# DATA PROTECTION AND EXPERIENCE OF STAKEHOLDERS AT THE UNIVERSITY OF NAIROBI

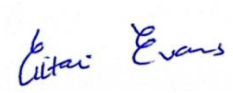
**BY**

**EVANS KINYUA GITARI**

**A MANGEMENT RESEARCH PROPOSAL SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF BUSINESS ADMINISTRATION(MBA)DEGREE-MANAGEMENT INFORMATION SYSTEM, FACULTY OF BUSINESS AND MANAGEMENT SCIENCE**

# DECLARATION

This research and proposal is entirely my own original work; it has not been presented or utilized at any other institution.

Signed  Date.....29th November 2023.....

**Evans Kinyua Gitari** **D61/38527/2020**

With my supervision and consent as the academic supervisor, this study proposal has been submitted and approved for evaluation.

Signed.....  ..... Date..... **5th December 2023**.....

**Dr. Nancy Mogikoyo Marika**

**Lecturer – University of Nairobi**

# ACKNOWLEDGEMENTS

I extend my gratitude to my supervisor, Dr. Nancy Marika, for her significant contributions and support during the creation of this research paper. The crucial factor in achieving success in this research project was her invaluable guidance.

# DEDICATION

To my father, Mr. Lloyd Gitari, my mother, Mrs. Kellen Karimi and my sibling, Martin Kirimi. Your steadfast encouragement and support during my MBA journey has my heartfelt gratitude. May God bless you all.

**TABLE OF CONTENTS**

## LIST OF TABLES

## LIST OF FIGURES

# ABSTRACT

Increasing usage of internet and computer machines over the last 30 years has increased the chances of cyberattacks, leakage of information and other unethical activity within large organizations. Kenya has laws that govern the data protection of any information stored but enforcement of such policies remains a challenge. The objectives of this study were to determine the compliance level of the university of Nairobi to data protection laws and the experiences the stakeholders have in relation to the data they have submitted to the University. Data was observed using a descriptive research design and data collected using a questionnaire administered to the stakeholders including students, teaching and non-teaching staff. Data analysis was done using SPSS version 26. Descriptive statistics including mean, frequency, percentages and standard deviations were used to determine the compliance level of the university to the data protection laws. Linear regression was used to determine how the data protection laws affect the experience of stakeholders at the university.

The regression model, with predictors relating to the data protection laws demonstrated a statistically significant relationship with stakeholder experience, The variability in stakeholder experience in safety of their data and trust in the university can be attributed to the considered data protection laws.

The study noted that the university had a high compliance level to the laws but a few gaps in compliance. The first gap was on the data protection principle of transparency where most respondents were not informed of the breaches that happened to their data. There was also non-compliance to the principle of integrity where respondents cited lack of control to their data, where the data could be changed without their authority and system instability that could cause errors and unauthorised modification to their data. Despite this, respondents had a high level of trust in the university policies of data protection and safety. They indicated would not make rush decisions in case of a breach. The study recommended the university to enhance their awareness campaigns on the breaches that happen, give more control to stakeholders and invest and upgrade their systems to strengthen data protection

# CHAPTER ONE: INTRODUCTION

## 1.1 Background of the Study

Global business and general development in the economy has led to generation of large amounts of data in public as well as private entities with the advent of improved technologies thus creating large data accessible to many individuals. However, there has been cases of cybercrimes and misuse of the data when data is used to send unsolicited content to users, when it's used to coerce users into actions, when it's accidentally revealed or lost, when it's used by government and unauthorised people for surveillance and so much more unethical activity (Kröger,Miceli & Müller ,2021). The issues have been highlighted by societies around the world and this has led to laws and regulations that prevent, detect and correct such issues with both public and private entities working to adopt or formulate policies in line with the laws (Kaplan, 2020).

Institutionally, Kenya has laws that govern data protection of any information collected, stored and used for both individuals and other entities, but enforcement of such law remains a challenge. This research will determine the compliance level of the university of Nairobi to the data protection laws relating to privacy by minimization, transparency, confidentiality, integrity and availability. The relation between the data protection laws at the university and the experiences of its stakeholders will be covered in-depth to determine opinions of stakeholders in sharing data with the university and their level of trust in security measures used by the university to secure their data.

It is expected that the university of Nairobi has complied to the government laws. Meyer and Rowan , (1977) stated that organisations comply to rules and regulations including

government laws regardless of whether they benefit from the laws or not. Compliance is seen as a requirement for survival. Pressure from its stakeholders also ensures they are collecting and processing data ethically and in accordance to the law, which is supported by the stakeholder theory (Freeman,1984). It implies that stakeholders should have an input in designing and implementing the data privacy and protection policies of the organizations.There are quite a number of researches done in relation data privacy and protection but no known study has covered compliance to already written laws in Kenya. There are currently no known studies researching the data privacy and protection experience of stakeholders in educational institutions in Kenya. The Study focuses on the compliance concept to already written laws and its relation to users.

### 1.1.1 Data protection

Data is information, facts and statistics that can be used for reasoning, transmission or discussions which can be found openly or from controlled locations requiring some form of authority for access (Odusote, 2021). This need to have controlled or authorised access to data is based on the principles of individual data privacy including; the right to be left alone, the right to have limited access to self, secrecy, the right to control one's personal data, personhood; the right to control personal identities and the right to intimacy described by Enerstvedt and Enerstvedt (2017) imply there is need for policies on data privacy and protection.

Data privacy can be violated when data is in the hands of institutions at four main stages, the first one being at the point of data collection. The second problem arises during processing, which includes storage, retrieval and alteration (Rustad & Koenig, 2019). The third one is on information dissemination where privacy is violated when information is

shared, transmitted and disclosed to third parties without consent (Anduvare & Mutula, 2019). Finally, the problem of invasion where privacy is violated through unauthorized destruction and retention of information for a person (Mwencha, Thuo & Muathe, 2019).

Solove (2008) argues that these social practices of collection, processing, dissemination and destruction, that cause privacy problems, require tailored legal and policy responses which are referred to data protection principles. The data protection principles include privacy by minimization, privacy by transparency and privacy by confidentiality, integrity and availability. The international laws, policies and guidelines that have been enacted from 1980 have addressed how data privacy and protection should be implemented by government and private entities, using these data protection principles, reflecting the increasing use of computers to process transactions. These include guidelines by the Organization for Economic Cooperation and Development-OECD-and the GDPR - general data protection regulations (Ikkinen-Piri, Rohunen & Markkula, 2018).

In Kenya, data privacy exists in its constitution under section 31. It indicates that a person has a right not to be searched, a person has the right to keep their property and possessions without seizure, they have the right to keep their communications private and also information relating to family or private affairs

Since the data privacy does not detail the practices that lead to breach of privacy and the practices required to protect that privacy, the data protection act 2019 and the data protection regulations 2021 were enacted. The two documents have information on laws, practices and technologies that companies/institutions should comply with in order to

protect personal information from unauthorised collection, processing, transmission or destruction.

The data protection general regulations 2021, section 27-part V requires data to be handled according the principles of data protection including principle of minimisation, principle of transparency as well as principle of confidentiality, integrity and availability.

### 1.1.2 Stakeholder Experience

The view of stakeholders in a firm is based on the group of people with similar or common goal to achieve (Freeman, 1984). Stakeholders of institutions/companies including customers, management and investors, have suffered severe consequences due to breaches of data privacy. A common cited example involved Target, a supermarket chain in the United States that suffered a system security breach resulting in the loss of over 70 million Credit and debit card details of their customers. This was after malware was introduced in the system. The CEO had to resign, the company and investors incurred a loss of 290 million to fix the breach (Plachkinova, 2018).

Locally in Kenya two mobile lending companies, white path company and Regus Kenya, were fined Kshs. 5,000,000 each by the office of the legal management of data due to the intrusion of their customer's mobile contacts.This is after customer compliants on social media and reporting to the data protection commissioner. The lenders were mining their customer's mobile contacts and sending threatening messages to the customer contacts in case of default (Office of the Data Protection commissioner-ODPC, 2021). This led to shame by the defaulters and privacy intrusion of the affected contacts.

In spite of all the data privacy violations, users seem to be open to sharing their data. The audit firm Ernst and Young conducted a global consumer privacy survey. The survey was to find out the awareness and attitudes of consumers towards data privacy. Younger generations (born between 1981 and 2012) are more concerned with their information power than the older generations (born between 1946-1980). However, the survey noted that the younger generations also shared their data more freely as they understood the technologies and derived benefit from the information they shared.

### 1.1.3 The University of Nairobi

This is an institution of higher learning that has its origin in 1947 when the government conceived the idea of a technical and commercial institute in Nairobi. In September 1951, a Royal Charter was issued to the Royal Technical College of East Africa and the foundation stone of the college was laid in April 1952. In 1970, the college was converted to the University of Nairobi. The university has grown to have campuses spread across the country offering different higher education courses to students (University of Nairobi, 2020).

Over the recent years the university has embarked in adoption of ICT. It uses such tools to manage its information and people. Ogutu (2017) studies this adoption and notes that the ICT tools promote information sharing in the organization.

The university has embraced open and distance learning. Online classrooms and libraries are replacing traditional campus facilities. The university is supported by the SMIS which is an Online Course Registration system. Students can self-service using this platform

(Wambugu & Kyalo, 2013) .The online systems have increased the quality of education and saved time for students and staff. They however collect huge amounts of personal information including identification information of users, financial information and other sensitive information. Currently, the university has set out to comply with the data protection laws. The laws recognize the institutions that collect data to have an obligation of protecting it.

The university has drafted and enacted a privacy policy detailing the information they collect and information they use (University of Nairobi.2023). It is posted on the university website and embedded in terms and conditions for the registration systems of the organisation. The privacy policy has information on the personal information or data that is collected by the university, the purpose for collection and processing and third parties using the data collected. The university has also registered with the data protection office as a data processor and controller as required by law (Office of Data Protection Commission, 2023)

University of Nairobi ICT annual report (2020) indicates that implementation of the requirements of the data protection laws has been hampered by reduced funding by the government, lack of adequate ICT personnel, slow procurement processes and rapid technological changes. There have however been minimal research studies on the University of Nairobi's compliance to the various articles and sections of the laws and the experience of stakeholders. This research will investigate the two issues.

