TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Vera Akinyi Onunda 177779IVSB

Small and Medium Enterprises and the 2019 Data Protection Act in Kenya: A Cybersecurity View

Bachelor’s thesis

Supervisor: Kaido Kikkas
Ph.D. Engineering
Taltech

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Vera Akinyi Onunda 177779IVSB

VÄIKESED JA KESKMISE SUURUSEGA ETTEVÕTTED JA 2019. AASTA ANDMEKAITSESEADUS KEENIAS: KÜBERTURVALISUSE VAADE

Bakalaureusetöö

Juhendaja: Kaido Kikkas
Ph.D. tehnikateaduste doktor
Taltech

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Vera Akinyi Onunda

01.12.2020

Abstract

Kenya passed its first data protection legislation Kenya Data Protection Act 2019 to protect the right of its citizen's private information. The purpose of this thesis to find out whether cybersecurity in SMEs has improved since the inception of the Kenya Data Protection Act of 2019. The study aim was to identify the level of preparedness in SMEs in terms of compliance with the new Data Protection Act and identify challenges they faced if any.

To carry out the cybersecurity assessment an online survey using Google Forms a survey administration software was used and the results were analysed. A comparative analysis is also done based on international experience versus a Kenyan experience on data protection regulation enforcement. It can be seen that some SMEs had taken initiative to comply with others partially implementing data protection measures. The study then concluded that Small enterprises were ready to comply with the Kenya data protection requirements, despite financial constraints and lack of clear guidelines on how to go about it. It also concluded that the medium enterprises, seem to have already begun in the process of trying to comply with the Kenya data protection act, despite financial constraints but still need the guidance of how to go about it.

This thesis is written in English and is 58 pages long, including 6 chapters, 10 figures, and 4 tables.

Annotatsioon

Väikesed ja keskmise suurusega ettevõtted ja 2019. aasta andmekaitseseadus Keenias: Küberturvalisuse vaade

Keenia võttis enda kodanike privaatsete andmete kaitseks vastu Keenia andmekaitseseduse(edaspid AKS). Käesoleva bakalaureusetöö eesmärgiks on teha kindlaks, kas ja mil määral on väikeste ja keskmise suurusega ettevõtete küberturvalisus, peale AKS vastuvõtmist 2019.aastal paranenud. Töös oleva uuringu sihiks on teha kindlaks ettevõtete AKS-iks valmisoleku tase ja leida võimalikud kitsaskohad.

Küberturvalisuse hindamiseks viidi Google Formsi abil läbi küsitlus, mille tulemusi seejärel analüüsiti, võrreldes Keenia kogemust teiste maade omaga. Selgus, et mõned ettevõtted on järginud AKS-i nõudeid täiel määral ning mõned osaliselt. Leiti, et Keenia väikeettevõtted on hoolimata piiratud majanduslikest võimalustest ja selgete juhiste puudumisest AKS-i hästi järginud, ent suuremad (keskmise suurusega) ettevõtted on küll protsessi alustanud, ent vajaksid selgemaid juhiseid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 56 leheküljel, 6 peatükki, 10 joonist, 4 tabelit.

List of abbreviations and terms

AU	African Union
CIC	Commission for the Implementation of the Constitution
DoS	Denial of service
DPC	Data Protection Commissioner
DPO	Data Protection Officer
EAC	East African Community
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GoK	Government of Kenya
ID	Identity Document
ICT	Information and Communication Technology
IoT	Internet of Things
ISMS	Information Security Management Systems
IT	Information Technology
KDPA	Kenya Data Protection Act
KEBS	Kenya Bureau of Standards
KICA	Kenya Information and communication Act
MoICT	Ministry of Information and Communications Technology
OECD	Organization for Economic Cooperation and development
OWASP	Open Web Application Security Project
SMEs	Small and Medium Enterprises
VPN	Virtual private network

Table of contents

List of figures

List of tables

1 Introduction

1.1 Problem statement

Data protection regulation has influenced in recent years the prioritization of resources by organizations for the implementation of cybersecurity measures. Research has shown that improved cybersecurity measures in organizations are linked to the need to achieve compliance [1].

1.2 Purpose and overview

The purpose of this thesis is to review since the inception of the Kenya Data Protection Act of 2019, whether cybersecurity in SMEs has improved or not. This comes amidst the background in which the Act was launched that claimed it was in line with international standards like the Budapest convention and matched the GDPR in the European Union.

It had previously been identified that SMEs had been facing numerous obstacles and challenges complying with Information technology legislation before the KDPA due to fragmentation of legislation and lack of adequate policy on both legal or regulatory and information technology infrastructure, which were to be addressed in the new Act.

Another reason for conducting such a study was to establish if much had changed from 2016 to 2019 when the new act had been drafted and published especially in terms of enhanced cybersecurity, legal enforcement, and improved infrastructure. This would give a new opportunity to look at this old problem afresh and offer clarity and insight into a better way of resolving the same in the future.

The research also aims to fill in the literature gap on the level of preparedness of Kenyan SMEs after the implementation of the Data Protection Act 2019 and make a contribution to knowledge for future research on how SMEs can be assisted on how achieve compliance in data protection.

The thesis is organized as follows:

- Chapter two provides an overview of the rise of the information economy and the history of legislative reforms in Kenya leading towards its first comprehensive data protection law.
- Chapter three covers the research methodology used in the study.
- Chapter four provides results and analysis of data collected and compares international implementation with Kenyan experience.
- Chapter five presents the proposed guideline for SMEs concerning legal obligations and information security cybersecurity measures.
- Chapter six provides a conclusion to the research and recommendations for future work.

2 Background

2.1 Rise of the information economy

Being the most predominant form of business in both developed and developing economies, Small and Medium-sized enterprises are very important [1]. They create jobs, are a source of innovation, and are the basic foundations of a vibrant, healthy, and stable economy [2] They also exist in all sectors of the economy, from those with low capital requirements to those with high capital and knowledge requirement, i.e. agriculture, wholesale and retail, professions and manufacturing of simple to sophisticated products respectively [2]. In the past, due to their significant contribution, a lot of research has been done on how to increase their access to capital, managerial frameworks, and technical abilities to improve competitiveness, enhance their resilience and maximize their efficiency in the production and sale of products and services in a national and international level [2].

In recent years, especially between the year 2000 to 2008, with digital technological advancement, especially communication technology becoming cheaper and more sophisticated leading to a proliferation of IoT devices [3]. The number of people connected to the Internet has increased exponentially. This has changed the way we communicate and with the compounded computing power, has led to significant changes in how businesses are managed and conducted establishing an information economy [3]. Data is currently being collected, stored, analysed to derive value in a meaningful form to be used for decision making for a competitive advantage and profit-making, without the consent of users. Big data has proven to be an added valuable asset to an organization, including small and medium enterprises [4].

As small and medium enterprises worldwide are now more than ever dependent on reliable and critical data for its day to day operations. Higher volumes of data are being collected and this has led to challenges in its management and storage. The challenge, however, is that organizations no longer store information in disks and tapes attached to the back of the computer but use new and sophisticated technologies like virtualization and cloud computing now developed, managed by third parties outside your business and based in different parts of the world. This has led to organizations having to take a comprehensive and systematic approach to ensure that all data or information collected and stored is protected and handled with integrity and confidentiality and is readily available to ensure business continuity [5].

However, this has also has created an ever-present risk to the companies on their data and information assets through being illegally assessed, by people internal or external to the organization for means other than why it was collected, either for profiteering in criminal activity or use of intellectual capital for other means [6]. This unparalleled opportunity for cybercriminals has resulted in new trends or behaviours which were non-existent in the past that have greatly affected individuals, government, and organizations [7]. Business operations have been disrupted, leaving reputations in tatters and creating extra costs used in that include identifying and remedying the situation, public relations cost to remedy the damage caused to reputation and high legal costs results in business closing resulting in job losses and economic shrinkages and instability.

Many SMEs have weak data protection measures in place. In general, cybersecurity attacks towards SMEs have been on the rise with 43% of cyber-attacks worldwide targeting small businesses with 70% being unprepared to deal with cyber-attacks this is according to 2020 cybersecurity attack statistics [8]. As Incidents of information breaches are increasingly being reported in newspapers and various reports, it has led all countries worldwide to adopt new technologies or mechanisms to deter cybercriminals. They also have been a need to come up with reforms on information technology policy through the creation of new regulatory and legal frameworks to deal with this new form of criminal activity in cyberspace [6].

In May 2018 the European Union's General Data Protection Regulation came into full operation with it applying to European companies within the Union and across the globe on companies collecting personal information of its citizens [6]. It was designed to modernize the laws that protect the sensitive and personal information of users of the internet and reshaped how technology is used to store and process information for profit [9]. It also gave the user the right to disappear, as well as withdraw data from the collection [9]. This was to be adopted by the member states in their domestic laws.

In line with the prevailing international developments in the information economy, Africa also followed suit, trying to come up with its Cybersecurity template on data protection and regulation for Economic Community of West African States (ECOWAS) states in 2010. Later the Africa Union (AU) set out a standard an African standard by coming up with a convention in 2014 [10].

2.2 Legislative reforms on data protection laws in Kenya

Kenya, having being inspired by the developments of GDPR, the standard for data protection globally, has adopted many of the guiding principles and come up with Data Protection Act (2019) that mirrors the GDPR guidelines and principles [11]. This however did not come about without challenges. Like many other African countries, it had little legislation or no data protection laws nor did its constitution have any against private data protection [11].

In Kenya, the Government of Kenya (GoK) had recognized the importance of SME’s to the economy and launched the Ease of doing a business project in 2002 to provide measures and regulations for SME’s in different economies at local and national levels through their life cycle and later set out to establish a long term blueprint of industrialization, Kenya Vision 2030 [12]. In the blueprint, it was recognized that Kenya needed to do a comprehensive and thorough analysis of six economic subsectors and deliver growth of 10% in several sectors including wholesale and retail, manufacturing, business process, and information technology-enabled business.

This underscored the importance in which the government had to be involved in the enhancement of cybersecurity protection and regulation in SMEs as they are a vital component of the economic stability and well-being of the country as business transactions moved from the paper economy to e-commerce platforms and especially mobile payment systems. Great strides were already being made in this regards, as the ministry of information and communication technology (MoICT) the year 2000 was established with the responsibility of

“…(1) formulating, administering, managing and developing the information, broadcasting and communication policy and (2) to facilitate the development of information communication and technology sector and its regulation [13].

