International Research Journal Of Business and Strategic Management

Vol 8, Issue 1, pp 25-40, April 9, 2026, © International Research Journal Publishers, ISSN 2710-2742 (online) www.irjp.org

Data Management Practices and Implementation of Data Privacy Regulations among Internet Service Providers in Nairobi City County, Kenya

[1*]Miriam Namudeche and [2]Dr. Emmy Rotich, Phd

[1*]Master's Student, Jomo Kenyatta University of Agriculture and Technology

[2]Lecturer, Jomo Kenyatta University of Agriculture and Technology

Accepted, April 9th, 2026

Abstract

Internet Service Providers (ISPs) in Kenya face increasing scrutiny regarding their compliance with the Data Protection Act (DPA) of 2019 due to the rapid growth of digital technologies and the resulting accumulation of personal data. Although Kenya has a well-established legal framework for data protection, most ISPs encounter operational, technical, and resource-related challenges that hinder full compliance. The study was anchored on Privacy Theory and the Resource-Based View to explain how organizational behavior, system effectiveness, privacy considerations, and internal resources influence the implementation of data privacy regulations. The study adopted a descriptive survey research design targeting ISP employees and customers in Nairobi City County, Kenya. The target population comprised 1,542,303 respondents, from which a sample size of 384 was determined using the Krejcie–Morgan formula. Data were collected using structured questionnaires and interview guides. Both descriptive and inferential statistical analyses were conducted using SPSS version 25. The findings revealed strong and statistically significant positive correlations between data management practices and the implementation of data privacy regulations. Specifically, Data Processing ($r = 0.751$) and Data Resources ($r = 0.799$) were all significantly associated with regulatory compliance ($p < 0.001$). The multiple regression revealed that a combination of these variables explained 89.8% of changes in the actual enforcement of data privacy regulations. Data Processing was the most influential ($\beta = 0.498$), followed by Data Resources ($\beta = 0.209$). The paper concludes that effective and integrated data management practices play a vital role in improving adherence to the data privacy regulation among the ISPs in Kenya. Compliance, reduced data breach, and customer trust are higher in those ISPs that invest in secure infrastructure, staff training and regulatory-compliant processes. The research suggests specific training of the ISP staff and enhancing the cooperation of ISPs with the Office of the Data Protection Commissioner. Moreover, compliance and preservation of user data in the highly dynamic digital landscape within the Kenyan context require constant supervision, capacity-building efforts, and the adoption of new advanced technologies.

Keywords: *Information Security, Regulatory Compliance, Data Processing, Organizational Resources, Consumer Data Protection*

INTRODUCTION

Adequate data management practices and adherence to the provisions of data privacy regulations

of the ISPs should be in place (Zichichi et al., 2022). These organizations store and process large volumes of user data and personal information, which requires sophisticated data management. Standards promote the quality, security, and usability of data while increasing the confidence of the users in the information they receive. ISPs have a critical role in facilitating access to the digital world for businesses, individuals, and institutions, making it essential to have sound practices of handling collected data (Fernandez, 2022). However, the increasing interconnectedness and density of digital networks, as well as accelerating rates of data generation and distribution, present challenges for the uniformity and security of data handling.

There has been increased emphasis on data privacy regulations in Kenya following the enactment of the Data Protection Act, 2019 (Mukuki & Assenga, 2024). This legislation aims at ensuring that local practices adhere to international regulations like the GDPR. To the ISPs in Nairobi City County, Kenya, these regulations are more than just the legal requirements that they have to meet, but rather tools that can be utilized to promote consumer confidence within the market (Erforth & Martin-Shields, 2022). Nevertheless, deficiencies in implementation, low visibility, and budgetary issues have prevented full compliance among some caregivers, which poses risks of data leakage and exploitation to the users (Kabata & Garaba, 2020).