## 1.2 Statement of the Problem

In Kenya, incidents of data breaches have been experienced. Personal data of company customers has been captured and used without their consent and some of it has been hacked. A survey by Communications Authority of Kenya (CA) in 2023 noted that one of the biggest threats to data protection was cyber-attacks. The organisations mostly targeted were financial, mobile service companies, healthcare and education entities. The information targeted is personal identification information, intellection property and financial information (Communications Authority, 2023)

There is a perception from some people that data protection matters to only people who have something to hide or people who commit crimes. Some people opine that data is important for analysis and decision making and therefore there should be no tough laws against its use (Kröger et.al ,2021). Due to these unethical uses of data, cyber-attacks and dangerous perceptions, most governments have come up with ways to protect customer data. In Kenya, there is the bill of rights and data protection laws of 2019 and 2021. Most scholars tackling the topic of data privacy, protection and ethics have done very little to review compliance to the laws and regulations and determine the experience of customers.

In 2021, Ernest and young surveyed the data protection principles in SACCOs, banks, insurance companies, and a number of healthcare facilities. The survey noted that 39% of the institutions did not know about the data protection act and had not complied with it. Nzuva (2019), studied the risk management of data breaches in the banking industry. The research noted that system vulnerabilities lead to data leakages and cybercrimes in banks. To prevent and recover from data breaches, it was recommended that banks consider back up plans like disaster recovery plans, strong and effective system architectures and consider

risk transference measures like use of the cloud.Ayugi (2021) conducted research on health institutions and noted that the institutions had robust data security strategies but still struggled with training staff, managing their insufficient budgets, keeping up with digital innovations and complying with the changing regulations. The researcher recommended institutions to focus on managing the noted gaps. In Kenya, studies have been done on banks and health facilities, but education institutions were not researched. Researches done on institutions of higher learning have been mainly done in foreign countries. An example is a study in USA on how students value their privacy in their workings. Some were unperturbed by the way the data was used by universities, some did not know that universities were collecting large amounts of their data and some did not understand the concept of privacy for them to have views ( Jones, Asher, Goben, Perr, Briney, & Robertshaw ,2020).

From the above, there are gaps in research on the topic data protections in institutions of higher learning in Kenya. Specifically, there are methodological gaps in which other studies have used interviews and review of only secondary information for data collection whereas the current study will use a questionnaire. Other studies have used descriptive statistics only but this study will include inferential statistics of cross tabulation chi square and regression to analyse the variables under study. Additionally, the theories used in various studies have not been combined in similar way as the current one that combines stakeholder theory and neo-institutional theory.

Based on the above, there are knowledge gaps regarding whether educational institutions are compliant with data protection laws. Additionally, what have stakeholders experienced in educational institutions in regard to their data. This study will delve into educational

facilities in particular, the University of Nairobi, to bridge the knowledge gap by answering the following:

1. Has the university of Nairobi complied with the requirements of the data protection laws in Kenya?
2. Have the data protection policies and laws affected the experiences of stakeholders at the University of Nairobi?

### 1.3 Objectives of Study

To evaluate how data protection policies affects stakeholder experiences at the University of Nairobi based on principles of data protection.

Specific Objectives

i. To establish the level of compliance to the data protection laws by the University of Nairobi.
ii. To determine the relationship between data protection and experiences of stakeholders at the University of Nairobi.

The research is based on the following hypothesis:

i. Compliance of data protection laws shapes the experience of stakeholders.

### 1.4 Value of Study

The study will be valuable to the University of Nairobi, as the management will understand their level of compliance to the data protection laws and identify any gaps. This will be beneficial to the University of Nairobi as compliance establishes trust with the regulator, the public and attracts more customers. Additionally, institutions of higher learning may use the findings of this study to benchmark their compliance to the data protection act.

The study will raise awareness of stakeholders in regards to their data privacy and protection. It will assist stakeholders critique the data collected by University of Nairobi and other institutions. Furthermore, policy makers will use the findings of the study to understand areas of improvement in the act and policies of various institutions. Finally, it is envisaged that researchers will reference the study for other matters related to data security. It will help researchers explore other areas not considered in this study.

# CHAPTER TWO: LITERATURE REVIEW

## 2.1 Introduction

Chapter two focuses in the related literature in the field of data protection while also expounding on the actual field empirical reviews. This will help explain the phenomenon at hand while also bringing up study gaps that will be used for further enhancement exploration in the field for current study. The chapter has the following sections the Theoretical framework; the independent variables which are the data protection principles; the dependent variable which is the stakeholder experience; the summary of literature review and gaps ; Lastly the conceptual framework.

## 2.2 Theoretical Framework

This section of the study sets out to explore the theories behind this current study in an effort to link the theories to practical implementation of data and privacy environment. The section is contained in two parts one containing the neo-institutionalism theory where the other holds stakeholder theory.

### 2.2.1 Neo-Institutionalism Theory

This theory was developed by John Meyer and Brian Rowan in 1977, proposed that organizations are influenced by institutional pressures, such as cultural norms, professional standards, and regulatory requirements. Subsequently, the institutional pressures are responsible for the shaping of institutional behaviour and decision-making. Organizations conform to institutionalized norms, values, and beliefs, regardless of their effectiveness or efficiency. Compliance with these institutionalized rules is seen as essential for legitimacy and survival (Voeten,2019).

The theory observes that, organizations face two types of institutional pressures: coercive and normative. Coercive pressures come from formal regulations and laws, while normative pressures arise from the beliefs and values of stakeholders such as customers, employees, and society at large. This has led to isomorphism. This means different organisations have now had the same practices in terms of regulatory compliances. (DiMaggio and Powell, 1998).

This research focuses on the rules and regulations on the data protection laws with the assumption that it incorporates values and norms of the society with regards to how data should be handled. The research expects the university of Nairobi to comply with the data protection laws due to this. In case there is no compliance with rules, then data protection issues that are related to the society values pressure the institution to comply. Additionally, based on the theory, stakeholders, professional standards and the market pressures also make the university comply to the best practices.

### 2.2.2 Stakeholder Theory

The Stakeholder Theory in management posits that the primary objective of any given entity is to generate value for its stakeholders. This theory, initially formulated by Freeman in 1984, has received support from prominent scholars such as Miles in 2017, Jones, Wicks, and Freeman in 2017, and Berman and Johnson-Cramer in 2019. Central to this theory is the notion of equitable cost-sharing and transparency in the agency principle, wherein all members within the entity understand and honor their roles. Furthermore, the Stakeholder Theory underscores the imperative of an entity's enduring existence, ensuring that it delivers benefits to its stakeholders while implementing corrective measures in all

endeavors. This approach facilitates audits and mitigates the risk-taking behaviors of agents who might otherwise engage in reckless actions.

The essence of the Stakeholder Theory is grounded in the belief that an institution can only thrive if it generates value for its stakeholders. In essence, stakeholders have no reason to retain their stake in the institution if it fails to contribute value to them. Consequently, it is essential for both the institution and its beneficiaries to maintain a vested interest in each other to prevent opportunistic behaviors in the institution's management and the engagement of stakeholders.

Stakeholders, as defined by Mugo in 2019, encompass a wide spectrum, including employees, customers, creditors, shareholders, and the surrounding community. The theory advocates for stakeholder experience as a critical aspect of organizational operations. In an institution, it is necessary to solicit stakeholder input to evaluate the practicality and the beneficial outcomes of institutional activities. Moreover, the theory's principles, which emphasize the interests of all stakeholders, imply that stakeholders should have a voice in shaping data privacy and protection policies. Given their nuanced understanding of the repercussions of a lack of such policies, it is vital that stakeholders are well-informed about these data privacy and protection measures. This study will focus on two primary stakeholder groups, namely, students and staff at the university, to delve into their roles and interests in shaping the institution's policies.

### 2.3 Data protection principles

In general ICT environment, data protection is seen as the concerted effort to keep data safe and protected in a manner that does not comprise its secrecy, usage and more specifically, free of being corrupted by either the processes or devices of storage (Rustad

& Koenig, 2019). The data protection act section 25 and the general regulations 2021, section 27-part V requires data to be collected, processed, disseminated and destroyed based on the principles of data protection which for this section are summarised as Principle of minimization, Principle of transparency and principle of confidentiality, integrity and availability.

### 2.3.1Principle of minimization

This principle requires that data collected and used by organisations, be restricted to the minimal amount possible for the purpose at hand and no unnecessary data should be collected or processed. This must be minimal but enough to make a decision (Danezis, Ferrer, Hansen, Hoepman, Metayer, Tirtea, & Schiffner,2015).

Minimization in the aspect of users can be achieved by hiding or concealing data from view once the data is no longer necessary for the purpose it was collected for or once its has outlived its relevance. Technologies like pseudonymization, anonymization and deleting data are used to ensure minimization (data protection regulations,2021). System designers chose a combination of these techniques that will be optimally protect the privacy of the personal data collected (Basdekis, Kloukinas, Agostinho, Vezakis , Pimenta, Gallo, & Spanoudakis, 2023). Additionally,

### 2.3.2 Principle of transparency

Enhancing privacy requires entities like organizations, systems and agents to be open and transparent about their operations, behavior, intentions and considerations in relation to the data they collect from stakeholders. Stakeholders should easily receive and understand this information provided. Entities are therefore obligated with developing the operational information that will be easily understood by the stakeholders. Transparency involves

explaining what the data collected will be used for, what automated processing will be done, the privacy enhancing technologies that will be used and third parties accessing the data. It also involves obtaining consent from stakeholders and alerting stakeholders in case of breaches in privacy of their data (Suzor, West, Quodling & York 2019).

Transparency requires clear, plain and simple language to be used for communication to a stakeholder to enable the stakeholder make decisions. It also requires providing understanding, training and awareness to the stakeholder on processing conducted on their data. (data protection regulations,2021).

Transparency ensures stakeholders have the same information and reduces information asymmetry that can create unfairness in relation between a stakeholder and an entity. It establishes trust with stakeholders as it signals the ability of the organization, system or agent to perform as promised. The limitation of the principle is that it can expose sensitive data and expose secrets of an entity to competition and attackers. It can also reduce trust of stakeholders in case they note the operational measures of the entity are weak. (Felzmann, Villaronga, Lutz, & Larrieux, 2020).

### 2.3.3 Principle of Confidentiality, Integrity and Availability

The growth of technologies over the last fifty years has led to growth of data mining techniques, large data storage technologies and management of data in one place. This has also led to increase in the risk of illegal access of data, unauthorized modification and interruption of service. Confidentiality is protection and prevention of data leakage to unauthorized persons. It allows only authorized persons to access data. Integrity prevents modification or alteration of data without authority from data custodians, while availability refers to access of information by stakeholders at any time. (Yang, Xiong & Ren, 2020)

Confidentiality is achieved by first classifying data that is considered sensitive and data that is open or non-sensitive. Information that is considered confidential by most entities include personally identifiable information like Biometrics of the fingerprints, iris, DNA; identification numbers, telephone contacts, financial information, educational information and ownership documentation like titles. (data protection act, 2019)

After classification, then privacy enhancing technologies can be applied to data to enhance confidentiality and Data integrity. Access controls which assign stakeholders privileges to access confidential information, attribute-based credentials to allow access to a system, authentication, encryption, anonymization and Pseudonymization are used to ensure confidentiality. Additionally, simple measures like restriction of physical access to stored documents, data storage devices and clean desk policy for organizations enhance data confidentiality and integrity. (data protection regulations,2021)

Odero (2010), studied the privacy practices in the banking industry used to protect customers. The researcher noted that bank employees behaved immorally by using customer data. The inquiry recommended staff are given just minimal privileges in computer systems to carry out their duty. Additionally, staff should sign integrity and confidentiality oaths to ensure they are bound to maintain confidentiality and integrity of data they handle.