Before this Kenyan parliament in 1998 passed into law The Kenya Information and Communications Act, which was considered overarching law for the information technology industry. It outlined through its regulations, the requirements and compliance standards by which licensed information and communication services providers who were data collectors and controllers were to ensure the privacy of users of telecommunications through sections 31, 83 (w), and 93(1). The following year regulations for the Kenya Information and communication (consumer protection) regulations 2010 were published, with guideline 15(1) on confidentiality, further strengthen privacy laws [14].

The Kenyan journey to data protection however began in 2006, with the East African Community (EAC), a Cyber law reform program, which was intended to establish a joint EAC framework for cyber laws for its partner states [15]. This inspired the Ministry of Information and communication technology (MoICT), to publish the draft Data Protection Bill in 2009 [15]. It was however criticized for being below recommended best practice guidelines of EAC, as it only protected data held by public authorities leaving the private sector unregulated [15].

In 2010 the EAC published the EAC framework for Cyber Laws (Phase 1), which promoted the regional harmonization and a joint legal response to challenges raised by the increased reliance of commercial and administrative activities, specifically on the internet and cyberspace environment [15]. In the same year, the Kenya constitution of 1963 was changed and a new constitution of 2010 [16], under articles 31 (c) and Article 31 (d) gave express recognition to the privacy of individuals, and schedule five gave a mandate to the drafting of a Data Protection Act. This was subsequently done by the Kenya Law Reform Commission under the direction of MoICT, which addressed concerns of the draft data protection bill of 2009, but was criticized for not being focused on the rights of citizens that it was poorly drafted and did not adhere to international standards [17, pp. 24-25].

The Commission for implementing the constitution (CIC) charged with the mandate of implementing the new constitution, tried to improve the draft data protection bill and forwarded it to the attorney general to present it to cabinet [18]. On the 11th of September 2014, the cabinet approved a data protection policy which formed the basis of the bill but it was never tabled in parliament for debate but was subjected to further scrutiny and improvement [18].

In 2014, section 411A was included in the Kenya Information and Communications Act (KICA) of 1998 [19], which up to then had been an overarching law for the information technology industry, outlining the regulatory requirements and standards to be adhered to by licensed information and communication service providers who were data collectors and controllers. The section was added to promote electronic transactions which had taken route in the country. However, certain cyber offenses were not covered by the Act, leading to the convening of various state agencies and information technology stakeholders to convene and form a national cybersecurity strategy and policy, in 2016 [13] which identified the following challenges: Inadequate skills in the cybersecurity sector; Insufficient awareness of cybersecurity issues among various stakeholders; An unconducive legal framework, and lack of related institutional infrastructure for ICT development and application; Inadequate regulatory capacity, especially in the face of the convergence of networks and services; Inadequate capacity for research into ICT-related legal and regulatory issues; and absence of a culture that fosters the adoption of internet security standards in various sectors [13].

There was a need for a national cyber strategy which eventually led to the need of improving the KICA incorporate all these changes, but eventually, a new stand-alone act was proposed in 2016, the computer and cybercrimes Bill which led to the publishing of the Computer Misuse and Cybercrimes ACT of 2018, which dealt with crimes and computer-related offenses, including, critical infrastructures mobile money, cybersquatting, block chain, and cryptocurrencies, etc., strengthening multi-agency collaboration network and supporting national cybersecurity resiliency [20].

Parliament inaction continued until May 2018, when the senate published a fresh private members bill, the Data Protection Bill 2018 [21]. During the same month, the MoICT constituted a task force to develop a data protection policy and bill. The two were concurrently opened to the various stakeholders and the general public for commentary though took an unusual step that was confusing in the legislation development process. This however facilitated input and it was suggested that a consolidation of the two be done and a data protection bill 2019 came into place, being signed by the president into law on November 8, 2019, after parliamentary processes.

3 Methodology

This chapter defines the research questions and shows the research methodology used for carrying out the study.

3.1 Research Design

Descriptive research using survey research method was considered with the following steps to implement the research design:

- Identification of population to sample
- Selection of the data collection method
- Questionnaire design.
- Limitations
- Presentation of results
- Results analysis and international comparative analysis
- Conclusion

Descriptive research enables the use of both quantitative and qualitative methods in data collection [22]. The quantitative method deals with numeric while the qualitative with non-numeric data collection that is used for analysis and interpretation.

The descriptive study has no hypothesis, easily manageable, and analysed data is enough to be used to make recommendations based on the results and visualized for easy understanding [23].

3.2 Research Question

The main research questions being:

- Does the introduction of a new data protection legislation impact the improvement of cybersecurity measures in Kenyan SMEs?
- What are the challenges faced by SMEs with cybersecurity measures implementation?

3.3 Data collection method

Survey research approach through the use of google forms was selected based on the following factors:

- Response rates
- Cost-effectiveness
- Time constraints
- Best way to reach the target sample population.

Surveys usually aim at comparative and representation picture of a particular population [24]. All SMEs in the list were given a chance to respond without prejudice and to participate in the survey.

3.4 Questionnaire design

To collect data sample of the study of the problems statement, the questionnaire was formulated to cover the following broad six categories;

1. How large is your organization?
2. Does your organization keep any private records of customer data (names, addresses, telephone numbers, email addresses, etc.?
3. As far as you know, is your organization subject to the Data Protection Act of 2019? In your opinion, what are the consequences of not complying with the DPA 2019?
4. Does your organization have any measures (policies, rules, regulations, strategies, etc. in place or being planned to prevent data breaches?
5. If you use preventive measures already, how do you estimate their effectiveness? If you do not use preventive measures, then why? Mark all that apply (not subject to DPA, too costly, ineffective, lack of know-how, not necessary)
6. Which steps does your organization usually take after discovering a data breach?

Descriptive statistics estimates, values calculated from a sample, values that approximate some property of the entire population [25]. The questions took into consideration the use of the descriptive research method using both quantitative and qualitative research. The final survey questions and link to survey questions can be found in appendix 2.

3.5 Population

The study included a group of small and mediums enterprises, found in the directory of membership in various trade associations in Kenya, including the Kenya Association Manufacturers, Kenya Horticultural associations, Kenya Medical Association, Kenya Insurance Association, Kenya Bankers Association, etc. who willingly participated in the research process and were informed that the survey was anonymous and all their responses will be confidential.

The participants were all voluntary, taken from across samples of various sectors in which SMEs operate. They were informed of the confidentiality and anonymity of the survey through an email introductory text.

3.6 Research Limitations

A questionnaire was designed, which consisted of 6 broad areas and 9 survey questions in addition to an open field question. The survey was designed with simplicity and user-friendliness in mind and administered through survey administration software Google forms. Despite this, several challenges occurred, this included:

- Time constraints affected the sample size. Interviewees were time-constrained to carry out the exercise to do a comprehensive study.
- Responses were not so forthcoming (non-responders) and were not all received in time this also affected the sample size. The author found that this could be an area that would benefit more from a more comprehensive and exhaustive study.
- Participants did not respond adequately, as they seem to have feared detection for prosecution if they had registered nor put in place compliance measures as the act was nearly one-year-old and uncertain with its enforcement since it was already made into law.
- Better design for a research question to gain more insight on the topic of using third parties to manage data with it being split into two. The question was as follows:

  Do third parties manage information for your business organization with documented agreements in place, when transferring data between your company and other organizations or individuals? Do you require the third party organization to comply with your data privacy and integrity expectations?

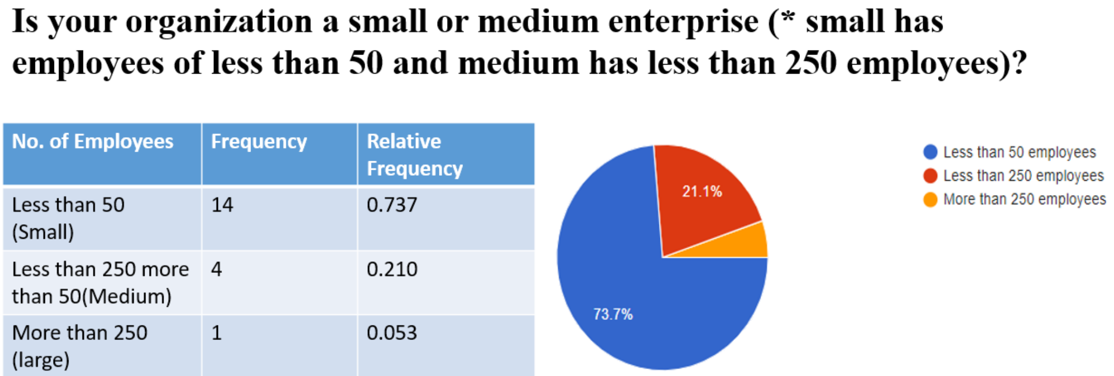
4 Results and analysis

This chapter focuses on presenting survey results, analysis of both survey results and international experience in enforcement of data protection laws internationally, and discussing the findings. The sample size was based on the 19 respondents from 200 emailed SMEs and this was used to represent the unbiased population and for data analysis.

4.1 Results

4.1.1 Size of the organization and business sector

The initial question was to find out which of the respondents fell under the category of SMEs. One objective of the study was to gauge the level of awareness of the SMEs towards the Act and what it meant in terms of impact and implications towards their business. Out of the respondents, 18 were SMEs making it 94.8% of the respondents with the majority falling under the category of small enterprises making up 73.7% of the respondents. The remaining respondent was from a large enterprise forming 5.3%. (see figure.1). These results indicated that most businesses in Kenya fall under the category of Small and Medium-sized enterprises with the minority being large enterprises and the majority being small enterprises with less than 50 employees.

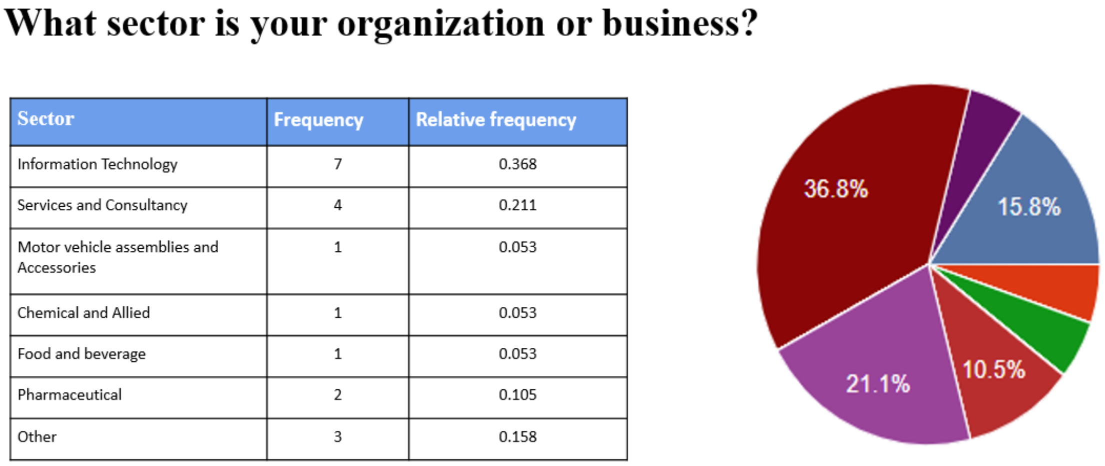


Is your organization a small or medium enterprise (* small has employees of less than 50 and medium has less than 250 employees)?