Technological capacity plays a critical role in shaping data management practices and privacy regulation implementation in Nairobi City County, Kenya (Wanekeya, 2023). ISPs need to spend more on these areas by implementing efficient systems, training employees, and forming strategic collaborations to overcome these gaps. It is also essential to actively engage with regulatory agencies when it comes to overcoming such obstacles as cyber risks and the lack of robust compliance structures (Mukuki & Assenga, 2024). Gaining an understanding of the current practices in data management and privacy regulation implementation among ISPs in Nairobi City County, Kenya, gives an insight into the current challenges and potential areas for enhancing data security and privacy in Kenya's emerging digital economy.

Statement of the Problem

The accelerating growth of digital technologies, together with Internet expansion, has generated a massive surge in data acquisition, storage, processing and utilization activities for different entities, especially Internet Service Providers. According to available data for early 2024, the internet realization rate in Kenya reached 40.8% while Nairobi City County recorded 52.4% penetration (Ademi, 2024). Mobile Network Operators gain access to large data sets comprised of user location information and both phone call logs and mobile money transaction records because SIM card registration is now required. The Data Protection Act of 2019 has been passed in Kenya, but implementation and enforcement problems persist mainly among ISPs.

Data privacy enforcement faces a significant weakness because Internet Service Providers show little commitment to following data protection requirements (Florido-Benítez, 2024). Multiple instances of data breaches, together with emerging reports of unapproved data sharing and inadequate data protection processes have generated essential doubts about how well the public regulatory structure works (Ibrahim et al., 2020). The period from July 2022 through June 2023 brought 855 million cyber threats (Florido-Benítez, 2024) to Kenya, which demonstrates how personal data remains exposed because data protection standards are insufficiently established. Digital services in Nairobi City County face increased security threats because they are the densest concentration in this area. Data privacy rights and ISP obligations remain unclear to many consumers since they have insufficient knowledge about them. The DPA rights awareness of many internet users remains low because of which they struggle to make responsible decisions about their data sharing activities (Kuner et al., 2020). The insufficient level of information

literacy causes people to remain uninterested in data protection systems, which lead to diminished effectiveness of privacy laws (Lancieri, 2022). Privacy concerns regarding online data access affect the majority of consumers because only 32% trust standard data protection protocols, according to research by the International Association of Privacy Professionals.

The Office of the Data Protection Commissioner (ODPC) struggles to assess and control data practices implemented by Internet service providers (ISPs) as part of its responsibility to enforce the DPA. The scarcity of evidence about ISP compliance creates doubts about current enforcement systems, which monitor their practices (Munyendo et al., 2023). The weak standards of penalties and insufficient auditing allow data breaches and privacy rights violations to endure, which makes it challenging to guarantee privacy protection. The absence of systematic evaluation regarding how Internet Service Providers implement the DPA creates a fundamental knowledge gap because researchers lack understanding about the legal compliance of data management (Maina, 2021; Ibrahim et al., 2020). Previous research about ISP adherence to the law provides scant information on general privacy concerns but lacks a specific analysis of how ISPs meet legal requirements.

This research investigates both data management techniques and data privacy regulatory compliance among Internet service providers operating within Nairobi City County. The study offers important implementation insight to regulators as well as policymakers through its evaluation of non-compliance zones, together with enforcement procedures and consumer privacy understanding. The expansion of Kenya's digital environment requires immediate attention to data privacy enforcement because it is essential for consumer protection and regulated Data Protection Act compliance. This study aims to establish whether there is indeed a relationship between data processing and data resources on the implementation of data privacy regulations among internet service providers in Nairobi City County, Kenya.

Objectives of the Study

The general objective of this study is to assess data management practices and implementation of data privacy regulations among Internet Service Providers in Nairobi City County, Kenya.

Specific Objectives

i. To examine the relation between data processing and implementation of data privacy regulations among internet service providers in Nairobi City County, Kenya.
ii. To analyze the relationship between data resources and implementation of data privacy regulations among internet service providers in Nairobi City County, Kenya.