Integrity ensures no unauthorised alterations happens and the personal data held by entities is correct. Additionally, system errors should not affect the integrity of data held in the systems and an audit trail of changes should be maintained (data protection regulations ,2021).

Availability ensures that data is accessible to users at any time. Disasters like cyberattacks, natural disasters and technical system failures can cause unavailability. Entities use large computing systems that can allow multiple users, privacy enhancing techniques like encryption to prevent cyber-attacks and use of data recovery systems to ensure data is available at all times (Basdekis et al, 2023).

While studying data breach risk management in Kenya commercial banks, Nzuva(2019) concluded that data leakage and breaches can be countered by implementing technological techniques to prevent and detect such breaches. Such techniques included data publishing, encryption and enforcing access rights to sensitive data. The researcher used survey questionnaires for the research, randomly sampled 36 out of 44 banks and used purpose sampling to select two participants from the IT department in each bank.

### 2.4 Stakeholder experience

The study assumes compliance to the principles of data protection creates safety of stakeholders' data. It also enhances trust of stakeholders in the data they share. Stakeholders experience cyber security breaches and cases of misuse of data, which shape their behavior in sharing data.

Misuse of data has been reported by stakeholders. Actions that constitute misuse include using information without authority of the owners, sending unsolicited content to users, coercing users into actions, or losing data. Users have cut relations with organisations after breaches (Zou,Mhaidli,Mcall,Schaub 2018) while others have initiated legal measures against institutions . University of Kabianga based in Kericho was ordered to pay Sh500,000 for using the image of a graduate in its marketing without the student's

consent((Kuria Vs university of  Kabianga , 2023). Mobile lending companies have been fined for mining telephone contacts in their customers' handsets and using the contacts to coerce the customers to pay their loans. The mobile lending companies are not transparent in their operations and did not seek consent of users in some cases, which led to complaints by customers who were affected by the data mining (ODPC,2023). Misuse has been cited when data is lost. Amadi & Ondabu (2023) noted that cases of missing student coursework and grades in institutions of higher learning was prevalent. This led to late graduation, loss of academic integrity and reputation of institutions. It was discovered that misplaced or lost records, errors in data entry, poor recording keeping, and system downtimes were the causes of missing course works and grades.  The study concluded that institutions should invest in strong technical systems that ensure availability of data, confidentiality and integrity when designing systems. They also need proper record keeping is required to ensure data is not lost.

In the last 20 -30 years' mass cyberattacks against large organizations have increased. The most common cybersecurity threats are ransomware, which are used to decrypt data in a system until an organization pays a ransom. Cyber criminals use sophisticated methods and therefore institutions are required to regularly check any system vulnerabilities to prevent cyber-attacks. (Hammouchi, Cherqi, Mezzour, Ghogho, & ElKoutbi 2019).  Social engineering has also been prevalent in Kenya especially in the mobile banking space. Mbuguah & Otibine(2022) indicated that social engineering is a form of cyber-attack that has been used to exploit human nature in order to obtain banking information and identity information .In kenya, users have reveled their personal information like mobile banking PIN numbers(MPESA) and IDs resulting to financial loss. The researcher concluded that

customer education on the various cyber-attacks should be done by organizations. Kshetri (2019) concluded that the increased cyber-attacks have been noted to be due to vulnerabilities in systems, lax security controls, lack of proper legislation and Lack of knowledge among technology users on how to protect themselves. Organizations need to continuously improve systems through penetrations tests and train their users on how to protect their data

Despite all the cyber security breaches and cases of data misuse, stakeholders have varied opinions in sharing information. The audit firm Ernst and young conducted a global survey to find the awareness and attitudes of consumers towards data privacy. The younger generations freely shared their data as they understood technologies and they received benefits. There was a similar study by Jones *et al*., (2020) which investigated the privacy views of students in 8 selected American universities. Interview questions were used on 15 selected undergraduate students per university. The students were selected via convenience sampling, random sampling and quota sampling. The opinions were varied. Some students did not understand data privacy and could not advise on their preferences, some did not know that their universities were collecting large amounts of data about them while others were unconcerned about their data and behavior. They considered the practice transactional.

### 2.5 Summary of Literature Review and Gaps

From the reviewed literature, the study came up with a summary of gaps for inspiration of the field implementation. The gaps are derived from methodological, conceptual and contextual observations in the studies thus presented and summarized in Table 2.1.

**Table 2.1: Summary of literature review and study gaps**

| Author (s) | Focus of Study | Methodology | Findings | Gaps |
|---|---|---|---|---|
| Nzuva(2019) | Enhancing data breach risk management in Kenyan banks | Randomly sampling 36 out of 44 banks with two participants per bank. Purposive sampling done for the participants. Only IT senior management selected because of their technical understanding | Strong and effective system architectures required to prevent data breaches and unavailability of data in banks. Use of technologies to prevent, detect and recover from data loss are required | Review of regulatory compliance to reduce risk of breaches was not done. Study reviewed banks while this study will review institutions of higher learning |
| Suzor, West, Quodling & York 2019 | Transparency in Commercial | Thematic analysis of 380 survey responses | Institutions should be transparent | Study done on transparency which is just |

| Author (s) | Focus of Study | Methodology | Findings | Gaps |
|---|---|---|---|---|
| | Content Moderation | of users whose content had automatically been moderated on social sites | when banning or moderating data posted by users on their platforms. They should be clear on the reasons for banning and who flagged the data | one part of data privacy and protection. This Study is to focus on three principles of data protection |
| Jones, Asher, Goben, Perr, Briney, & Robertshaw ,2020 | Student views on data power and privacy in learning systems and college education | Multi institution study of 8 randomly chosen universities in USA. Chose 15 students per university using various sampling methods like quota, convenience, | Concluded that students had varied opinions on how their data is used. Some did not understand privacy policies, some were | Small sample limits the precision and diversity of views obtained. Study done in first world and only considered students as |

| Author (s) | Focus of Study | Methodology | Findings | Gaps |
|---|---|---|---|---|
| | | snowball and random sampling | perturbed by their use of information and others were okay with the information collected as long as they benefited from it. | stakeholders. This study will have a Kenyan university and will include students and staff of the university. It will have a proportionate sample to the population |
| Kshetri (2019) | Issues of cyber-security and how it promote other crime related to cyber in the | Analysis of secondary data regarding cybersecurity threats in Africa between 2016-2019 | Increased cybersecurity threat in Africa over the last 3 years. Legislation required to reduce cyber | Used secondary data and only studied cybersecurity threats. The study will use primary data and review |

| Author (s) | Focus of Study | Methodology | Findings | Gaps |
|---|---|---|---|---|
| | | | threats, training of users and improved system through penetration tests. | measures to prevent data breaches through other cyberattacks and other types of attacks.. |

## 2.6 Conceptual Framework

A conceptual framework presents in diagrammatic fashion the relationship between study variables with ease of visualising the linkages among them (Cooper & Schindler, 2019. Specifically, the conceptual framework acts as a route map in identifying how the concept or element in the inquiry relates. In the current study, the predicted element is stakeholder experience while the predictor one is represented by principles of data protection including minimisation, transparency and confidentiality, integrity and availability. The principles of the data protection form the independent variables that will be studied. They are expected to shape the compliance and also the experiences of the stakeholders.

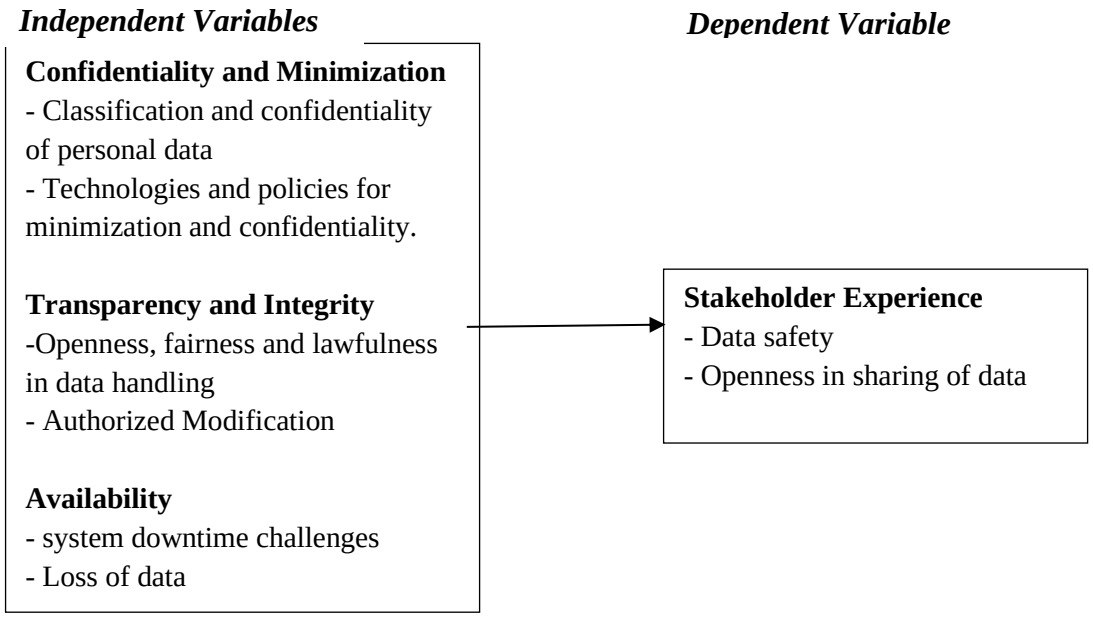



**Figure 2.1: Conceptual Framework**

# CHAPTER THREE: RESEARCH METHODOLOGY

## 3.1 Introduction

Chapter three describes the methodology of the study. The section includes the procedures used in managing the information to be collected from the field of study. Additionally, some management or administrative procedures are provided as a guide to the field exercise of data collection.