No. of Employees	Frequency	Relative Frequency
Less than 50 (Small)	14	0.737
Less than 250 more than 50(Medium)	4	0.210
More than 250 (large)	1	0.053

Figure 1. Size of organization

The majority of the respondents were in the IT sector forming 36.8% which was a total of 7 respondents with 4 that is 21.1% being in services and consultancy,2 of the respondents were in the pharmaceutical sector forming 10.5% with Chemical and Allied, Food and Beverage and Motor vehicle assemblies and accessories each being 5.3% of the total respondents with other sectors taking the remaining 15.8% (see figure. 2).



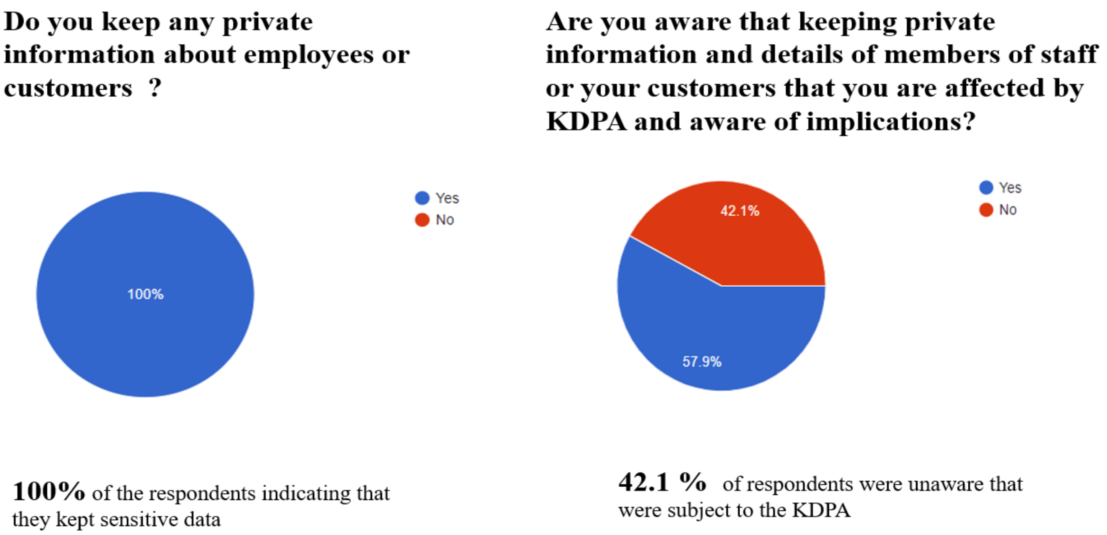
What sector is your organization or business?

Sector	Frequency	Relative frequency
Information Technology	7	0.368
Services and Consultancy	4	0.211
Motor vehicle assemblies and Accessories	1	0.053
Chemical and Allied	1	0.053
Food and beverage	1	0.053
Pharmaceutical	2	0.105
Other	3	0.158

Figure 2. Kenyan Business sectors

4.1.2 Organization keeping personal data and awareness of KDPA

To find out which of the respondents kept sensitive data and were aware of the KDPA. 100% of respondents indicated that they kept sensitive data with 57.9 % indicating they were aware of the act and its implications to their organization (see figure. 3).



Do you keep any private information about employees or customers ?

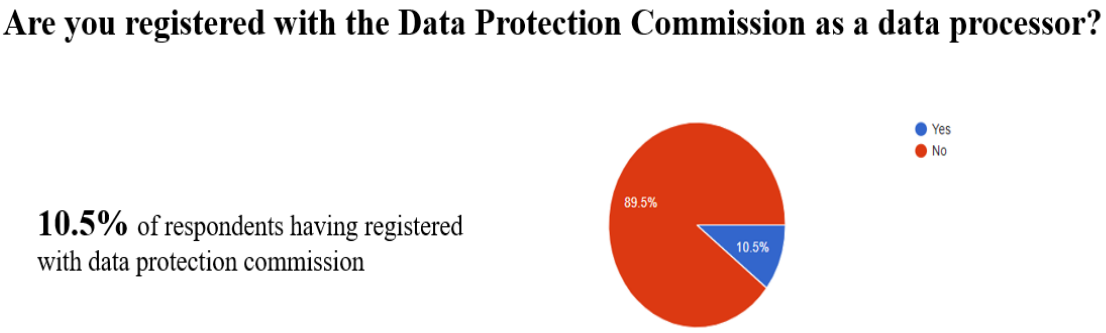
Are you aware that keeping private information and details of members of staff or your customers that you are affected by KDPA and aware of implications?

100% of the respondents indicating that they kept sensitive data

42.1 % of respondents were unaware that were subject to the KDPA

Figure 3. Data processors level of awareness

On further analysis of whether the 57.9% of respondents had taken steps or initiatives towards achieving compliance, it was seen that only 10.5% (2 respondents) took steps out of the 11 respondents who were aware of the KDPA impacts to their organization. This meant that 18.14 % of respondents aware of KDPA saw the need to register with the Data Protection Commissioner (see figure. 4).



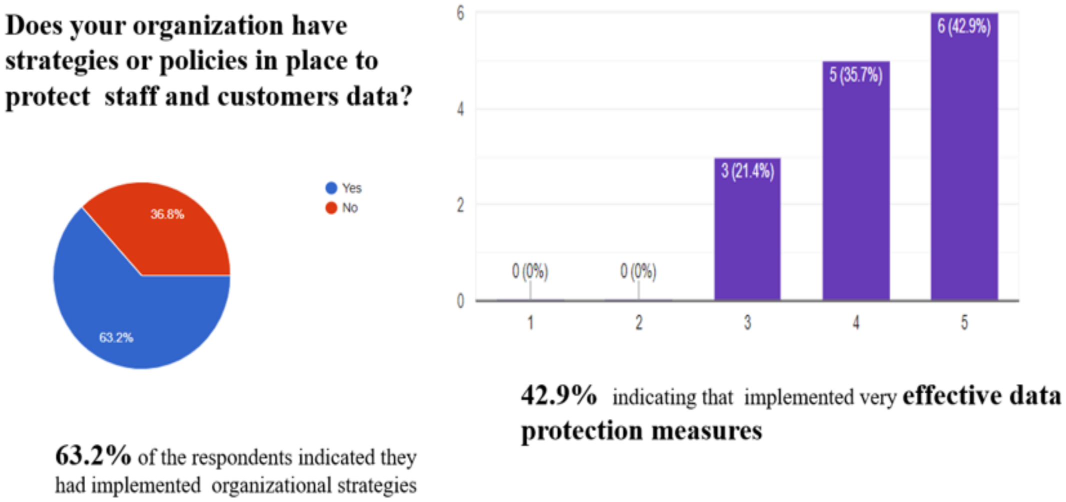
Are you registered with the Data Protection Commission as a data processor?

10.5% of respondents having registered with data protection commission

Figure 4. Registered with data protection commission

Another objective was to find out if organizations had taken any steps towards implementing data protection measures. In figure 5 it can be seen that 63.2 % (12) of the respondents had implemented data protection strategies or policies on how to protect sensitive and private data of staff and customers with 36.8 (7) of the respondents not implemented them.

4.1.3 Organizations with documented procedures and data protection measures



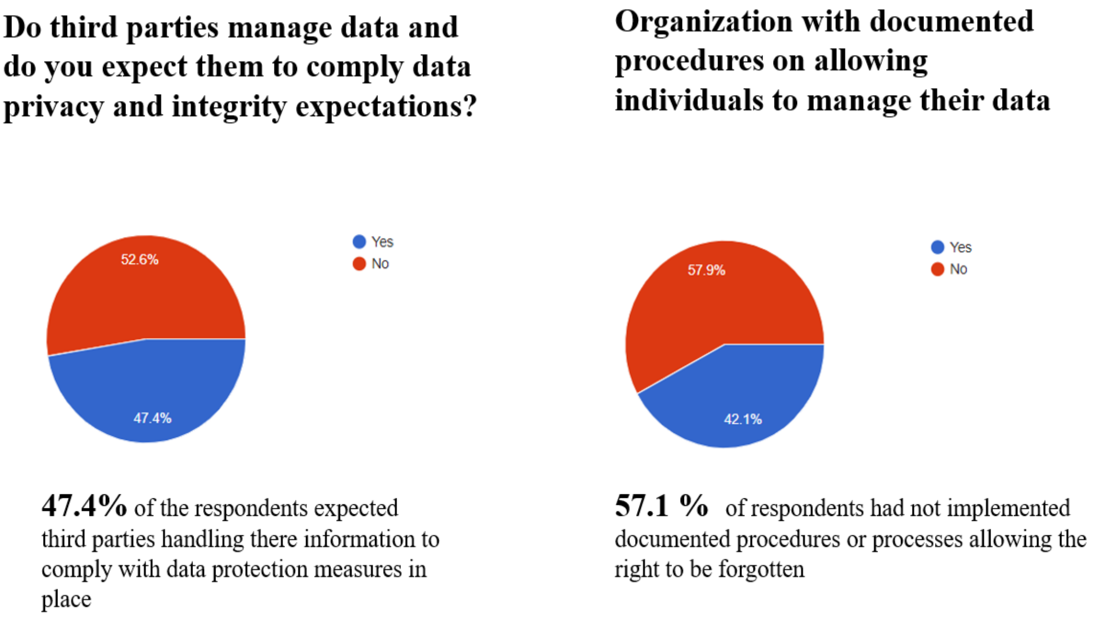
Does your organization have strategies or policies in place to protect staff and customers data?

63.2% of the respondents indicated they had implemented organizational strategies

42.9% indicating that implemented very **effective data protection measures**

Figure 5. SMEs with Organizational strategies

Data collected on organizations that had strategies in place and the responses on how effective their data protection measures were noted. 12 respondents indicated that they had organizational strategies and measures in place with .14 respondents rating the effectiveness of the organizational data protection measures and strategies in place with the medium being 4, mode 5 and this was done using the Likert scale.