LITERATURE REVIEW

Theoretical Framework

Privacy Theory

The privacy theory also informs the current study. This theory was first developed by Samuel Warren and Louis Brandeis in 1890. Privacy Theory focuses on the principles and practices that govern the processing of personal data, emphasizing the need for transparency, accountability, and consent. This theory is particularly relevant to the study objective, as it provides a framework for understanding how data processing activities align with legal requirements and ethical standards in data privacy. By examining how ISPs in Nairobi City County, Kenya, implement data processing practices, the study can identify gaps and strengths in compliance with privacy regulations. This theory helps to highlight the importance of lawful data processing and the implications of non-compliance. Moreover, it can guide ISPs in adopting best practices that not only fulfill regulatory obligations but also enhance consumer trust and data security. By integrating Data Protection Theory, the study can contribute to a deeper

understanding of the complexities involved in data processing and its impact on privacy regulation implementation.

Resource-Based View (RBV)

The study was also anchored on a Resource-Based View (RBV). This theory was first developed by Barney in 1991, and it posits that a firm's resources and capabilities are critical for achieving competitive advantage. This theory is relevant to the study objective as it allows for an exploration of how data resources such as technology, human capital, and organizational processes affect ISPs' ability to implement effective data privacy regulations. By examining the quality and availability of these resources, the study can assess how they influence compliance with privacy regulations and the implementation of data privacy regulations among Internet Service Providers in Nairobi City County, Kenya. The RBV highlights that ISPs with superior data management resources are likely to perform better in regulatory compliance, thus enhancing their reputation and consumer trust. This theory provides a strategic lens through which to analyze the interplay between data resources and regulatory practices, offering insights into how ISPs can leverage their capabilities to improve data privacy outcomes in Nairobi City County, Kenya.

Conceptual Framework

A conceptual framework is the visual representation of a written description of the relationship between variables. This mostly implies the relationship between independent and dependent variables in the sense of how different factors of independent variables affect the dependent variables. Below is a conceptual framework of the relationship between data processing and Data Resources as independent variables and effective data privacy regulations as the dependent variable in Figure 1.

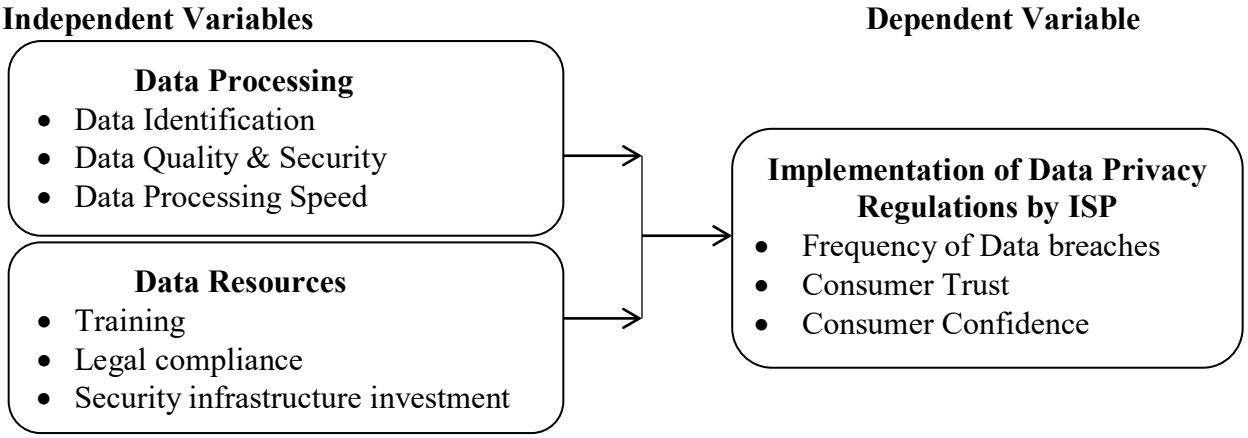

Figure 1: Conceptual Framework

Empirical Review

Data Processing and Implementation of Data Privacy Regulations among ISPs

According to Tosza (2021), the implementation of data privacy laws by Internet service providers (ISPs) has been strongly discussed internationally. There is a changing nature of the data processing practices of ISPs in response to new privacy regulations. The authors contend that ISPs need to handle regulatory confusion, particularly relevant in countries with strong legal regimes such as the European Union's General Data Protection Regulation (GDPR). Based on their results, it is clear that compliance not only fosters consumer trust but also motivates all ISPs to implement best practices related to data management. The study emphasizes the necessity for ISPs to implement transparent data processing policies and invest in technologies that ensure