## 3.2 Research Design

In this study, data will be collected from primary and secondary sources. Secondary sources will be the available information on the government laws, the university of Nairobi policies and information on the data protection commissioner website. A descriptive research design has been chosen as the primary methodological approach due to its suitability for the extensive collection of quantitative data from various participants. This research design involves the impartial observation and documentation of subject behaviour, refraining from any form of influence or manipulation, as elucidated by Creswell (2016). This model is particularly concerned with elucidating the current or past state of phenomena, enabling the preliminary identification of outcomes. Moreover, this design facilitates the delineation of causal relationships between the variables under scrutiny, as expounded by Cooper and Schindler (2019).

The selection of this research design is apt as it enables the systematic collection of pertinent data related to the research variables, with subsequent analysis utilizing

appropriate statistical techniques. Furthermore, it affords the opportunity to explore the interconnections existing between the dependent variable and the independent variable, thereby serving the research objectives effectively. Specifically, as the study takes place at one location, The University of Nairobi, there will be total focus on the subjects of study.

### 3.3 Population of the Study

This is the group that provide information (Cooper & Schindler, 2019). Similarly, units of observation represent the actual source of data collection from which the unit of analysis is assessed (Kothari, 2017). In this study therefore, the unit of observation will be teaching staff, non-teaching staff and students of the University of Nairobi. This will make it suitable for the study to gather information on assessing the study phenomenon.

The research will focus on the University of Nairobi with a population of 1,500 teaching staff, 2,300 non-teaching and 45,000students (University of Nairobi fact file, 2023). The study will apply stratified sampling technique for selecting the sample. There will be 2 groups; staff and students.

### 3.4 Sample and Sampling Techniques

This refers to the organization of the items to be investigated (Cooper & Schindler, 2019). The study will determine the sample sizes for both staff and students using the Yamane formula:

$$n = \frac{N}{1+Ne^2}$$

Where

n is the sample size

N is the population

E is the desired precision (5%)

This means that the staff and students' sample will be as shown below.

Staff= $\frac{3800}{1+3800\ X\ 0.05^2}$

Students=$\frac{45{,}000}{1+45{,}000\ X\ 0.05^2}$

This will give 362 Staff and 396 Students

However, using stratified sampling, the study will allocate 60% to staff and 40% to students. Sample size of 30% to 70% is ideal for research work (Mugenda and Mugenda 2006)

This means that the Staff sample size: 0.6×362≈189.4737=217

While Student Sample size: 0.4×396≈ 158.59=159

Therefore, the study will use a sample of 217staff and 159 students to give 376 respondents

This will give a good representative sample for both strata.

The sample size for this research will be 376 respondents from the University of Nairobi.

The sampling technique will be stratified random sampling of staff and students with a total of 376 respondents required. Most of the data protection measures are implemented by staff therefore a high sample will be considered at 217 staff and 159 students. The advantage of convenience sampling for stratification is that it increases an expedited data collection process (Cooper & Schindler, 2019). To get the 376 target respondents out of the total population of 48,800, the study will use proportions as shown in Table 3.1.

**Table 3.1: Sampling Proportions at the UoN**

| **Category** | **Total Number** | **Stratified Percentage** | **Sample** | **Sample Size** |
|---|---|---|---|---|
| Staff | 3,800 | 0.6 | 362 | 217 |
| Students | 45,000 | 0.4 | 396 | 159 |
| **Total** | **48,800** | **1** | **758** | **376** |

Source: Research Data (2023)

### 3.5 Data Collection Instruments

Kothari (2017) recommends use specific methodology tools. To facilitate field data collection, the study will utilize a structured questionnaire which is fast in collecting data on phenomena. The main instrument is the questionnaire to be administered to the general respondents at the University of Nairobi. The instrument is chosen because it can reach the respondents quickly and creates anonymity. The questionnaire is meant to capture the aspects at the responding site with respect to all the study objectives. The questionnaire will be divided into demographic section and thematic section that covers all the objectives

of the study. A Likert scale on the ratings of 1 to 5 will be applied on the logical questions of the questionnaire.

### 3.6 Data Collection Procedure

Once the study is approved for field visit by the faculty, the questionnaire will be administered to the respondents. The researcher then will explain the value of the inquiry. Participants will be requested for consent before proceeding with the survey. Piloting will be done to establish the instrument validity and reliability. A time frame of 2 weeks will be sufficient for the collecting or returning of the questionnaires.

### 3.7 Validity and Reliability

In order to establish the usability of an instrument, Cooper and Schindler (2019) recommends testing the same for validity and reliability.

#### 3.7.1 Validity

Validity pertains to the extent to which the information derived accurately reflects the phenomenon under investigation, as emphasized by Cooper and Schindler (2019). To ensure the validity of this research, the researcher will employ construct validity, a method in which the questionnaire is structured into distinct sections, with each section specifically tailored to address a particular research objective, closely aligning with the sub-constructs delineated within the study's conceptual framework. Additionally, content validity will be upheld through consultation with the supervisor, further corroborating the research's accuracy and fidelity to the study's core objectives.

### 3.7.2 Reliability

This is usually taken to mean the capability of an instrument to repeatedly collect correct data over different locations or respondents (Cooper & Schindler, 2019). Scholars argue that reliability can be verified by testing the consistency of observation of an outcome after repeated trials. Reliability testing will be based on the Cronbach Alpha model. Instruments parts with less than the Cronbach coefficient of 0.7 would have to be rejected or reworked. Reliability would therefore require all parts of the instrument to be well over 0.7.

## 3.8 Data Analysis and Presentation

Data analysis and presentation will comprise tables as well as averages and standard deviation. There will be one questionnaire which will be divided into sections with Section one covering general demographic information, section 2 to 4 will cover the independent variables , section 5 the dependent variable and lastly section 6 covering the technical knowledge on data protection for technical experts. Quantitative data will be analysed using descriptive statistics as well as inferential statistics processed through computer package SPSS-version 26 in which the frequency and means will be determined while a liner regression model will be used to explain the link on the elements.

$$\mathbf{Y=\mu_0+ \mu_1X_1+\mu_2X_2+\mu_3X_3 + \varepsilon}$$

Where:

Y = Stakeholder Experience

$X_1$ = minimization Minimization and confidentiality

$X_2$ = Transparency and integrity

$X_3$ = Availability

$\mu_0$ = Y intercept as a coefficient

$\mu_1, \mu_2, \mu_3$ = Coefficient representing change of Y

$\varepsilon$ = error term

### 3.9 Ethical Considerations in the Research Study

To ensure the adherence to ethical standards in the field research profession, this study will make use of all available communication channels. A primary focus will be placed on maintaining confidentiality among all involved parties, with a strict commitment to utilizing the collected data solely for academic purposes. It is essential to underscore that no portion of the generated report will be employed beyond the authorized domains specified by the University of Nairobi (UoN). Furthermore,data collection will be conducted with honesty and decency at every stage, strictly adhering to the information outlined in the data collection instrument.

# CHAPTER FOUR: DATA ANALYSIS, RESULTS AND DISCUSSION

## 4.1. Introduction

This chapter presents the findings from the collected data and also the analysis of the data based on the overall objective of the research. The chapter also undertakes an in-depth discussion of the findings in relation to the existing literature, theoretical frameworks and previous research findings from other earlier studies.

## 4.2 Response Rate

The research was carried out on a sample of 376. The researcher reached out to 217 staff and 159 students. Out of these number 70% response rate was achieved with 151 staff and 111 students responding. This is a good response rate. This is because Mugenda and Mugenda (1999) suggested that a response rate of 60% is acceptable. The study's outcomes are systematically presented in Table 4.1.

**Table 4.1 is a Summary of Response Rate**

| **Category** | **Frequency (f)** | **Percentage %)** |
|---|---|---|
| Questionnaires completed | 263 | 70 |
| Questionnaires not returned | 113 | 30 |
| **TOTAL** | **376** | **100** |

**Source: Research Data (2023)**

## 4.3 Demographic Characteristics of Respondents

The analysis reveals different results as shown below.

### 4.3.1 Gender

The study sought to establish gender of the sample. The results obtained are presented on table 4.2

**Table 4.2: Distribution of Participants by gender**

| Gender | Frequency (f) | Percentage (%) |
|---|---|---|
| Male | 186 | 71 |
| Female | 77 | 29 |
| **Total** | **263** | **100** |

**Source: Research Data (2023)**

From table 4.2 male was 72%. However, females were only 77 accounting 29%. This means that there are more male workers and students within the University.

### 4.3.2 Age

The analysis included review of the age. The table 4.4 below depicts the findings.

This analysis was done to help determine the average age of the respondents. The findings are well presented in the table 4.2 below.

**Table 4.2: Age of the Participants**

| Age (years) | Frequency | Percentage |
|---|---|---|
| Below 18 | 0 | 0 |
| 18 – 23 | 75 | 28 |
| 24-41 | 34 | 13 |
| 42-58 | 100 | 39 |

| | | |
|---|---|---|
| Above 58 | 54 | 20 |
| **Total** | **263** | **100** |

**Source: Research Data (2023)**

From the above table, it is evident that 28% of the respondents were aged between 18-23 while 13% were aged between 24-41 years. These are mostly students. However, 39% were aged between 42-58 years while 20% were above 58. These depict majority who were the staff.

### 4.3.3 Role in the University

This was done and the results are shown in table 4.3 below.

**Table 4.3: Role**

| Role | Frequency | Percentage |
|---|---|---|
| **Student** | 111 | 42 |
| **Lecturer** | 76 | 29 |
| **Support Staff** | 58 | 22 |
| **Technical Staff** | 18 | 7 |
| **TOTAL** | **263** | **100** |

**Source: Research Data (2023)**

Table 4.3 presents a breakdown of roles among the participants. The data, derived from 263 respondents, reveals a diverse distribution of roles, with students constituting the largest group at 42%, followed by lecturers at 29%, support staff at 22%, and technical

staff at 7%. The table reflects a comprehensive representation of the university's stakeholder landscape. The distribution of roles underscores the importance of considering perspectives from various university constituents, ensuring a holistic understanding of the implications of data protection on diverse stakeholders within the academic community.

### 4.4 Data Reliability

This test was done using Cronbach's Alpha. The results are supported by the results shown in the table below.

**Table 4.5 Data Reliability**

| Construct | Cronbach's Alpha | Comments |
|---|---|---|
| Data minimization | 0.70 | Accepted |
| Data Confidentiality | 0.77 | Accepted |
| Data Integrity | 0.78 | Accepted |
| Data Transparency | 0.75 | Accepted |
| Data Availability | 0.79 | Accepted |
| Stakeholder experience | 0.81 | Accepted |

In the table above, the reliability test conducted using Cronbach's Alpha for the various constructs in the study evaluating the impact of data protection policies on stakeholder experience at the University of Nairobi yielded favourable results. The Cronbach's Alpha values for each construct, including Data minimization (0.70), Data Confidentiality (0.77), Data Integrity (0.78), Data Transparency (0.75), Data Availability (0.79), and Stakeholder experience (0.81), all surpassed the commonly accepted threshold of 0.70 for internal consistency. These results indicate a high level of reliability in the measurement of each construct, supporting the validity and consistency of the survey instrument. The findings suggest that the study's data collection tools effectively captured the intended dimensions

of data protection policies and stakeholder experience, reinforcing the credibility of the research outcomes and providing a solid foundation for drawing meaningful conclusions.