Do third parties manage data and do you expect them to comply data privacy and integrity expectations?

47.4% of the respondents expected third parties handling there information to comply with data protection measures in place

Organization with documented procedures on allowing individuals to manage their data

57.1 % of respondents had not implemented documented procedures or processes allowing the right to be forgotten

Figure 6. Organizations documented procedures or Processes

It was interesting to note that 47.4% (9) of the respondents indicated they use third parties to manage their data and with documented agreements in place (see figure. 6).

In figure 6 it can be seen 42.1% (8) of the respondents had documented processes or procedures on how to manage individual requests for data access, copies, corrections, and removal of personal information. 57.1% (11) indicated that had none.

4.1.4 Challenges in the implementation of data protection measures

What are the reasons or challenges leading to your organization or business not or partially implementing preventive data protection measures

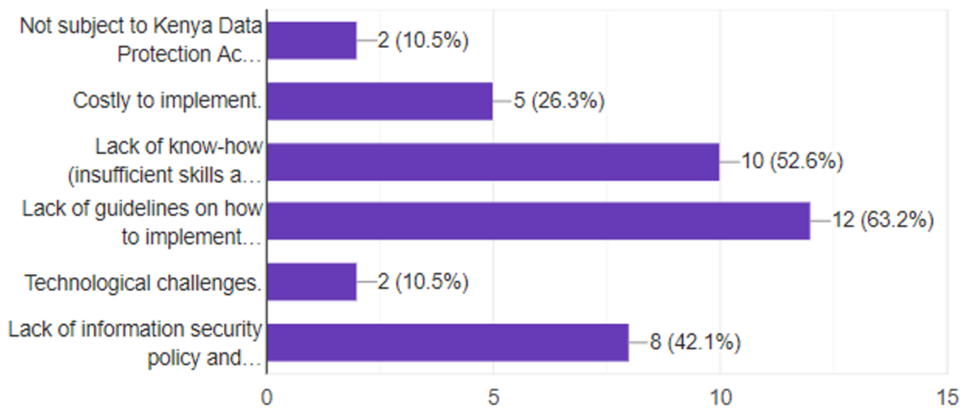


Figure 7. Challenges faced by SMEs

Challenges	**Frequency**	**Relative Frequency**	**Percentage**
Lack of guidelines	12	0.632	63.2
Lack of Know-how	10	0.526	52.6
Lack of security policies and strategies in the organization	8	0.421	42.1
Costly to implement	5	0.263	26.3
Technological challenges	2	0.105	10.5
Not subject to KDPA	2	0.105	10.5

Table 1. Frequency count on SMEs challenges

The two main reasons that respondents felt strongly about in terms of organization partially or not implementing data protection measures included lack of guidelines 63.2 % (12) of the respondents and lack of information security policies and strategies being 42.1%(10) of the respondents (see table. 1).

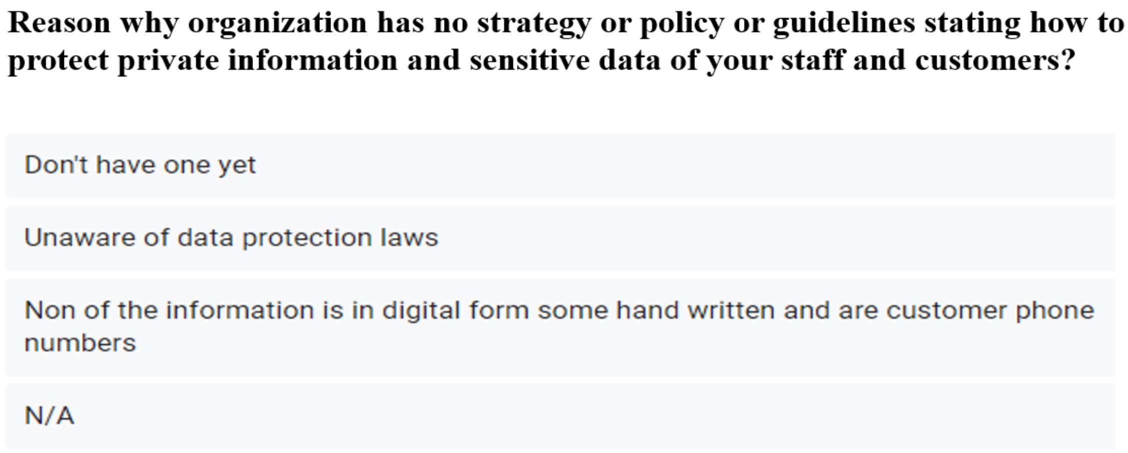
26.3% (5) of respondents felt that it was costly to implement and on further analysis of individual responses it was noted that most of the respondents who felt this way were all the respondents that fell under the category of medium-sized enterprises having more than

50 with less than 250 employees and with only one small-sized enterprise indicating the same. It can be seen that medium-sized enterprises felt more strongly about cost more than small and large enterprises.

10.5% (2) of the respondents felt that they had technological challenges in implementing data protection measures.

It was interesting to note that 10.5% (2) of the respondents felt that they were not subject to KDPA yet they kept sensitive data. It also points towards the research questions on awareness of KDPA on SMEs.

The result from the open-ended question on reason why organizations had partially implemented data protection measures and on further analysis of individual responses it was noted that first two respondents to this question both lacked awareness of the KDPA 2019 and were both small enterprises within the IT sector. One indicated just kept customers' phone numbers and private information in a non-digital format with the remaining respondent having indicated earlier that had organizational strategies in place so gave an opt-out response.



Reason why organization has no strategy or policy or guidelines stating how to protect private information and sensitive data of your staff and customers?

Don't have one yet

Unaware of data protection laws

Non of the information is in digital form some hand written and are customer phone numbers

N/A

Figure 8. Feedback on the organization's lack of strategies.

4.2 International experiences in the enforcement of Data protection regulations

4.2.1 Staggered implementation of the act

As compared to Kenya the ACT implementation stages were not staggered with a longer time lime as seen in:

- EU GDPR was enacted in May 2016 with a two-year implementation plan with enforcement taking effect in May 2018.

- POPI Act of South Africa was enacted in 2013 with three stages with the first stage encompassing the appointment of Information regulator and development of regulation with enforcement taking effect in the second stage that begun on 1 July 2020 affecting businesses and responsible parties [26].

4.2.2 Principles and obligation of personal data protection

A comparative analysis of EU GDPR and KDPA principles [16] was done as seen in table. 2

Principles relating to data processing and protection		
Principles	**KDPA 2018**	**EU- GDPR- Article**
Lawfulness, fairness, and transparency	25-b.	5-a.
Purpose limitation	25-c.	5-b.
Data minimization	25-d.	5-c.
Accuracy	25-f.	5-d.
Storage limitation	25-g.	5-e.
Integrity and confidentiality	25-3. Kenya Information and Communications Act, 1998 is inserted.	5-f.
Accountability	51-a.	5-2.

Table 2. Comparison of KDPA vs EU GDPR principles

The following principles were found to be similar with slight variation.

- **Purpose limitation**
  EU GDPR purpose limitation had some exceptions that allowed archiving for public interest, scientific, historical, research, or statistical purposes.
  KDPA purpose limitation is defined in section 39(d) with exceptions for archiving is for historical, statistical, journalistic literature, and art or research purposes [16, p. 27].

- **Integrity and confidentiality**- Kenya Information and Communications Act 1998 section 29(f) addressed this principle with a link to this added to KDPA 2019 section 41.

4.2.3 Data subject rights comparison between EU and Kenya

A comparison was done on the data subject rights between EU GDPR [27] and KDPA [16] and overview given in table 3.and a lot of similarity on the implementation noted.

Data subject rights	**KDPA -Section**	**EU GDPR- Article**
Right to be informed on the use of their data upon collection.	26-a.	13
Right to be informed on the processing of personal data by third parties and safeguards in place.	29-d.	14
Right of access.	26-b.	15
Right to rectify.	26-d.	16
Right to be forgotten.	26-e.	17
Right to restriction of processing.	34	18
Right to data portability.	38.	20.
Right to object.	26-c.	21.
Right not to be subjected to automated decision making	35.	21-22.

Table 3. Comparison between KDPA and EU GDPR data subject rights

4.2.4 Government awareness initiatives and support

Data Protection week in Europe an ongoing initiative since its inception on 26 April 2006 by the council of Europe that takes place annually [28]. It is one of the good initiatives to create awareness to everyone on their rights regarding their data. Creating awareness to individuals is needed to help them question data processors handling of their private data. This is key in helping change the laid back attitude towards security seen in organizations.

4.2.5 Challenges faced by SMEs implementing GDPR

The Star II project supported by the EU to create awareness about the General Data Protection Regulation (GDPR) in SMEs that was launched in August 2018 for 2 years recognized the following challenges faced by SMEs [29]:

- High compliance costs in terms of money and time to achieve minimum compliance due to resources (financial and personnel), cost of hiring a DPO, training, and creating awareness.
- Lack of in-house expertise with consultants being too costly.
- Challenges adapting to new regulation and incorporating into daily routines.
- Fear and uncertainty over new regulation.
- Lack of practical guidance in terms of best practices and guidelines.
- Lack of clarity around the regulation.
- The complexity of the GDPR document.

The challenge that was most worrisome to SMEs in the Star II project was noted to be time, understanding the legal terminologies, implementation of both of the technical and organizational measures and its practicality, lack of straight forward guidelines and uniformity of legal requirements for both large enterprises and SMEs. Based on the results found from the study one can see that challenges are universal and a fresh approach might be needed when implementing guidelines for SMEs in consultation with SMEs with varied resources. Key suggestions and recommendation in tackling the challenges faced by SMEs were noted in the star project as follows [29]:

- Need for more detailed how-to guidelines and sample templates.
- Clearly defined obligations for SMEs with regards to GDPR.
- The provision of e-learning resources.
- Showcasing best practices from other countries with aim of gaining knowledge.
- The provision of self-assessment tools.
- Adoption of a fear-free approach in the enforcement of compliance when regulators are dealing with SMEs.
- Create SME standards, Self-assessment tools, and newsletters for SMEs.

The recommendations could be used in future studies to further assist SMEs to achieve compliance.

4.3 Key findings and discussion

This section presents the main findings of the research. It can be seen through the results that though the level of awareness was over 50% and a few SMEs had already taken steps in achieving compliance and had effective policies and effective data protection measures in place.