user data is protected from breaches, thereby fostering a culture of accountability.

A study by Karale (2021) examined how the data processing device affects privacy enforcement laws in different countries. McCarthy points out that although many countries have comprehensive data protection legislation, the reality is different; ISPs have very different implementations of this legislation. It looked into the role of regulatory bodies in promoting compliance and in maintaining data processors complying with their best practices. The research sheds light on how to create a leaner, cheaper, and easier environment for innovation. Karale (2021) revealed that there is a need for continued cooperation between ISPs and regulators to resolve issues in data privacy, which in this context is further complicated by the continuing advances in technologies. This study calls for a global dialogue on harmonizing data privacy regulations to create a more secure digital environment for users worldwide.

Implementation of data privacy legislation by ISPs (Internet service providers) in Africa is riddled with problems. According to Hersi (2022), paraphrasing the issues ISPs have in Nigeria, the state of data processing practice in Nigeria is presented in this work, emphasizing the necessity of robust regulatory structures. According to the authors, following the introduction of the Nigerian Data Protection Regulation (NDPR), many ISPs have access problems on the road to compliance because of the lack of infrastructure and lack of knowledge of data privacy regulations. Their study makes it clear that good data management practices are also important to create users' trust and improve the overall security of digital services. Hersi (2022) also established that governmental support and capacity-building support in greater ISPs contribute to enhancing data privacy legislation compliance.

Barasa (2023) pointed out that a further study focused on the ISP's challenges in implementing data privacy regulations in Kenya. The authors stress that although the Data Protection Act (DPA) offers a legal context for processing data, much has been left to too many ISPs who are not equipped with the bandwidth, expertise, and understanding of when legal requirements must apply. Based on their conclusions, it is found that user knowledge about data privacy rights is also limited, thus adding to the difficulty of regulation enforcement. Barasa (2023) recommended the need to focus training packages for ISPs and mass media awareness initiatives are crucial tools in closing the knowledge deficit. They argue that fostering a culture of data protection is vital for enhancing user confidence and promoting responsible data processing practices among ISPs in Kenya.

In Kenya, Akanfe et al. (2020) assessed the adoption of data privacy laws is becoming more and more crucial as digital services grow in popularity. The study aimed to assess the effectiveness of the Data Protection Act (DPA) in guiding ISPs' data processing practices. The authors concluded that although the DPA has set benchmarks, a lack of awareness and inability to manage resources are making implementations on the part of the ISPs a challenge. The study underlines the need for ongoing training and support of ISPs so that ISPs can implement data privacy measures appropriately. It also pointed out that cooperation among stakeholders, i.e., the government, ISPs, and civil society, is essential to implement a matrix of accountability in data processing.

Mutua (2023) conducted a study on data privacy perception among users, focusing on the role of ISPs in Kenya. Their results demonstrate that a significant number of users are not informed about their rights accorded by the DPA, which raises potential data misuse. The findings of the study demonstrated that increased awareness of the users is key to fostering informed consent and responsible data processing of ISPs. The study, therefore, proposed that ISPs should give importance to transparency in data processing undertaken by them to merit trust amongst the

people. They conclude that a proactive approach to user education, coupled with stringent regulatory enforcement, is key to enhancing data privacy in Kenya's digital landscape.