### 4.4.1 System Used

Prior to determining the data protection laws and experiences of stakeholders at UON, it was important to determine the major systems storing user data at UON. As indicated Ogutu 2017, the university has adopted various systems of storing data including the student management information system. The study tried to establish the demographic that has adopted the use of the various university systems. The analysis was done. The results are shown in the table 4.4 below

**Table 4.4-Systems used**

| Systems | Used | Percentage (%) | Not used | Percentage (%) | Total |
|---|---|---|---|---|---|
| Student Management information System (SMIS) | 222 | 84.7 | 41 | 15.3 | 263 |
| ECLASS/ E-learning | 226 | 86.1 | 37 | 13.9 | 263 |
| University of Nairobi (UON) Email | 248 | 94.4 | 15 | 5.6 | 263 |
| Zoom/Google Meet/Teams | 215 | 81.4 | 48 | 18.6 | 263 |

**Source: Research Data (2023)**

Table 4.4 provides insights into the systems used by participants in the study, with percentages reflecting their perceived adoption and use. The UON email emerges as the most used system, with 94% of respondents, indicating a relatively high level of use among respondents. ECLASS/E-learning follows closely with 86% of respondents acknowledging its use. The Student management information system (SMIS) has been managed or accessed by 84% of the respondents , and Zoom/Google Meet/Teams is rated the lowest with a percentage of 81% , indicating a more consistent but comparatively less positive evaluation. These findings offer valuable insights into the perceived adoption of various systems, guiding potential improvements or adjustments to better meet the needs of stakeholders in the context of the study's focus on data protection policies.

### 4.5 Data Protection Principles

This was done based on the principles of minimization and confidentiality as well as the transparency, integrity and availability. The results and analysis of the principles is shown below.

#### 4.5.1 Minimisation and confidentiality

This was done to show the models and details that students and staff use to register in the university systems. The results are shown in table 4.5 and 4.6 below

**Table 4.5-Registration Details Submitted**

| Registration details | Submitted | Percentage (%) | Not submitted | Percentage (%) | Total |
|---|---|---|---|---|---|
| Identification (ID) | 249 | 94.4 | 14 | 5.6 | 263 |
| Static details | 190 | 72.2 | 73 | 27.8 | 263 |
| Biometric data (fingerprint, voice or face print) | 69 | 26.4 | 194 | 73.6 | 263 |
| Academic certificates | 124 | 47.2 | 139 | 52.8 | 263 |
| Financial Information | 88 | 33.3 | 175 | 66.7 | 263 |
| Health information | 14 | 5.6 | 249 | 95 | 263 |
| Ownership information | 0 | 0 | 263 | 100 | 263 |
| Family details | 7 | 2.8 | 256 | 97 | 263 |

**Source: Research Data (2023)**

The data privacy policy of UON indicates that the university collects personal information that identifies an individual including the name, ID. No and phone number. This information is used for providing the functionality of UON services and fulfilling user requests, to complete their transactions and to communicate about UON offerings and operations. Table 4.5 presents an evaluation of the personal information collected by the University of Nairobi systems, focusing on aspects related to minimization. The responses are reflected through percentages. From the response 94% of respondents indicated they provide Identification and 72% have provided their static details like name and telephone number. Biometric information, academic information and financial information are also provided in the university systems but at lower degree that the others. The information is used by UON to provide education services, Financial and transactional services.

Information on health status, ownership details and family details are barely collected on the systems under study. It implies the university has complied with the principle of minimization which restricts minimal data to be collected for just the purpose at hand

Confidentiality was done and the results are shown in table 4.6 below.

**Table 4.6-Data Confidentiality**

| Statement | **Mean** | **SD** |
|---|---|---|
| I have been assigned a user name and password to access systems under section 1 | 4.901 | 0.977 |
| The password(s) I use on the systems are hidden from view after entry (hashed). | 4.990 | 0.965 |
| My personal information is only available after logging in with my credentials | 4.891 | 0.874 |
| My personal information is only accessible to me and not to the public | 4.801 | 0.843 |
| **Average** | **4.89575** | |

From UON's privacy policy and the data protection act , personal information that identifies an individual , example Name ID, biometric details, is classified as sensitive information and therefore confidentiality measures should be applied in the systems that collect and use such data. Table 4.6 indicates that the participants report a positive experience with assigned usernames and passwords for system access, reflected in a mean

score of 4.901, indicating a strong consensus on the effectiveness of user authentication to prevent unauthorised access. The concealment of passwords from view after entry, as indicated by a mean score of 4.990, further underscores a high level of confidentiality where passwords are anonymized through masking. This supports the principle of minimization and confidentiality which requires personal data to be concealed. Additionally, respondents express confidence that their personal information is only accessible through proper login credentials, with mean scores of 4.891 and 4.801 for post-login access and restricted public visibility, respectively. This access control and attribute based technical controls mean that there is a positive perception regarding the confidentiality of user data within the university systems, highlighting the success of existing security measures and emphasizing the importance of maintaining such standards in the context of data protection policies. Based on this the university of has complied with the principle of minimization and confidentiality.

### 4.5.2 Transparency and Integrity

This was analysed to determine the level of data integrity and transparency. The results are shown in table 4.7 and 4.8 below

**Table 4.7-Data transparency**

| | **Mean** | **SD** |
|---|---|---|
| I was informed of the reasons for collection of my personal information when registering to the systems | 4.189 | 0.761 |
| I accepted and submitted my personal information to the university systems on my own volition | 4.991 | 0.893 |

| | | |
|---|---|---|
| I have been informed of breaches that have happened on my data example hacking | 3.190 | 0.541 |
| **Average** | **4.457** | |

**Source: Research Data (2023)**

Table 4.7 provides insights into the perceived transparency of data among respondents at the University of Nairobi. Mean scores and standard deviations offer a glimpse into participants' attitudes and experiences regarding transparency. The data indicates a relatively positive perception of transparency, with a mean score of 4.189 for being informed about the reasons for personal information collection during system registration. Additionally, participants express a high level of agency in data submission, as evidenced by a mean score of 4.991, suggesting that they willingly provided personal information to university systems. However, the lower mean score of 3.190 for being informed about data breaches, such as hacking incidents, indicates a potential area for improvement in communicating and addressing security incidents to enhance overall data transparency and awareness. This means that there is need for clear communication and transparency in data collection processes and ensuring users are well-informed and engaged in cyber security breaches and incidents that involve misuse of data . Based on the means the university of Nairobi is compliant to the principle of transparency but they need to create more awareness on their transparency measures related to cyber security breaches and misuse of data.

**Table 4.8-Integrity Measures**

| | **Mean** | **SD** |
|---|---|---|
| No erroneous personal data about me exists in UON systems | 4.881 | 0.971 |
| My identification details like the ID, telephone number and name in the systems cannot be amended without my authority | 3.190 | 0.876 |
| System errors cannot cause changes on the captured personal information in UON systems | 3.198 | 0.422 |
| **Average** | **3.756** | |

Table 4.8 illuminates the perceived integrity measures within the University of Nairobi (UON) systems, providing valuable insights into participants' perspectives on the accuracy and control over their personal information. The data suggests a high level of confidence in the integrity of personal data, with a mean score of 4.881 indicating strong agreement that no erroneous information about respondents exists in UON systems. However, concerns arise regarding the control participants have over their identification details, as reflected by a lower mean score of 3.190, indicating that there may be a perceived lack of authority in amending certain information. Similarly, the mean score of 3.198 for the inability of system errors to cause changes in captured personal information suggests some reservations about the robustness of measures to prevent unintended modifications. This confirms the view that the university should find ways of ensuring users have not only

accurate data but also a sense of control over the information captured in university systems, emphasizing the need for robust integrity measures to maintain data accuracy and user trust.

### 4.5 Experience of stakeholders

#### 4.5.1 Data opinions of Stakeholders

This was done and the data is presented in table 4.11 below

**Table 4.11: Data opinions of Stakeholders**

| Statement | Mean | SD |
|---|---|---|
| Only people who have something to hide are afraid to share data | 3.027 | 0.933 |
| Sharing data is okay as long as I benefit from it | 3.444 | 0.674 |
| Before I share data, I must understand how it will be collected and how it is used. | 4.638 | 0.866 |
| I worry about how data will be used but I share it because I trust the organization | 4.014 | 0.761 |
| **Average** | **3.781.** | |

**Source: Research Data (2023)**

Table 4.11 explores the diverse perspectives and experiences of stakeholders regarding data sharing. The data indicates that the majority of respondents express a relatively positive attitude towards data sharing, with a mean score of 4.638 for the statement " Before I share data, I must understand how it will be collected and how it is used". This suggests

that stakeholders are generally receptive to sharing their information if they are well informed of its use. It underscores the importance of stakeholder's place on transparency and comprehension in data sharing processes .Moreover, the mean score of 4.014 for the statement " I worry about how data will be used but I share it because I trust the organization indicates that data sharing worries are mitigated by a trust in the organization's handling of their information. "Sharing data is okay as long as I benefit from it" has a low mean score of 3.027 which implies that respondents are aware of dangers in data privacy . "Sharing data is okay as long as I benefit from it" has a low score of 3.4.4 .These findings emphasize the significance of transparent communication and perceived benefits in fostering a positive stakeholder experience regarding data sharing within the studied context.

### 4.5.2Data Safety and Measures to Control Data Loss

This was done to determine level of measures. The results are shown in table 4.12 below.