The level of awareness of SMEs in regards to KDPA was partial with 58% who were aware to 42% not aware as seen in the figure. 3 and figure 4 with the number of registered respondents to the Data Protection Commission office. This may be attributed to the recent appointment of a Data Protection commissioner whose role was to enforce regulations [30] and to provide guidelines for various business sectors. The appointment took longer than the 21days after the enactment of the ACT.

Punitive fines seem not to have spurred the respondents to become compliant. This could be due to the same reasons addressed by the stakeholders in the drafting of the ICT policy 2016 were main issues mentioned include skills gap, stakeholder's inadequate cybersecurity awareness, laxity in implementation of IT security standards across various sectors due to laid back culture dealing with security-related issues (see table 2) and also legal challenges in interpreting the law due to lack of research and awareness on ICT related legal and regulatory issues [31, p. 35]. Another indicator was the two respondents who indicated that are not subject to KDPA yet kept sensitive data attributed to also lack of awareness.

Sector	**IT**		**Chemical & Allied**		**Services & Consultancy**		**Other**		**Motor vehicle and Assembly**		**Pharma**		**Food & Beverages**	
Questions	**yes**	**No**	**Yes**	**No**	**yes**	**no**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**	**Yes**	**No**
Aware of KDPA	3	4		1	4		2	1	1		2		1	
Registered with Data Protection Commission	1	6		1		4		3		1	1	1		1
Organization's data protection Strategies and policies	3	4		1	3	1	3		1		2			1

Third party managing data and policies in place	3	4		1	2	2	1	2	1		1	1	1	
Individual right To manage data Policies in place	2	5		1	1	3	2	1	1		2			1

Table 4. Sector Analysis of Cyber maturity

Table 4. indicates the cyber maturity of various SMEs across different sectors. Cyber maturity in term mainly used to determine the cybersecurity readiness within an organization using the Plan-Do-Check-Act approach based on processes, strategies, and policies in place. This involves having strategies and policies in check, being proactive in cybersecurity-related matters, measuring or having metrics in place to checkout ISMS policies have in place, and act through having preventative measures and correcting those that do not measure up.

The lack of security standards can also be seen by the number of firms certified by KEBS in regards to ISMS with only seven organizations in the country being listed [32]. This also indicates the number of organizations that have taken the implementation of security policies and compliance seriously. It can be seen the responses on organization policies and strategies (see figure. 5). The respondents selected having no organization policies in place yet had effective measures indicating they might have implemented data protection measures but lacked organizational strategies and policies. Organizational policy and compliance in terms of meeting external and regulatory requirements is an area that needs addressing and constant updating when it comes to SMEs. It can be seen through the results that out of the 63.2%(12) of the respondents with policies and strategies on data protection that only 10.5% (2) of the respondents had registered in the data protection commission indicating the lack of constant updating and improvement of security policies (see figure. 5). Another indicator could be the (42.9 %) 6 of the 14 respondents that felt that had effective data protective measures not seeing the need to constantly update organizational strategies and policies.

The challenges faced by SMEs seems to need a more proactive approach from both organizations and the government in term of creating awareness of data protection measures and legislation. The proactive approaches include organizations improving on governance in terms of strategies where use metrics to analyse data security risks within the organizations, updating company policies to also look at legal or regulatory requirements and continuous training and through educating of personnel on issues touching on cybersecurity and implementation of security best practices within the organization. The government also needs to be more proactive in the implementation of guidelines and creating awareness for both its citizens and all organizations in general in matters related to cybersecurity.

Respondents that indicated had technological challenges were all from the IT sector this also showed that more needs to be done in terms of how students are trained on matters related to cybersecurity and also this could mean there is still a skills gap in cybersecurity. The cost of training in cybersecurity and the availability of affordable courses on matters related to cybersecurity may also be a factor.

Economic challenges in terms of cost were mainly indicated by medium-sized enterprises who felt strongly as respondents that factors leading to partial implementation or not implementing data protection measures for compliance. This is seen by all respondents with more than 50 and less than 250 employees selecting this option.

Education through continuous awareness pieces of training and skills development and having mapped out guidelines are key in creating good security practices within an organization. Lack of guidelines on how to achieve compliance also was a legal challenge faced by SMEs in interpreting what the law required them to do.

4.4 Kenyan experience on enforcement of the data protection ACT

According to section 6 (3) on the appointment of data commissioner, it states that

"The Public Service Commission shall within twenty-one days of receipt of applications under subsection (2)— (b) shortlist qualified applicants; (c) publish and publicize the names of the applicants and the shortlisted applicants" [16]

Public Service Commission scheduled the conducting of interviews for more than 21 days as was required by the law. This was challenged by lawyer Adrian Kamotho leading to the suspension by the labour court on the process of appointing a Data Commissioner. The Data Commissioner's role is to oversee the implementation of and be responsible for the enforcement of this Act as seen in section 8 of the KDPA. This could be one reason why organizations were still relaxed on the data protection act especially for those who were aware.

The KDPA section 74. Further states that the Data commissioner may *"*Develop sector-specific guidelines in consultation with relevant stakeholders in areas such as health, financial services, education, social protection and any other area as the Data

Commissioner may determine” [16]. This means that various sectors may have different enforcements and different guidelines it all depends on the Data commissioner.

The lack of publication of draft regulations accompanying the act for early awareness and the wholesale implementation of the KDPA being enforced on organizations or SMEs despite their limited resources and without any government assistance on the compliance process.

5 SME guideline on data protection

This section aims to offer a simple guide to SMEs on what needs to be done as a step towards achieving compliance to KDPA 2019 from a cyber-security perspective.

5.1 Scope

The objective of this guide is to

- Provide SMEs an overview in the implementation of technical and organizational security measures on KDPA 2019 from a cybersecurity perspective best on best practices and standards.

- Encourage SMEs to use a continuous process of information security improvement based on resources at hand.

5.2 KDPA Legal obligations

According to the KDPA technical and organizational measures that must be considered under data protection by design of default by data processor or controller under section 41(4) include) [16] :

a) Identification reasonably foreseeable internal and external risks to personal data under the person's possession or control.
b) Establish and maintain appropriate safeguards against the identified risks
c) Pseudonymisation and encryption of personal data.
d) Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
e) Verify that the safeguards are effectively implemented.
f) Ensure that the safeguards are continually updated in response to new risks or deficiencies [16].

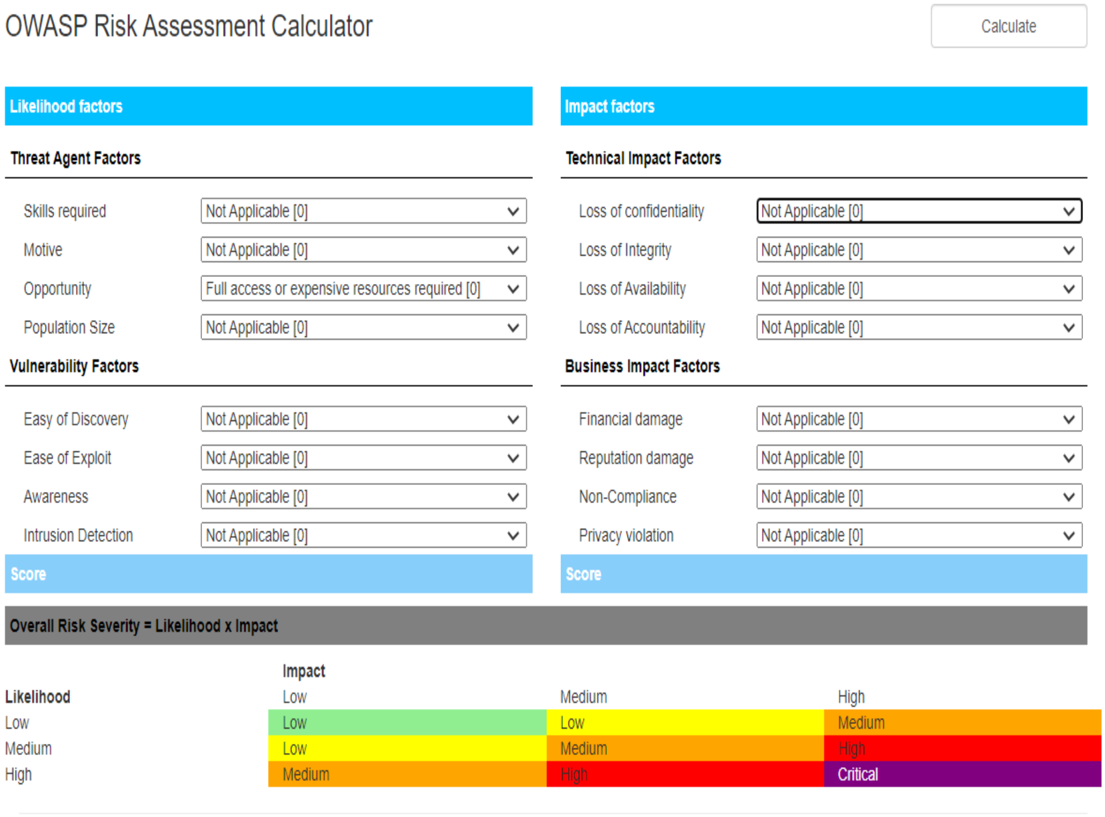
Organization measures touching on data transmission over information or communication network that controller must consider is defined in Section 42 and includes the [16]:

- State of technological development available.
- Cost of implementing any of the security measures.
- Special risks that exist in the processing of the data.
- Nature of the data being processed.

5.3 Identification and management of internal and external risks

Risks are anything that has the probability of impacting a company or business bottom line. Risks components are as follows:

- The chance an event can occur or risk (risk= impact X likelihood). OWASP offers a free risk rating calculator as seen in figure 9. an example of free online resources that can be cost-effective.
- The likelihood or chance an event can occur and is usually categorized as high, low, or medium.
- Impact or outcome if the event occurs.
- Consequences of an event if it occurs on the asset.