Data Resources and Implementation of Data Privacy Regulations among ISPs

A study by Singh and Shanker (2024) focused on the critical role of Internet Service Providers (ISPs) in the data privacy regulatory space. In Singh and Shanker (2024), it is revealed that ISPs are responsible for much of the control and supervision of user data as they have to adhere to strict regulatory limits to protect the right to privacy of the consumers. The paper demonstrates that ISPs often act as gatekeepers that monitor what reaches the end audience and, at the same time, are entrusted with data protection from attacks. This evidence indicates that successful data privacy legislation improves not only trust among consumers but also promotes a competitive market structure. In addition, the present work supports the development of a holistic regulatory environment that can obligate ISPs for data protection, thereby fulfilling the safeguards of user rights within the digital world.

Laurer and Seidl (2021) conducted a study laying focus on the effect of the General Data Protection Regulation (GDPR) in Europe, which requires ISPs to develop strict control for data (13). The research identifies how GDPR has transformed data privacy practices, compelling ISPs to adopt robust security measures and transparent data processing policies. Laurer and Seidl, (2021) maintain that the regulation has made a notable contribution to raising the awareness of users about data privacy and contributed to the greater responsibility of ISPs. The study illustrates how continuous supervision and enforcement are crucial for compliance and proposes that an analogous system might be important in other countries to improve the protection of data and user trust for digital services.

In DRC, Musole and Rwabashi (2021) examined the challenges ISPs are encountering in applying data privacy regulations across the continent. The research also shows that, despite the enactment of the data protection law across African countries, the quality of implementation is low due to the discrepancy in available resources and user's ignorance of the topic. Musole and Rwabashi (2021) emphasized the need for capacity building within regulatory agencies and ISPs to enable proper implementation of data privacy legislation. Their results indicate that cooperation among governments, ISPs, and civil society is necessary to establish a favorable ecosystem for data protection with a consequence of increased user trust in digital services in Africa.

In Nigeria, Okesola et al. (2020) conducted a study on the internet service providers' responsibilities in botnet mitigation and ISP's function for privacy protection. The paper highlighted that a growing concern for data leakage arises and that the possibility of using anonymized data for ISPs to offer compliance with the Nigeria Data Protection Regulation (NDPR) is of no small moment. Evidence from the literature review is that while ISPs are only now beginning to deploy better data management methods, there remain significant gaps in the awareness and education of ISP users of their rights. Okesola et al. (2020) support the implementation of targeted messaging campaigns to educate users on data privacy, as well as user responsibilities of ISPs. Their results highlight the need to develop an environment of data privacy that enables users and ISPs to give privacy a central role in operations.

In Kenya, Bock et al. (2021) assessed the effects of the Data Protection Act (DPA) implementation and its potential impact on the ISPs. The study shows that the DPA has already implemented a legal framework, to protect personal data, but enforcement still suffers. The study established that compliance poses much of a challenge for ISPs because of a lack of knowledge of the regulations and a lack of resources. In the research, increased capacity to undergo training

and support for ISPs that would enable them to undertake measures in terms of data privacy significantly is recommended. Furthermore, the study emphasized the need for ongoing dialogue between ISPs, regulators, and consumers to build trust and ensure that data protection is prioritized in Kenya's digital landscape.

Ziwa (2021) examined users' views on data privacy among Kenyan ISP consumers. According to the results, it is found that a large number of users do not know their data rights or the obligation of ISPs according to the DPA. Juma (2022) also established that there is a need for user education programs to illustrate and encourage informed consent for data processing. Their research indicates that enhancing user knowledge about data privacy can lead to greater accountability among ISPs. In suggesting prioritizing the creation of a culture of transparency and trust in Kenya to better serve the needs of users and service providers in the digital ecosystem, the authors argue that this is key to fully realizing the potential of data privacy regulations.