**Table 4.12: Safety Measures**

| Measures | Mean | SD |
|---|---|---|
| Staff integrity preventing alteration and leakage of your data | 4.189 | 0.863 |
| System stability at UON preventing data loss | 4.110 | 0.752 |
| Strong technological systems by UON preventing unauthorized access to your data | 4.890 | 0.986 |

| | | |
|---|---|---|
| Transparency by UON on the parties accessing your data | 4.411 | 0.761 |
| UON preventing misuse of your images for marketing purposes | 3.091 | 0.564 |
| Lodge a legal suit against the University for breach of privacy | 3.001 | 0.937 |
| Report to the office of the data protection commissioner | 2.102 | 0.110 |
| Organize protests against the university, with the other students affected | 3.018 | 0.451 |
| Report to the ICT department and demand an explanation. | 4.901 | |
| Highlight the issue on social media | 1.104 | 0.610 |
| Cut relations with UON and exit | 0.000 | 0.000 |
| **Average** | **3.073.** | |

**Source: Research Data (2023)**

Table 4.12 presents an assessment of the perceived safety measures and control mechanisms implemented by the University of Nairobi (UON) to prevent data loss and protect user information. The data reveals generally positive perceptions among respondents. Staff integrity, aimed at preventing alteration and leakage of data, receives a mean score of 4.189, indicating a high level of confidence in the trustworthiness of university staff. System stability at UON, crucial for preventing data loss, is perceived

positively with a mean score of 4.110. The use of strong technological systems by UON to prevent unauthorized access to data is highly rated, reflected in a mean score of 4.890. Transparency in informing users about parties accessing their data receives a mean score of 4.411, demonstrating a favorable perception of UON's communication practices. However, respondents express some reservations about the university's ability to prevent the misuse of their images for marketing purposes, as indicated by a lower mean score of 3.091. The data also highlights alternative actions respondents might consider in case of data breaches, such as legal actions, reporting to the data protection commissioner, organizing protests, or resorting to social media. Importantly, the option of cutting relations with UON and exiting receives a mean score of 0.000, suggesting that leaving the university is not perceived as a viable response to data safety concerns. This showed that transparent communication, technological robustness, and proactive measures are important in building and maintaining user trust regarding data protection within the university setting.

### 4.5.3Systems to Inform Users

This was done to know the level of user information sharing. The results are shown in table 4.13 below.

**Table 4.13-System to inform users**

| Item | Mean | SD |
|---|---|---|
| UON Privacy policy | 4.922 | 0.851 |
| Terms and conditions on systems | 4.178 | 0.725 |

| | |
|---|---|
| Information of physical informs | 3.190 |
| **Average** | **3.684.** |

**Source: Research Data (2023)**

Table 4.13 data indicates a high level of satisfaction with the UON privacy policy, as reflected in a mean score of 4.922, suggesting that users feel well-informed about the university's approach to handling their data. Similarly, terms and conditions on systems receive a positive mean score of 4.178, indicating users perceive clarity and transparency in the rules governing their interaction with university systems. However, the lower mean score of 3.190 for information on physical forms suggests some reservations or room for improvement in conveying data-related information through traditional, non-digital means. This confirms that there is need for clear and accessible online documentation in ensuring that users are well-informed about data policies and procedures within the university environment.

### 4.5.3 Data Availability

This was done to determine the level of data availability in the systems. The results are shown in table 4.9 below.

**Table 4.9-Data availability**

| Statement | **Mean** | **SD** |
|---|---|---|
| I can access the personal information I have shared with university of Nairobi | 4.162 | 0.862 |

| | | |
|---|---|---|
| I have not experienced any case of lost personal data in UON systems. | 4.910 | 0.958 |
| UON systems are stable and have minimal downtimes | 3.901 | 0.671 |
| **Average** | **4.324.** | |

**Source: Research Data (2023)**

Table 4.9 assesses the perceived level of data availability within the University of Nairobi (UON) systems, offering insights into participants' experiences and perspectives. The data suggests a moderately positive perception of data accessibility, with a mean score of 4.162, indicating that respondents feel they can access the personal information they have shared with the university. Furthermore, a higher mean score of 4.910 for not experiencing any cases of lost personal data in UON systems underscores a sense of security and reliability in terms of data retention. However, the mean score of 3.901 for the stability of UON systems with minimal downtimes suggests some reservations about system reliability. This means the university should not only maintaining data availability but also ensuring system stability to instil user confidence in accessing and retrieving their personal information within the university's data infrastructure.

### 4.4.7 Lost Data

The analysis was done to evaluate the level of lost data in the systems based on the response on table 4.9 above. The results are depicted in table 4.10 below

**Table 4.10-Lost Data**

| Measure | Frequency | Percentage (%) |
|---|---|---|
| Course Work | 26 | 10 |
| Financial information | 19 | 7 |
| Contact details | 8 | 3 |
| Health information | 0 | 0 |
| Educational certificates | 0 | 0 |
| None | 210 | 80 |
| Total | 263 | 100% |

Table 4.10 provides insights into the perceived level of lost data within the University of Nairobi (UON) systems, indicating participants' experiences and concerns. The respondents had high confidence ins systems maintaining data as indicated in 4.9. However, the small percentage of respondents who lost data majorly lost course work which was only 10% of the respondents. 7% of the respondents indicated to have lost financial information on the system, while 7% had lost contact details. Over 80% of the respondents had not lost any data in the systems under study. The data reveals a relatively positive perception regarding the retention of critical personal information, suggesting a high level of confidence in the system's ability to preserve academic records. Notably, no respondent had lost education certificates and health information submitted on the systems under study , indicating a strong consensus that data loss in these categories is perceived as non-existent. This indicates that there is need for continuous improvement in data

management practices, particularly in areas where concerns about potential data loss persist, to enhance the overall reliability and integrity of UON systems.

### 4.6 Regression Analysis

The regression was done and the results are shown below.

#### 4.6.1 Model Summary

This is depicted below.

**Table 4.16-Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .801[a] | .641 | .301 | 1.11870 |

b. Predictors: (Constant), Minimization and confidentiality, Transparency and integrity and Availability

***Source: Research Data (2023)***

Dependent Variable: stakeholder experience

The regression analysis, as summarized in Model 1, demonstrates a statistically significant relationship between the predictors (Minimization and Confidentiality, Transparency and Integrity, and Availability) and the dependent variable, stakeholder experience. The coefficient of determination (R Square) is 0.641, indicating that approximately 64.1% of the variability in stakeholder experience can be explained by the combined influence of these predictors. The adjusted R Square, accounting for the number of predictors in the model, is 0.301. The standard error of the estimate is 1.11870, reflecting the average

variability between the observed and predicted values. The positive correlation coefficient (R = 0.801) indicates a strong positive relationship between the predictors and stakeholder experience. The results suggest that the considered data protection policies, encompassing aspects of minimisation, confidentiality, transparency, and availability, significantly contribute to influencing stakeholder experience at the University of Nairobi.

### 4.6.2 ANOVA

This was done and the results are shown below

**Table 4.17-ANOVA**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 42.371 | 4 | 11.834 | 8.811 | .000[b] |
| | Residual | 83.911 | 258 | 1.101 | | |
| | Total | 120.219 | 262 | | | |

a. Dependent Variable: Stakeholder experience

The analysis of variance (ANOVA) results for the regression model assessing the impact of data protection policies on stakeholder experience at the University of Nairobi reveals a statistically significant relationship. The regression model, comprising predictors such as Minimization and Confidentiality, Transparency and Integrity, and Availability, collectively contributes to explaining the variance in stakeholder experience. The significant F-statistic of 8.811 with a corresponding p-value of .000 indicates that the model is effective in explaining the variability in stakeholder experience, supporting the hypothesis that data protection policies influence stakeholders' engagement. The regression model's overall significance is confirmed by the ANOVA test, reinforcing the study's objective to evaluate the effects of data protection policies based on principles of data protection on stakeholder experience at the University of Nairobi.

### 4.6.3 Regression Coefficients

**Table 4.18-Regression Coefficients**

| Model | Unstandardized Coefficients | | Standardized Coefficients | | |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | t | Sig. |
| (Constant) | 1.724 | .471 | | 3.980 | .000 |
| Minimization and Confidentiality | .277 | .125 | .210 | 2.190 | .070 |
| Data Transparency | .153 | .156 | .071 | .178 | .230 |
| Data Integrity | .188 | .133 | .087 | .424 | .581 |

| | | | | | |
|---|---|---|---|---|---|
| Data Availability | .122 | .101 | .334 | 1.237 | .194 |

**Source: Research Data (2023)**

$Y_2 = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$

$Y_2$ represents the stakeholder experience

$\beta_0$ represents the Constant (Co-efficient of intercept)

$X_1$ represents the Minimization and confidentiality

$X_2$ represents the data Transparency

$X_4$ represents the data integrity

$X_5$ represents the data Availability

ε. Is the Error Term

$B_1 \ldots B_3$= Regression co-efficient of three variables

The regression equation (Y) based on the coefficients presented in Model 1 is:

*Y=1.724+(0.277×Minimization and Confidentiality)+(0.153×Data Transparency)+(0.188×Data Integrity)+(0.122×Data Availability)+ϵ*

The regression coefficients provide detailed insights into the impact of various data protection policy components on stakeholder experience at the University of Nairobi. Firstly, the intercept (constant) term (β0) is 1.724, indicating that when all predictor variables are zero, the estimated stakeholder experience is 1.724. Moving to the specific predictors, the coefficient for Minimization and Confidentiality (β1) is 0.277, and while it does not reach conventional significance levels (p = 0.070), it suggests a positive relationship with stakeholder experience. The coefficient for Data Transparency (β2) is

0.153, indicating a slight positive impact that is not statistically significant ($p = 0.230$). Data Integrity ($\beta 3$) has a coefficient of 0.188, but its significance level ($p = 0.581$) suggests a lack of statistical support for its impact on stakeholder experience. Notably, Data Availability ($\beta 4$) has a coefficient of 0.122 with a significance level of 0.194, suggesting a positive impact that falls short of conventional statistical significance. These findings collectively emphasize that while certain aspects of data protection policies, such as Minimization and Confidentiality and Data Availability, show promising trends towards influencing stakeholder experience, further investigation and potentially larger sample sizes may be needed to confirm their statistical significance.

The regression coefficients ($\beta 1$ to $\beta 4$) quantify the impact of the respective predictor variables (Minimization and Confidentiality, Data Transparency, Data Integrity, and Data Availability) on the stakeholder experience. It's important to note that in the context of evaluating data protection policies' effects on stakeholder experience at the University of Nairobi.

This means that the regression coefficients provide a nuanced understanding of how specific elements of data protection policies influence stakeholder experience at the University of Nairobi. While certain components, such as Minimization ,Confidentiality, and Data Availability, show positive trends, the lack of statistical significance for some coefficients emphasizes the need for further exploration and potentially refining the model. This analysis contributes valuable insights into the nuanced relationship between data protection policies and stakeholder experience, providing a foundation for future research and policy development within the university context.

### 4.7 Discussion of the Findings

The findings of the study indicated that the response rate was 70%. The study reached out to 217 staff and 159 students, resulting in 151 staff and 111 students responding. This response rate surpasses the 60% threshold suggested by Mugenda and Mugenda (1999) as acceptable. The high response rate contributes to the reliability and validity of the study's findings, providing a representative sample of the university community's perspectives on data protection policies. The systematic presentation of response data in Table 4.1 indicates that 263 questionnaires were completed, with only 113 not returned, reflecting a robust engagement with the research instrument.