Likelihood factors

Threat Agent Factors

Skills required: Not Applicable [0]
Motive: Not Applicable [0]
Opportunity: Full access or expensive resources required [0]
Population Size: Not Applicable [0]

Vulnerability Factors

Easy of Discovery: Not Applicable [0]
Ease of Exploit: Not Applicable [0]
Awareness: Not Applicable [0]
Intrusion Detection: Not Applicable [0]

Score

Impact factors

Technical Impact Factors

Loss of confidentiality: Not Applicable [0]
Loss of Integrity: Not Applicable [0]
Loss of Availability: Not Applicable [0]
Loss of Accountability: Not Applicable [0]

Business Impact Factors

Financial damage: Not Applicable [0]
Reputation damage: Not Applicable [0]
Non-Compliance: Not Applicable [0]
Privacy violation: Not Applicable [0]

Score

Overall Risk Severity = Likelihood x Impact

	Impact		
Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	Critical

Figure 9. Screenshot of OWASP Risk calculator by Ivan Markovic [33]

According to the KDPA impact assessment must include [16]:

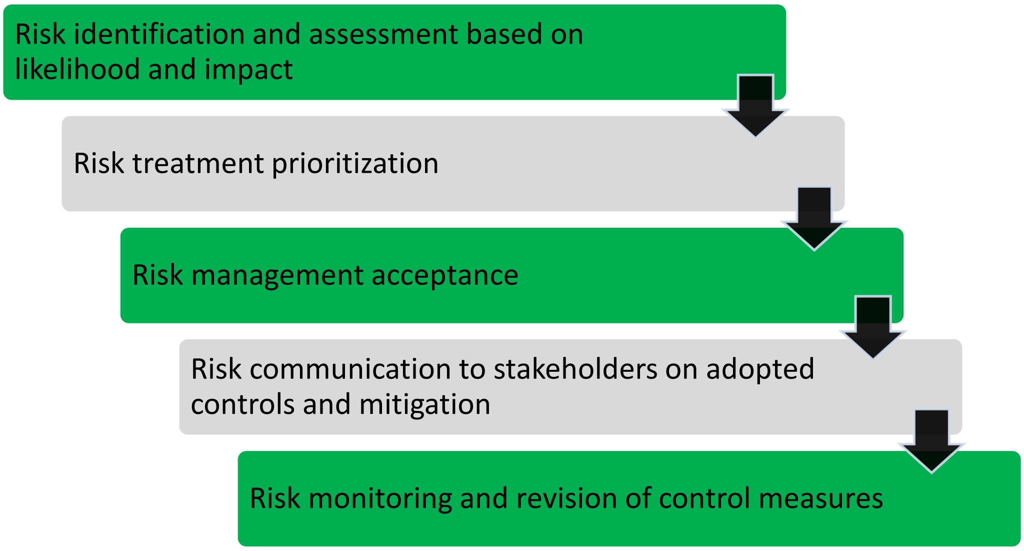
- Description of processing operations, purpose, and where the applicable legitimate interest of the data processor or controller.
- Basic processing operations with its purpose.

- Risks and rights of the data subject.
- Security measures proposed to address risks and safeguards taking into account how it has been implemented with compliance with the act, how it addresses the rights and legitimate interests of the data subject and any other concerned person.

Internal risks are the risks identified within the organizations that affect day to day operations while external risks are unpredictable risks that cannot be controlled and can include things like natural disasters and cyber-attacks. Information security is the process of implementing safeguards against the identified risks to secure data using a risk management strategy.

5.3.1 Risk Management strategy

Figure 10. defines the stages used in implementing a security risk management strategy [34].



Risk identification and assessment based on likelihood and impact

Risk treatment prioritization

Risk management acceptance

Risk communication to stakeholders on adopted controls and mitigation

Risk monitoring and revision of control measures

Figure 10. Stages in security risk management

Risks assessment helps with the identification of risks levels that are in turn used to prioritize their treatment and should be:

- Carried out by qualified personnel within ISMS trained or hired by the organization for cost-effectiveness and continuity of the risk assessment process as compared to hiring a consultant.

- Periodic for security risks evaluation in terms of the effectiveness of adopted controls and update them if needed.
- Defined and considered from the onset when dealing with external suppliers in terms of external risk assessment.

Acceptance criteria methodology to be used should be clearly defined by management and documented with:

- Baseline security criteria or minimum security objective has to be defined first for any given system with its complexity dependant on organization internal and external risks [34, p. 84].
- Adopted controls must be cost-effective with implementation cost and maintenance less than the impact of the risk to the business.

5.3.2 Asset management

Asset management must be documented as part of ISMS and entails:

- Asset identification and inventory taking of items based on information, software assets, physical assets, services, people, and intangible assets like brand and reputation.
- Linking of assets responsibility to owners, location, security controls measures like access restrictions even during disaster recovery and its maintenance throughout its lifecycle.
- Defining asset use, return on termination of contract or agreement.
- Asset classification is based on importance to the organization, sensitivity, legal requirement, and how it is assessed and handled with regular review.
- Defining secure handling procedures of assets and media in terms of removal, disposal, and physical transfer.
- Physical and environmental security for asset protection from unauthorized access with risk assessment identifying security gaps in physical controls put in place and procedures of access and security.
- Back-up equipment also should not be stored in the same place with safety measures on environmental hazards implemented.

5.3.3 Supply Chain Risk Management

Supply chains pose a risk to a business both internally and externally therefore it is key to:

- Identify suppliers allowed to access organization information and processing facilities with access controls approved and monitored by the asset owner within your organization.
- Oversee supplier lifecycle through standardized processes
- Establish access controls supplier needs to meet for business and contractual obligations.
- Establish monitoring and audit requirements based on information access in supplier agreements.
- Establish contingency plans in incident management in supplier agreements that touch on identified risks with clearly defined accountability.
- Awareness training of customers and suppliers should be done for management and mitigation of risk.
- Monitor and review suppliers' services based on performance with an individual assignment to confirm if conditions in the agreement are met.

All these should be documented in the risk management strategy or plan and according to KDPA 2019 data controller cannot transfer accountability. This is seen in penalty notice under section 62. which is determined by the Data Commissioner. The data controller should ensure all the risks from the supply chain are covered. Risks in supply chains range from external and environmental threats to geopolitical ones and include issues like quality, security, service, resilience, integrity, and health and safety [34, p. 259].

5.4 Implementation of organizational measures

5.4.1 Security management

Information security policies and management must be stipulated and approved by management and conveyed to employees after its publication. It should be consistently reviewed for business continuity and its success. This is in line with ensuring continuous updates of safeguards in regards to the changing risk landscapes and identified gaps that are outlined in KDPA 2019.

5.4.2 Business continuity management

Business continuity processes being key to the organization should be identified based on information security requirements, documented and managed through:

- Identification of business processes during risk assessment based on likelihood and impact on business.
- Mapping out the identified business processes that match a business continuity strategy.
- Identification of assets critical to the business process.
- Understanding the impact of interruptions and the effects of incidents on the business.
- Establishing adequate resources are available to address identified requirements.
- Addressing staff safety and protection of assets and information systems.
- Keeping up to date insurance covering identified risks.
- Regularly updating plans and strategies based on verifications, reviews made and improvements based on what have learned. Plans should have well-defined procedures to ensure availability and timely restoration of any interruptions affecting critical business processes with the process or system owner responsible for updating and maintaining the recovery plan with proper storage of main copies [34].

5.4.3 Organization of information security

Security policies should also cover internal organization information security and remote working procedures for effective security measures when accessing, processing, or storing data or information.

The internal organization of information security forms the baseline security criteria and involves: defining roles and responsibilities, segregation of duties where having more than one person to complete a task to minimize misuse of assets and strengthen security from within, engaging specialist forums involved with information security and having a culture of incorporating information security in project management [34].

Working from home or remotely consideration should be taken on how information assets are accessed based on permitted devices, access type granted to an employee with remote server access administration, and procedures on server policies are updated.

Employees should be made aware of security threats that may arise from mobile device use like malware, lack of accepting software updates that usually come with security fixes and patches, lack of backup procedures, and lack of physical security towards devices to prevent unauthorized access. According to OWASP top, ten mobile risks include the following [35]:

- Improper platform usage
- Insecure data storage
- Insecure communication
- Insecure authentication
- Insufficient cryptography
- Code tampering
- Reverse engineering
- Client code quality
- Extraneous functionality

Organizations when carrying out a risk assessment should come up with technological measures that are then documented as security policies for both mobile devices and teleworking or remote working to ensure effective security measures when accessing, processing, or storing data or information.

5.4.4 Human resource security

Human resource security demands:

- Implementation of background checks on potential employees based on identified risk with laws, regulations, and business needs factored in.
- Designating responsibilities and roles of employees and contractors within their contractual agreements and verifying they fulfil stated information security responsibilities according to organization policies and procedures.
- Carry out awareness training for employees and contractors in regards to updated organization policies related to their job descriptions.

- Defining of information security policies, its validity, and protection of organization with regards to change or termination of an employment contract with contractor or employee notified immediately.

- Formalization and of the disciplinary process against employees who instigates a data security breach.

5.4.5 Physical and environmental security

Involves establishing and securing boundaries around critical infrastructure accommodating sensitive information or processing facilities and protecting them from external and environmental threats. The security measures include limiting access only to authorized personnel, securing organization equipment and spaces for asset protection and employees.

Controlling of delivery or loading access points from unauthorized persons and separation of such zones from information processing facilities should also be considered.

5.5 Implementation of technological measures

5.5.1 Access management and control

Access control should be implemented with a consistent internal and external level of security to contain threats within or outside the organization. An access control policy and rules need to be clearly defined with awareness training done to avoid unauthorized disclosure of information. Access controls should be consistently monitored and constantly reviewed with its design considering:

- legislative obligation
- identified risks during the risk assessment
- information classification
- user roles and
- all security requirements reviewed like system configurations, remote access through VPNs, networks security and services, extranet for business to business (b2b) support to user authorizations to external connections.

Access to a program source code and use of utility programs that can override controls in place and system should also be restricted.

Users should be managed through the use of strongly encrypted passwords, showing of physical proof like smart card technology and biometrics-based on a combination of this method with privilege assigned based on roles. All of these should be done using secure login procedures. ISO27002 advocates users should have

- Unique IDs that cannot be easily guessed.
- Access rights documented that are approved by nominated owners that are duly signed by owners and copy given to them and HR for their personnel file indicating access rules that have to abide by before are given access.
- Removal of access rights of employees who leave the organization and IDs that are no longer used within the organization [34, pp. 162-163].

Users should be responsible for passwords by making them confidential, use two-factor authentication, regularly change their passwords, change temporary passwords, and not to the auto store unless having a passphrase or share password [34].

Verification of User IDs should be constantly checked to verify users given access match those present in the logs. Privileges should be implemented based on the system ID, privileges it contains, user category allocated that privilege, and the user is given less privilege according to secure design principles unless authorized.

5.5.2 Data security

Cryptography and Pseudonymisation

On determining the level of protection from risk assessment organizations should proceed to choose the cryptographic controls to use that are clearly defined and documented in ISMS. The policy statement should include:

- Risk being addressed and why cryptographic protection was selected.
- Access to the required level of cryptographic protection.
- Management of the encryption keys and roles and responsibilities associated with it.
- Information classification if more than one cryptographic standards are used
- Policy communicated to the user before the standard use.
- Any legislative obligation.
- Documentation if organization policy doesn’t allow encryption [34].