Implementation of Data Privacy Regulations among ISPs

According to Hartzog & Richards (2020), data protection is presented as an absolute right in the European Union, and privacy is comparable to any other human right. This commitment to individual freedoms has both taken off internationally and regionally, and this growth in data protection is in line with the role it plays in the information age. From a business perspective, any outage in ISP communication and service delivery could lead to substantial user losses. These breaches can also deprive users of the ability to publish critical information to the public, not just for the people that have contracts with the ISP but also for the society at large, that has a stake in accessing this information. For example, a bank account holder may incur a financial loss if they are unable to cover an e-ticket purchase via e-banking due to an ISP service outage related to causes.

Cooray (2023) in Malaysia has shown that an Internet Service Provider (ISP), or an Internet Access and Service Provider (IASP), is one of those intermediary companies, the ones playing significant roles in a wide range of activities in a digitalizing era like e-government, e-learning, e-banking, and e-business, etc. ISPs do it by allowing communities to go online and use various ICT as end users. The digitization and processing of electronic data and information depend on the internet connectivity. Thus, such interactive companies offering internet services and electronic information are critical for promoting electronic transactions. Users can access cyberspace via an ISP, whereby they can access much sought-after useful and entertaining information. For example, in Indonesia, the Internet has become deeply embedded in daily life, especially for urban populations. This trend parallels that of communities in industrialized areas of Europe and the US, where the web has been used for information access for a long time but also as one of the ways to store personal information.

Garcia (2024) points out that Internet Service Providers (ISPs) are commonly perceived as gatekeepers to the web, noting the importance of their role in issues arising in the digitalization process. Interface (e.g., intermediary organizations, ISPs) is seen to respond to the challenge of offering internet access to audiences, i.e., website owners and cyberspace residents. In this role, maintaining the quality of Internet services for different kinds of users, including government organizations, schools, businesses, and people using the Internet for transactions, is part of the activities of a staff member. Inter-process communication IPCs are being increasingly correlated with liabilities in the area of Cloud Computing Services, especially regarding the storage of individual data. In addition to accessing the internet for information purposes, users use the internet to store personal and business sensitive information that is an attractive target for

intrusion. In this sense, ISPs have obligations the prevent such security threats. Liyanaarachchi et al. (2021) highlights the duty of Online Service Providers to protect user data against data breaches. Incidents and attacks, are increasing in frequency both around the world and locally, emphasizing the critical requirement for strong data protection.

According to Kröger et al. (2021), people are exposed to risks not only through security breaches but also through the possible and intended exploitation of users' data linked to government policies. For instance, in early 2017, the Indonesian government mandated mobile phone users to register their numbers, requiring personal data such as identity cards and family cards. This resulted in cases where information was misused, for instance, the use of customer information to subscribe to several cellular numbers without explicit permission. Communities affected by breaches of confidentiality and misuse of personal data stored in cloud services or mandated by government policies have the right to seek accountability from those responsible for the losses incurred.

METHODOLOGY

The study adopted a mixed study design to investigate data management practices and the implementation of data privacy regulations among Internet Service Providers (ISPs) in Nairobi City County, Kenya. It details the research design, target population, sampling procedures, data collection instruments, validity and reliability measures, data analysis techniques, and hypothesis testing framework.

The study used a descriptive survey research design with a cross-sectional approach, conducted during normal institutional operations. A mixed-methods strategy was employed, integrating both quantitative and qualitative approaches to provide comprehensive insights. Quantitative data were collected using structured questionnaires to assess compliance levels and data management practices, while qualitative data were obtained through interviews to capture stakeholder experiences and perspectives.

The target population comprised ISP staff and internet consumers aged 20 years and above in Nairobi City County, totalling 1,542,303 individuals. Using the Krejcie and Morgan (1970) formula, a representative sample size of 384 respondents was determined. Proportional sampling was applied to select ISP key leaders, staff, and consumers. Questionnaires with open- and closed-ended items, structured on a five-point Likert scale, served as the primary data collection instruments, supplemented by secondary data from ISP annual reports.

Data collection followed formal authorization procedures, including a letter of introduction from JKUAT, and emphasized confidentiality and voluntary participation. A pilot study involving 5% of the sample was conducted to test the validity and reliability of the research instruments. Content and construct validity were ensured through expert review, while reliability was assessed using Cronbach's alpha coefficients.