The demographic characteristics of the respondents, as outlined in Tables 4.2, 4.4, and 4.3, provide valuable insights into the composition of the participant pool. The gender distribution indicates a higher percentage of male respondents (71%) compared to females (29%), suggesting a gender imbalance within the university community. The age distribution reveals that a significant proportion of respondents are aged between 41 and 58 years (39%), indicating a substantial representation of staff members, while those aged 18 to 23 years (28%) and 24 to 41 years (13%) are primarily students. The roles of respondents vary, with students constituting the largest group (42%), followed by lecturers (29%), support staff (22%), and technical staff at 7%.

The presented data and analyses offer a comprehensive overview of stakeholders' perspectives on data protection principles and practices at the University of Nairobi. The evaluation of systems used (Table 4.4) provides valuable insights into the perceived effectiveness of various platforms, with the university of Nairobi email receiving the highest rating, guiding potential improvements aligned with data protection policies.

Registration details (Table 4.5) reveal a high level of minimization where only relevant information is collected by the university for use. This is inline with the university data privacy policy, data protection act 2019 and data protection regulations 2021. The confidentiality of data (Table 4.6) is well-regarded, emphasizing the success of technological techniques to prevent unauthorised access as outlined by Yang, Xiong & Ren (2020). Transparency and integrity (Table 4.7) indicate a positive perception but reveal the need for enhanced communication about data breaches.

The analysis of integrity measures (Table 4.8) reflects stakeholders' confidence in the accuracy of personal data but raises concerns about users' control over certain information. Data availability (Table 4.9) showcases positive perceptions about stakeholders easily accessing their information and minimal loss of data. This is contrary to a study by Amadi & Ondabu (2023) which indicated prevalence of lost course work in university systems. Data availability (Table 4.9) indicates a need for improvement in system stability. Lost data (Table 4.10) demonstrates confidence in academic record retention and reveals minimal loss of course work and financial information. (Table 4.11) demonstrates the opinions of stakeholders in regard to their data . most respondents require information on how their data will be used before they share it and some share it due the trust they have with the organisation. Most respondents do not support that data should be shared as long as benefits are derived. This is in line with the study done by Kröger, et al(2021). Safety measures (Table 4.12) depict a positive view of staff integrity and technological systems, emphasizing the importance of transparency in building user trust. Systems to inform users (Table 4.13) receive generally high ratings, with suggestions for improvement in traditional communication methods.

The regression analysis conducted to assess the impact of data protection policies on stakeholder experience at the University of Nairobi yielded significant results. The model, consisting of predictors such as Minimization and Confidentiality, Transparency and Integrity, and Availability, demonstrated a statistically significant relationship with stakeholder experience, as evidenced by the high R Square value of 0.641. This implies that approximately 64.1% of the variability in stakeholder experience in safety of their data and trust in the university can be attributed to the considered data protection principles. The positive correlation coefficient (R = 0.801) further indicates a strong positive relationship between these principles and stakeholder experience. The findings suggest that the principles of data protection, encompassing minimization, confidentiality, transparency, and availability, significantly contribute to influencing stakeholders' engagement and experiences at the university.

The ANOVA results reinforce the model's effectiveness in explaining the variability in stakeholder experience. The significant F-statistic of 8.811 and a corresponding p-value of .000 indicate that the regression model is successful in elucidating the impact of data protection policies on stakeholder experience. This supports the initial hypothesis that these policies play a crucial role in shaping the level of engagement among stakeholders at the University of Nairobi. It underscores the importance of robust data protection measures in fostering a positive environment for stakeholders, aligning with broader efforts to enhance trust and compliance in the university's data management practices.

Examining the regression coefficients provides a nuanced understanding of how specific components of data protection policies influence stakeholder experience. While Minimization and Confidentiality and Data Availability exhibit positive trends, with coefficients indicating a positive impact, the lack of statistical significance for some coefficients, such as Data Transparency and Data Integrity, suggests the need for further investigation. The regression equation generated from these coefficients ($Y=1.724+(0.277\times\text{Minimization and Confidentiality})+(0.153\times\text{Data Transparency})+(0.188\times\text{Data Integrity})+(0.122\times\text{Data Availability})+\epsilon$) serves as a valuable tool for predicting stakeholder experience based on the considered data protection policy factors. In summary, these findings emphasize the importance of continuous efforts to enhance data protection policies at the University of Nairobi, recognizing their pivotal role in shaping stakeholder engagement and trust within the institution.

# CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

## 5.1: Introduction

The section has details on summary findings, conclusions, recommendations and limitation of the study

## 5.2 Summary of findings

The purpose of the study was to determine the level of compliance of university of Nairobi to the data protection laws/principles and the experiences of stakeholders in regards to these data protection laws.

The university of Nairobi has complied to the principle of minimization by collecting and using information that is relevant for the purpose of providing education services, enabling financial and transactional servicing. This includes identification information, biometric information and financial payments. Personal information that is irrelevant for the university purposes is not collected in the systems under study. This includes Family details of stakeholders and land and vehicle ownership details. The university has complied to the principle of confidentiality by use of technological techniques like anonymisation, attribute-based and access control measure to prevent unauthorised access to stakeholders' profiles in the systems under study.

The study demonstrates that there are gaps to compliance with the principles of transparency and integrity. It indicated that the university is transparent about why it collects data and obtains consent of stakeholders. However, transparency in informing stakeholders about cyber security breaching received a low rating meaning more awareness

should be created to ensure stakeholders are aware of breaches relating to their data. The study also indicated there was a low level of compliance in the principle of integrity. The study noted the lack of control by stakeholders to their data and the existence of system instability which had the risk of unintended modification

The findings show that the level of compliance to the principle of availability is high. The only gap noted was instability of UON systems causing downtimes. University of Nairobi should ensure systems uptime is enhanced to increase stakeholder confidence.

The study demonstrates that compliance to the principles of data protection results to the safety of stakeholders data and increased level of trust in an organisation. Stakeholders are open to share data as long as they understand how it will be used. Furthermore, in case of breaches stakeholders are unlikely to cut ties with the university, raise the issue on social media or organise protests. Their likely course of action will be to raise the issue with the IT department, report to the data protection commissioner or take legal action.

### 5.3: Conclusions

The university of Nairobi has a high level of compliance with the data protection laws. There are however gaps in transparency of security incidents, system downtimes and risks in integrity of system data due to unstable systems and unauthorised modification. The university should enhance and create more awareness of the security incidents that affect stakeholder data, enhance systems to give stakeholders more control of their data and lastly invest in systems that will reduce system downtimes

Despite these stakeholders have a high level of trust in the organisation as they would not rush to make drastic actions incase of a breach of their data. They would not take extreme measures like cutting ties, organising protests and raise issues on social media.

### 5.4 Limitations

The time taken to conduct the study was minimal and respondents involved had a challenge in filling the questionnaire due to their busy education and work environments. This was partially overcome by use of online questionnaires which could be filled and returned within a short time.

Some respondents especially the university staff members were not forthcoming with information as the felt their privacy would be infringed and they would end up revealing organisation secrets. The participants were assured of the anonymity of the study and the questionnaire was moderated to ensure the secrets of the university were not revealed.

### 5.5 Recommendations

The study only concentrated on the university of Nairobi and its education systems. Future studies should check the compliance with data protection laws for other educational institutions and sectors.

From the findings of this study, it is important that the university of Nairobi complies with the data protection laws as they enhance safety of stakeholder's data and trust that stakeholders have. The university must strive to create awareness of their data protection principles and polices. The university should enhance transparency of cyber security breaches, upgrade systems to minimise downtimes and give stakeholders more control of their data. Lastly, the respondents have a high level of trust in the university in regards to

their data. To maintain the level of trust and enhance security measures, the university should consider opinions that users /stakeholders have in data protection.

.

# REFERENCES


Ahmed, G. (2021). Improving IoT privacy, data protection and security concerns. International Journal of Technology, Innovation and Management (IJTIM), 1(1).

Amadi, O. J., & Ondabu, F. K. (2023). Understanding The Causes And Consequences Of Missing Marks In Kenyan Universities: A Qualitative Analysis.

Alam, A. (2022). Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records. In Smart Data Intelligence: Proceedings of ICSMDI 2022 (pp. 307-320). Singapore: Springer Nature Singapore.

Ayugi, E. D. (2021). Information Security Strategies and Patient Data Privacy Among Health Facilities in Nairobi (Doctoral dissertation, University of Nairobi).

Basdekis, I., Kloukinas, C., Agostinho, C., Vezakis, I., Pimenta, A., Gallo, L., & Spanoudakis, G. (2023, April). Pseudonymisation in the context of GDPR-compliant medical research. In 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN) (pp. 1-6). IEEE.

Communications Authority of Kenya (2023). Cyber-Security Report https://www.ca.go.ke/sites/default/files/2023-06/Cybersecurity%20Report%20Q2%202022-2023.pdf

Cooper, D. R., & Schindler, P. S. (2019). Business Research Methods (12th ed.). New York: McGraw Hil.

Creswell, J. W. (2016). Research design: Qualitative, quantitative, and mixed methods approaches. Thousand Oaks, California: SAGE Publications, Inc.

Dean of students(2020), Students information handbook, 2020-2021https://uonbi.ac.ke/students-information-handbook-20202021

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and data protection by design-from policy to engineering. arXiv preprint arXiv:1501.03726.

DiMaggio, Paul (1998). "The New Institutionalisms : Avenues of Collaboration". Journal of Institutional and Theoretical Economics (JITE). 154 (4): 696–705

Earp, J. B., & Payton, F. C. (2001). Data protection in the university setting: Employee perceptions of student privacy. In *Proceedings of the 34th Annual Hawaii International Conference on System Sciences* (pp. 6-pp). IEEE

Ernst and Young (2020).Global Consumer privacy 2020, https://assets.ey.com/content/dam/ey-sites/ey-com/es_es/topics/resilient-enterprise/ey-global-consumer-privacy-study-2020-single-pages.pdf.

Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards transparency by design for artificial intelligence. Science and Engineering Ethics, 26(6), 3333-3361.

Freeman, R.E.(1984),strategic management: A stakeholder approach, Pitman publishing, Boston, MA

Gattiker E, Kelly,H (1999).Information systems research Vol 10. No 3, pp 233-254

Government of Kenya(2019).The Data protection Act 2019. Retrieved from: https://www.odpc.go.ke/dpa-act/ Date Accessed: 24/5/2023

Graeff T.R , Harmon S.K,(2002). Collecting and using personal data: consumers' awareness and concerns ,Journal of Consumer Marketing Vol 19. Pp 302-318,

Haase, S., & Buus, L. (2020). Translating government digitalisation policy in higher education institutions: the Danish case. Nordic Journal of Digital Literacy, 15(4), 246-258.