Cryptographic and pseudonymisation are key in protecting data at rest and are important if used effectively throughout the cryptographic key lifecycle.

In the preliminary of KDPA "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; [16] . this is similar to article 4(5) of the GDPR.

Cryptography implementation involves:

- Defining cryptographic policies and controls.
- The architectural design of a system based on identified risks
- Encryption implementation on application stack and its keys.
- Minimization of sensitive data storage
- Algorithms to use, its security level, and its key management with the key stored separately from data.

5.5.3 Operations security

Control 12. of ISO 27002 and ISO 27001 A.12 both touch on operations security. Well defined and documented procedures with responsibilities are assigned and availed to all concerned staff under guidance from the DPO or Organization information security advisor. Operation security covers:

- Change management with any changes affecting information security in an organization, business processes, information processing facilities, application software, and systems are controlled [34].
- Capacity management with system performance monitoring with regards to resource use.
- Separation of development, testing, and operational environments for minimization of unauthorized access or modification of the operational environment.
- Malware protection and awareness training.
- Regular backup of information, software, and system images based on documented comprehensive backup policy. The backup process is done automatically in a central location separate from where original data is stored. ISO 27002 recommends a minimum level of backup that is accurate with records indicating server location and time and date it was done, a backup should also be secured and if on a media tested with recovery and restoration processes well

documented, critical paper files with photocopies stored in a remote location, with expert advice given for critical applications and finally retention time of backup information defined in policies [34].

- Logging and monitoring to detect threats and anomalies, not in line with organizations policies should be considered. Anomalies could be repeated and many incorrect login attempts, network behaviour anomalies like unexplained traffic that is consistently targeting a specific point, and any deviations within the network or behaviour of users within the network. Logs help with audit trails and should be protected if kept for a limited period for investigative purposes in case of a data breach or incident.
- Event logging policy is based on risk assessment done and organization needs and is usually approved by management after information security officer recommendation. An event is an observation made from an occurrence while the incident is the accumulation of these events that leads to damage or creates a risk to the organization's assets. As a minimum, event logs should contain user IDs, dates and times of log-on log-off, terminal identity or location; details of attempted and successful and/or rejected access attempts to systems, data or applications, changes to system configurations, use of privileges, system utilities and applications, details of files and networks accessed and any alarms triggered, and details of either activation or deactivation of protection systems such as anti-malware software [34, p. 268].
- Fault logs implementation with security continuous monitoring and resolutions done upon review. All logs should have protective safeguards to ensure the integrity and also be able to be filtered for easy management and monitoring of logs.
- Paper logs kept by system or operations admin that cover incident information, the duration of events, details, errors, back-up related information, and logs on the person doing entries. This should be continuously checked and monitored and audits done as part of the incident management.
- Clocks from devices within the network should be accurately synchronized uniformly across the network for easy incident investigation and audit trails with Date Time format to be used indicated in the ISMS document.

- Controlled software installation on operation systems based on adopted procedures.
- Management of technical vulnerabilities to prevent their exploitation through timed, organized evaluation and implementation of measures addressing the associated risks.
- Carefully planned information system audit controls and verification that disrupt business processes the least while ensuring data availability.

5.5.4 Communications security

Mainly touches on network security management and information transfer. Network security controls, the security of network services, and segregation of network services are listed in A.13 of ISO 27001 and involves the protection of networks to maintain confidentiality, availability, and integrity of information systems and applications. The network manager is usually assigned this responsibility and usually helps identify security mechanisms, levels, and requirements. Networks should be continuously monitored to identify threats, tested in terms of recovery, and security procedures defined and improved on.

Information transfer policies and procedures should be clearly defined to protect all communication channels with agreements drafted if it involves third parties. Identification, documentation, and regular updating of confidentiality agreements and non-disclosure agreements should be done by an organization with electronic messaging given protective measures.

5.5.5 System development, acquisition, and maintenance

Security requirements of information systems according to ISO 27001 A.14 includes:

- Information security requirements analysis and specification.
- Application service security and protection in public networks from fraud, unauthorized disclosure, modification, and contracts.
- Protection of its application services transactions from incomplete transmissions and misrouting, unauthorized disclosure, and message alteration.

Information security in development and support processes entails:

- Established and implemented secure development policies.

- System change control procedures, technical review of application based on platform changes that can affect critical business-critical applications. Formal system change control procedures should be properly authorized with risk analysis carried out on the determined changes to ensure that data integrity, confidentiality, and availability are retained. This in turn should be properly documented based on the authorized levels, system version, audit trail on change request with system documentation and user procedures being updated and records kept in a centralized place [34] The process should be approved with verification of changes done when there is the least possible disruption to the business and with back-ups done before changes are implemented. Testing should be done and verify to ensure business-critical processes are operating as expected.
- Restriction and control on changes to software packages. Changes to software packages should be only done after a risk assessment has been done according to ISO/IEC 27002 and changes to integrity processes and controls are approved and supported by the vendor of the software.
- Implementation, documentation, maintenance, and application of secure system engineering principles.
- Establishing and Securing development environment for system development and integration during the SDLC.
- Supervision and monitoring of outsourced system development by the organization.
- System security testing to verify security functionalities implemented.
- Establishment of system acceptance testing and criteria for new information systems or changes made to old versions.

Secure systems engineering principles and methods should be also considered that touch on application security, infrastructure security for all systems and networks within the organization, and operation security on organizations systems and documented.

OWASP secure design principles [36] can be considered when implementing these measures in software and include:

- Implementing layered defence
- Implementing a fail-safe for software resilience in case of failure.
- Minimizing user access and limiting the time needed to complete operation through the principle of least privilege.

- Compartmentalization of duties through the separation of duties.
- Complete mediation where authorization is checked on every request.
- Open design where design review does not affect protective measures in software
- The least common mechanism where users and processes must be on the same level of privilege.
- Psychological acceptability promotes transparency and ease of use to the user when using the software.
- Weakest link principle where the resilience of software depends on the protection of its weakest component.

Securing outsourced development work through outsourced work that touches on organization security policies on software quality and ability to carry out audits. Software acceptance criteria should be agreed on by the stakeholders and documented. Maintenance in general also involves keeping:

- Keeping software up to date.
- Implementing controls against malware while creating awareness.
- Practicing the principle of segregation of duties where responsibilities are shared and dispersed for critical business-critical functions for sustainable risk and access control management.
- Hardware maintenance and replacement of old hardware that is not up to date for productivity and cost-effectiveness.
- Regular audits and security testing.
- Risk assessment on supplier's network security.
- Equipment maintenance.
- Have a good back-up strategy and keep inventory up to date.

5.6 Information Security Incident management

Incident management procedures should ensure continuity within the organization and should be well tested and include how to respond to incidents and have a fall back plan in case the first response is not effective. Incident management encompasses:

- Incident impact analysis

- Assigning of responsibilities and related procedures and actions to be taken in case of an incident. Response reporting procedure should be drafted by DPO or information security officer within the organization and with communication having:
    a. Information on how to report an incident and to whom
    b. time to take when responding to an event and
    c. informant being informed of response taken within a given time frame or pending resolution of the cause.
- Immediate communication to the people affected by the incident through defined communication channels. Employees should be encouraged to report any incident or event as they occur to management without fear of repercussions. Communication helps with ensuring that immediate actions are taken to ensure that new risks are quickly identified and resolved and system design is improved on by employees tasked with this role within the organizations. Communication also helps with incident management and reduce damages that may result from an event or incident.
- Internal reporting of an incident.
- Incident assessment and classification of the security event.
- Incident containment involves responding to the incident based on documented procedures.
- Collection and preservation of evidence related to the incident based on defined documented procedures.
- Documentation of steps taken to rectify and steps to take if the incident goes beyond jurisdiction.
- Improvement through learning from security incidents and using the documented steps for effective mitigation of future security incidents and review of security risks and their classifications.

Notification and communication of data breach due to unauthorized access is defined in Section 43 of KDPA and involves:

- Notification of breach within 72 hours upon becoming aware of Data commissioner.

- Inform affected data subjects on breach only when identity is known and security safeguards like encryption are not implemented by the data controller or processor with the following relayed:
    a. Description of nature of data breach.
    b. Description of measures taken to address data breach.
    c. The measures data subject should take to mitigate data breach effects.
    d. Identity of unauthorized person who accessed the data if known.
    e. Name and identity of Data Protection Officer (DPO) or contact point if data subject requires more information.
- Notification with the reason of delay if takes more than 72 hours upon discovery.
- Notification of personal data breach within 48 hours upon discovery.
- The data controller also has to record facts, the impact or effects of a data breach, and mitigation measures are taken.

5.7 Role of Data Protection Officer

The designation of the Data Protection Officer is clearly defined in section 24 of KDPA 2019 [16]. Guidelines or codes of practice may be issued by Data Commissioner for DPOs, Data processors, and controllers.

SMEs who act as data controllers or processors based on resources can obtain a DPO through hiring, assigning an employee whose tasks and duties have no conflict of interest, or through a group of entities that hires the DPO that is equally accessible by all.

A DPO should have:

- Name and contact details readily available as a point of contact to obtain information with names published by the data controller or processor on the website and communicated to the Data Commissioner.
- Relevant academic or professional knowledge and technical skills related to data protection.

The main role of the DPO will be:

- To advise Data controllers, Data Processors, or employees on legal requirements on the act and related laws.
- Ensure employer is compliant with the act.

- Facilitate capacity building of staff carrying out data processing operations.
- Provide recommendations with regards to data protection impact assessment.
- Collaborate with DPC or authorities on data protection matters.

6 Conclusion

Kenya has come a long way from not having privacy and data protection legislation despite having many challenges before inception to implementation which is an ongoing process.

However, the study concluded that:

1. Small enterprises were ready to comply with the Kenya data protection requirements, despite financial constraints, lack of financing, and lack of clear guidelines on how to go about it.

2. The medium enterprises, seem to have already begun in the process of trying to comply with the Kenya data protection act, despite financial constraints.

My recommendations, for medium enterprises, the government should come out with a financial model to support them in the implementation of the act, like in other developed countries. SMEs need training on how to prepare a general guideline on how to go on with the process, which can be improved further as time goes on, as seen below.

1. Do a gap analysis on the data your organization collects?
2. Do a cyber-risk assessment?
3. Appoint a committee to implement the project and a budget for the process of preparing relevant policies and procedures in your organization.
4. Start to implement the outcomes.
5. Review or add to the policies as required.

