (1967). Elementary sampling theory