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. Procedia Computer Science, 151, 1004-1009.

Herranen, O. (2022). Institutions in Neo-institutionalism. In The Invisible Order: A Relational Approach to Social Institutions (pp. 43-63). Cham: Springer International Publishing.

Ikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology*, *71*(9), 1044-1059.

Kothari, C. (2017) Research methodology: Methods and techniques. (2nd ed). New Delhi: New Age International (P) Limited, Publishers.

Kröger, Jacob & Miceli, Milagros & Müller, Florian. (2021). How Data Can Be Used Against People: A Classification of Personal Data Misuses. 10.2139/ssrn.3887097.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81.

Kushnir, I. (2023). Rational-Choice Neo-Institutionalism in Europeanization in the UK and Germany: A Toolkit Offered by Their Memberships in the European Higher Education Area. European Education, 1-17.

Kuria v University of Kabianga (Petition E002 of 2022) [2023] KEHC 809 (KLR) (10 February 2023) (Judgment), http://kenyalaw.org/caselaw/cases/view/251166/

Ma, C., Li, J., Ding, M., (2020). On safeguarding privacy and security in the framework of federated learning. IEEE network,63 ,34(4), 242-248.

Marković, M. G., Debeljak, S., & Kadoić, N. (2019). Preparing Students for the Era of the General Data Protection Regulation (GDPR). *TEM Journal*, *8*(1).

Marks, A. (2007). Exploring universities' information systems security awareness in a changing higher

Martin, Y. S., & Kung, A. (2018). Methods and tools for GDPR compliance through privacy and data protection engineering. In 2018 IEEE European symposium on security and privacy workshops (EuroS&PW) (pp. 108-111). IEEE.

Mbuguah, S. M., & Otibine, T. O. (2022). A Survey of Awareness of Social Engineering Attacks to Information Security Management Systems: The Case of Kibabii University Kenya. International Journal of Computer Applications Technology and Research, 11(06), 187-192.

Meyer, J., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology, 83, 340-363.

Mishra, R. A., Kalla, A., Braeken, A., & Liyanage, M. (2021). Privacy protected blockchain based architecture and implementation for sharing of students' credentials. Information Processing & Management, 58(3), 102512.

Nikou, S., & Maslov, I. (2021). An analysis of students' perspectives on e-learning participation–the case of COVID-19 pandemic. The International Journal of Information and Learning Technology, 38(3), 299-315.

Njenga, K., Garg, L., Bhardwaj, A. K., Prakash, V., & Bawa, S. (2019). The cloud computing adoption in higher learning institutions in Kenya: Hindering factors and recommendations for the way forward. Telematics and Informatics, 38, 225-246.

Nzuva, S. (2019) Enhancing Data Breach Risk Management: A Case Study of Kenyan Commercial Banks. *Constitution*, *47*, 48..

Odusote, A. (2021) Data Misuse, Data Theft and Data Protection in Nigeria: A Call for a More Robust and More Effective Legislation. *Beijing Law Review*, **12**, 1284-1298.

Office of the data protection commissioner,2023, ODPC issues Penalty Notices, https://www.odpc.go.ke/odpc-issues-penalty-notices-against-whitepath-company-limited-and-regus-kenya-and-an-enforcement-notice-against-ecological-industries-limited/

Ogutu, J. (2017). adoption of information communication and technology on historical research at university of nairobi kenya: implication on teaching and learning process. Asian Journal of Educational Research Vol, 5(2).

Plachkinova, M., & Maurer, C. (2018). Security breach at target. Journal of Information Systems Education, 29(1), 11-20.

Rizi, M. H. P., & Seno, S. A. H. (2022). A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. Internet of Things, 20, 100584.

Solove, D.J. (2002). “Conceptualizing privacy”, California Law Review, Vol. 90. No.1. pp. 62-69

Solove, D. J. (2008). Data mining and the security-liberty debate. The University of Chicago Law Review, 75(1), 343-362.

Suzor, N. P., West, S. M., Quodling, A., & York, J. (2019). What do we mean when we talk about transparency? Toward meaningful transparency in commercial content moderation. International Journal of Communication, 13, 18.

University of Nairobi,(2023). University of Nairobi, about us. https://www.uonbi.ac.ke/fact-file Date Accessed, 09/11/2023

Voeten, Erik (2019). "Making Sense of the Design of International Institutions". Annual Review of Political Science. 22 (1): 147–163.

Vu, P., Adkins, M., & Henderson, S. (2019). Aware, but don’t really care: Student perspectives on privacy and data collection in online courses. Journal of Open, Flexible and Distance Learning, 23(2), 42–51. https://search.informit.org/doi/10.3316/informit.980808045440057

Wambiri, D., Masinde, J., & Mugambi, F. (2023). Big Data and Personal Information Privacy in Developing Countries: A Case of Kenya.

Wambugu, L., & Kyalo, D. (2013). Open and Distance Education as a Strategy for Improving Higher Education in the 21st Century in Kenya-a Case of the University of Nairobi. *Journal of Education and Practice*, *4*(14), 25-35

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.

Zou, Y., Mhaidli, A. H., McCall, A., & Schaub, F. (2018). " I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 197-216).

# QUESTIONNAIRE

Dear respondent,

This is to welcome you to this academic research in pursuit of a Master's degree for a topic entitled DATA PROTECTION AND EXPERIENCE OF STAKEHOLDERS AT THE UNIVERSITY OF NAIROBI. The study is confidential and observes all research and university protocols. All responses will be used strictly for academic purposes. Thank you and direct any inquires to the lead researcher, I, Evans Kinyua on 0705221692 or 0737443571.

Welcome

**Section 1: General Information**

1. Indicate your gender.

   A. Male, B. Female

2. Indicate your age.

   A. Below 18 years, B. 18 – 23, C. 24 – 41, D. 42 – 58, E. Above 58 years

3. What is your role at the University of Nairobi (UON)

   A. Student, B. Lecturer, C. Support staff D. Technical staff

4. Which system have your registered, managed, supported or used to carry out UON business (Tick √. all possible options)

| | |
|---|---|
| 4.1 Student Management information System(SMIS) | |
| 4.2 ECLASS/ E-learning | |
| 4.3 University of Nairobi(UON) Email | |
| 4.4 Zoom/Google Meet/Teams | |

**Section 2: Minimisation and confidentiality**

5. What personal information/data below did you provide to enable registration to the system(s) mentioned in section 1? (Tick √. all possible options)

| | |
|---|---|
| 5.1 Identification (ID, registration number, staff number) | |
| 5.2 static details (name, telephone number,adress) | |
| 5.3 Biometric data (fingerprint, voice or face print) | |
| 5.4 Academic certificates like KCSE, KCPE, bachelor's degree etc | |
| 5.5 Financial Information like fee payment, bank account details | |
| 5.6 Health information example HIV status, etc | |
| 5.7 Ownership information like your title deed and logbook details | |
| 5.8 Family details like children names, age, clan etc | |

6. Which of the following measures are used by university of Nairobi to promote confidentiality of data when accessing the systems under section 1. Tick √ Only one option per row

| | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 6.1 I have been assigned a user name and password to | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| access systems under section 1 | | | | | |
| 6.2 The password(s) I use on the systems are hidden from view after entry (hashed). | | | | | |
| 6.3 My personal information is only available after logging in with my credentials | | | | | |
| 6.4 My personal information is only accessible to me and not to the public | | | | | |

**Section 3: Transparency and Integrity**

7. Which of the following transparency measures have been applied by the university in relation to your personal information/data. Tick √ Only one option per row

| | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 7.1 I was informed of the reasons for collection of my personal information when registering to the systems | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 7.2 I accepted and submitted my personal information to the university systems on my own volition | | | | | |
| 7.3 I have been informed of breaches that have happened on my data example hacking | | | | | |

8. What integrity measures have been applied by the university of Nairobi in relation to the systems in section 1?

| | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 8.1 No erroneous personal data about me exists in UON systems | | | | | |
| 8.2 My identification details like the ID, telephone number and name in the systems cannot be amended without my authority | | | | | |
| 8.3 System errors cannot cause changes on the captured | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| personal information in UON systems | | | | | |

**Section 4: Availability**

9. Answer the following questions by marking √ only one option per row

| | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 9.1 I can access the personal information I have shared with university of Nairobi | | | | | |
| 9.2 I have not experienced any case of lost personal data in UON systems. | | | | | |
| 9.3 UON systems are stable and have minimal downtimes | | | | | |

10. Kindly tick any data item below that you have lost in UON systems? (Tick √. All possible options)

| | |
|---|---|
| 10.1 Course work or Exam marks | |
| 10.2 Financial information(payment) | |

| | |
|---|---|
| 10.3 Contact details | |
| 10.4 Education certificates | |
| 10.5 Health information | |
| 10.6 Others(indicate) | |

**Section 5: Experience of stakeholders**

11. What are your opinions about sharing your personal data/information? (Tick √. Only one option per row)

| | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 11.1Only people who have something to hide are afraid to share data | | | | | |
| 11.2 Sharing data is okay as long as I benefit from it | | | | | |
| 11.3 Before I share data, I must understand how it will be collected and how it is used. | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| 11.4 I worry about how data will be used but I share it because I trust the organization | | | | | |

12. In your opinion which of the following measures ensures safety of your data at UON(Tick √. Only one option per row)

| **Measures** | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 12.1 Staff integrity preventing alteration and leakage of your data | | | | | |
| 12.2 System stability at UON preventing data loss | | | | | |
| 12.3 Strong technological systems by UON preventing unauthorized access to your data | | | | | |
| 12.4 Transparency by UON on the parties accessing your data | | | | | |
| 12.5 UON preventing misuse of your images for marketing purposes | | | | | |

13. Which of the following measures are you likely to take in case you experience a breach, hack or loss of personal information shared with University of Nairobi(UON)? (Tick √. Only one option per row)

| **Measures** | **Strongly Agree** | **Agree** | **Don't know** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| 13.1 lodge a legal suit against the University for breach of privacy | | | | | |
| 13.2 Report to the office of the data protection commissioner | | | | | |
| 13.3 Organize protests against the university, with the other students affected | | | | | |
| 13.4 Report to the ICT department and demand an explanation. | | | | | |
| 13.5 Highlight the issue on social media | | | | | |
| 13.6 Cut relations with UON and exit | | | | | |

**SECTION 6: For staff only**

14. What means do the UON systems have to inform users on the reasons for collecting information? (Tick √. all possible options)

| | |
|---|---|
| 14.1 UON Privacy policy | |
| 14.2 Terms and conditions on systems | |
| 14.3 Information of physical informs | |
| 14.4 Others(indicate) | |

15. Do you train users on data collection, data sharing and how they should protection their personal information while using the UON systems?

A. Yes, B. No