References

[1] "OECD.ORG," 2020. [Online]. Available: http://www.oecd.org/industry/smes/SME-Outlook-Highlights-FINAL.pdf . [Accessed 10 11 2020].

[2] N. Al-Qirim, "Electronic Commerce in Small to Medium-sized Enterprises: Frameworks, Issues.," Integrated Book Technology, 2003, p. 230.

[3] M. Pierer, Mobile Device Management: Mobility Evaluation in Small and Medium-Sized Enterprises, 2016.

[4] J. Reuvid, in *Managing cybersecurity risk*, London: Legend Press, October 1, 2019), p. 128.

[5] S. G. A. Shrivastava, "Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments 2nd Edition," John Wiley & Sons, Inc, 2012.

[6] C. A. a. W. S., "IT Governance A manager's guide to Data security and ISO27001/ ISO 27002. 4th ed.," Kogan page limited, 2008, pp. 10-15.

[7] Z. K. S. a. S. L. A. Qasimi, "Cyber Law and Cyber Security in Developing and Emerging Economies, page 230," Northampton, MA, Edward Elgar, 2010, p. 230.

[8] "Purplesec," 2020. [Online]. Available: https://purplesec.us/resources/cyber-security-statistics/. [Accessed 7 12 2020].

[9] "GDPR.EU," [Online]. Available: https://gdpr.eu/. [Accessed 1 11 2020].

[10] M. laibuta, "The International Forum for Responsible Media Blog," 18 6 2020. [Online]. Available: https://inforrm.org/2020/06/18/two-years-on-the-impact-the-gdpr-has-had-on-privacy-and-data-protection-in-kenya-mugambi-laibuta/ . [Accessed 28 11 2020].

[11] D. Coleman, "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of data protection laws," *Michigan Journal of Race and Law*, vol. 24, p. 431, 2019.

[12] W. B. Group, "Ministry of Industrialization, Trade and Enterprise development GoK," 2018. [Online]. Available: https://www.industrialization.go.ke/index.php/kenya-ease-of-doing-business-2018. [Accessed 10 11 2020].

[13] J. M. A. T. K. NANJIRA SAMBULI, "gp-digital.org," [Online]. Available: https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf. [Accessed 10 11 2020].

[14] “Communications Authority of Kenya,” [Online]. Available: https://ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010-1.pdf. [Accessed 28 11 2020].

[15] A. B. Makuliko, “,” in *African Data Privacy laws” Law, Governance and technology series 33*, Springer International Publishing AG, 2016, pp. 317-336.

[16] “Kenyalaw.org,” 3 2020. [Online]. Available: [3], 2020. [Online]. Available: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.. [Accessed 14 8 2020].

[17] A. B. Makulilo, 2013. [Online]. Available: http://repository.out.ac.tz/326/1/Kenya%27s_DP_2012-Many_leakes_still_unplugged.pdf. [Accessed 25 10 2020].

[18] A. B. (. Makulilo, in *African Data Privacy laws” Law, Governance and technology series 33*, Springer International Publishing AG , 2016, pp. 317-336.

[19] “Communications Authority of Kenya,” [Online]. Available: https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf. [Accessed 24 11 2020].

[20] “Kenya law,” [Online]. Available: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf. [Accessed 3 11 2020].

[21] “Ministryof ICT, Innovation and Youth affairs GoK,” [Online]. Available: https://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf. [Accessed 20 11 2020].

[22] “Business research methodoology,” [Online]. Available: https://research-methodology.net/descriptive-research/. [Accessed 17 12 2020].

[23] “The Association for Educational Communications and Technology,” [Online]. Available: http://members.aect.org/edtech/ed1/41/41-01.html. [Accessed 18 12 2020].

[24] B. Gillham, “Developing a Questionnaire,” London, Bloomsbury, 2008, p. 18.

[25] K. H. Jarman, “The Art of Data Analysis :,” in *How to Answer Almost Any Question Using Basic Statistics*, New York, John Wiley & Sons, Incorporated, 2013, p. 179.

[26] G. Gerber, “["Guidelines on the implementation of Protection of Personal Information (POPI) Act - SERR Synergy",” 2020. [Online]. Available: https://serr.co.za/guidelines-on-the-implementation-of-protection-of-personal-information-popi-act-by-gideon-gerber. [Accessed 28 11 2020].

[27] “Legislation: GDPR Regulations,” *Official jouranl of the EU,* vol. 59, p. 156, 2016.

[28] “Council of Europe,” [Online]. Available: https://www.coe.int/en/web/data-protection/data-protection-day. [Accessed 29 11 2020].

[29] “Trilateral research,” [Online]. Available: https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf. [Accessed 19 12 2020].

[30] “Parliament of Kenya.,” [Online]. Available: http://www.parliament.go.ke/house-committee-vets-first-data-commissioner-kenya. [Accessed 1 12 2010].

[31] "Ministry of ICT GoK," [Online]. Available: http://icta.go.ke/pdf/National-ICT-Policy-20June2016.pdf#:~:text=COMMUNICATIONS%20TECHNOLOGY%20%28ICT%29%20POLICY.%20JUNE%202016.%202.%201,employment%20creation%20as%20espoused%20in%20Kenya%E2%80%99s%20Vision%202030.. [Accessed 4 12 2020].

[32] KEBS, " (2020). ISMS Certified Firms.," [Online]. Available: https://www.kebs.org/index.php?option=com_content&view=article&id=214&Itemid=410. [Accessed 28 Nov 2020].

[33] I. Marković, "OWASP Risk Assessment Calculator," [Online]. Available: https://www.security-net.biz/files/owaspriskcalc.html. [Accessed 19 12 2020].

[34] A. a. W. S. Calder, IT Governance A manager's guide to Data security and ISO27001/ ISO 27002. 6th ed., 285-287: Kogan page limited., 2015.

[35] "OWASP," [Online]. Available: https://owasp.org/www-project-mobile-top-10/. [Accessed 2020 12 16].

[36] "OWASP DEV/GUIDE," [Online]. Available: https://github.com/OWASP/DevGuide/blob/master/02-Design/01-Principles%20of%20Security%20Engineering.md. [Accessed 10 12 2020].

[37] L. S. Sterling, The Art of Agent-Oriented Modeling, London: The MIT Press, 2009.

[38] 12 11 2020. [Online]. Available: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf.

[39] C. Neagu., " The importance and role of small and medium-sized businesses," vol. Theoretical and Applied Economics, no. XXIII (3), pp. 331-338, 2016.

[40] G. S. a. S. Alok, , information storage and management: storing, managing and protecting digital information in classic, virtualized and cloud environments, 2nd edition., 2012.

[41] "Verizon," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/. [Accessed 29 11 2020].

[42] S. Tharnish, "Security magazine," 28 02 2020. [Online]. Available: https://www.securitymagazine.com/articles/91806-as-cyber-attacks-become-more-prevalent-heres-why-your-small-business-is-at-risk. [Accessed 10 11 2020].

[43] "International trade centre," [Online]. Available: https://www.intracen.org/uploadedFiles/intracenorg/Content/Publications/Kenya_SME_Comp_final_low_res.pdf. [Accessed 11 11 2020].

[44] [Online]. Available: https://ictpolicyafrica.org/en/document/5e5qwt608ps?page=3. [Accessed 11 11 2020].

[45] "Kenya Law," [Online]. Available: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010. [Accessed 10 11 2020].

[46] [Online]. Available: http://constitutionnet.org/sites/default/files/the_data_protection_bill_2012_revised_10th_jan2012.pdf. [Accessed 12 11 2020].

[47] [Online]. Available: https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf. [Accessed 13 11 2020].

[48] “Kenya law,” [Online]. Available: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf. [Accessed 12 11 2020].

[49] D. Cramer, “Advanced Quantitative Data Analysis,” McGraw-Hill International (UK) Ltd, 2003, p. 13.

[50] A. C. &. S. Watkins, “IT Governance,” in *A Manager’s Guide to Data Security and ISO27001/ISO 27002* , London and philadephia, Kogan page, 2015, p. 368.

[51] “OWASP Top Ten,” [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed 10 12 2020].

[52] “OWASP SAMM,” [Online]. Available: https://owaspsamm.org/model/. [Accessed 7 12 2020].

[53] “NIST,” June 2009. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-46/rev-1/archive/2009-06-16. [Accessed 17 12 2020].

[54] “OWASP cheat sheet series,” [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html. [Accessed 17 12 2020].

[55] A. Werlof, 1 June 2018. [Online]. Available: https://alexewerlof.medium.com/gdpr-pseudonymization-techniques-62f7b3b46a56. [Accessed 17 12 2020].

[56] “cyberwatching.eu,” [Online]. Available: https://cyberwatching.eu/cyberwatching-information-notice-tool. [Accessed 19 12 2020].

[57] [Online]. Available: https://owasp.org/. [Accessed 19 12 2020].

[58] “ISO,” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en. [Accessed 19 12 2020].

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Vera Akinyi Onunda

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Small and Medium Enterprises and the 2019 Data protection Act in Kenya: A Cybersecurity view, supervised by Kaido Kikkas.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

01.12.2020

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2- Survey questions and responses

a) Is your organization a small or medium enterprise (* small has employees of less than 50 and medium has less than 250 employees)?

b) What sector is your organization or business?

c) Do you keep any private information about employees or customers e.g. Names, telephone numbers, physical address, emails, pictures, voice mails, etc., and is it in a centralized place, where it is stored, processes, and managed?

d) Are you aware that keeping private information and details of members of staff or your customers that you are affected by the Data Protection Act in Kenya? And can face fines for non-compliance with the Act?

e) Are you registered with the data protection commission as a data processor?

f) Has your organization written out a strategy or policy or guidelines stating how to protect private information and sensitive data of your staff and customers?

If yes, how effective are these measures?

If no? can you elaborate on the reasons why?

g) Do third parties manage information for your business organization with documented agreements in place, when transferring data between your company and other organizations or individuals? Do you require the third party organization to comply with your data privacy and integrity expectations?

h) Does the business area have documented procedures or processes to manage requests from individuals that allows them access to, copies of, corrections to, or removal of their personal information?

i) What are the reasons or challenges leading to your organization or business not or partially implementing preventive data protection measures?

PRIVACY AND DATA PROTECTION RISK ASSESSMENT OF SME IN KENYA QUESTIONAIRE (google.com)

PRIVACY AND DATA PROTECTION RISK ASSESSMENT (Responses).xlsx - Google Sheets