Quantitative data were cleaned, coded, and analyzed using SPSS version 25. Descriptive statistics, correlation analysis, ANOVA, and multiple regression analysis were employed. Diagnostic tests for linearity and multicollinearity were conducted using tolerance and VIF criteria. Hypotheses were tested at a 5% significance level using a multiple regression model examining the relationship between processing and resources, and the implementation of data privacy regulations.

FINDINGS AND DISCUSSIONS

Descriptive statistics

Data Processing and Implementation of Data Privacy Regulations among Internet Service Providers

The study aimed to assess the relationship between data processing and the implementation of data privacy regulations among Internet Service Providers (ISPs) in Nairobi City County, Kenya. Data processing was measured by speed, accuracy, security, compliance with standards, and staff competence. On whether ISPs process internet usage data quickly without quality issues, a majority 72.29% agreed, 18.47% disagreed, and 9.24% were neutral (mean = 2.54, SD = 0.79). Regarding accuracy of data handling, 57.83% agreed, 26.91% disagreed, and 15.26% were neutral (mean = 2.31, SD = 0.87), showing room for improvement in precision.

Security during processing was highly affirmed, with 94.40% agreeing, only 1.20% disagreeing, and 4.40% neutral (mean = 2.93, SD = 0.30). Likewise, 91.60% agreed that processing speed meets organizational needs, with minimal disagreement (0.40%) (mean = 2.91, SD = 0.30). Compliance with international standards was also rated very high 96.40% agreement and 3.60% disagreement (mean = 2.96, SD = 0.19). Lastly, staff training was almost unanimously endorsed, with 98% agreement (mean = 2.98, SD = 0.14).

The findings indicate that ISPs demonstrate strong capacity in secure, timely, and standards-compliant data processing, with well-trained staff. However, accuracy levels, while generally positive, present an improvement opportunity. Enhancing precision would further strengthen regulatory compliance and stakeholder trust.

Table 1: Data Processing and Implementation of Data Privacy Regulations

Statement	Agree	Disagree	Neutral	Mean	Standard Deviation
I believe ISP process internet usage data quickly without quality issues.	72.29%	18.47%	9.24%	2.54	0.79
ISP data handling is accurate.	57.83%	26.91%	15.26%	2.31	0.87
ISP has security measures to protect data during processing.	94.40%	1.20%	4.40%	2.93	0.30
ISPs data processing speed meets their needs.	91.60%	0.40%	8.00%	2.91	0.30
ISP data processing aligns with international standards.	96.40%	3.60%	-	2.96	0.19
ISP staff are trained to securely process data.	98.00%	2.00%	-	2.98	0.14

Data Resources and Implementation of Data Privacy Regulations among Internet Service Providers

The study aimed to analyze the relationship between data resources and the implementation of data privacy regulations among internet service providers (ISPs) in Nairobi City County, Kenya. Data resources were assessed through indicators such as staff training, security infrastructure, legal compliance, financial adequacy, efficiency in resource use, and alignment with organizational goals. Findings show that a large majority of respondents (93.2%) agreed that ISP staff receive regular training on data resources and management, with a mean score of 2.93 (SD = 0.25), indicating strong consensus. However, responses were more divided on the adequacy of investment in security infrastructure, with 34.54% agreeing, 35.74% disagreeing, and 29.72% neutral (mean = 1.99, SD = 0.84), suggesting room for improvement.

A vast majority (91.16%) agreed that legal compliance is strictly upheld (mean = 2.89, SD = 0.39), highlighting ISPs' commitment to regulatory adherence. Additionally, 78.4% of

respondents indicated that financial resources for data management are sufficient (mean = 2.67, SD = 0.67), though 11.6% disagreed and 10% remained neutral. Efficiency in the use of data resources was affirmed by 96.4% of respondents (mean = 2.95, SD = 0.29), and an even higher proportion (98.8%) agreed that data resources align with organizational goals (mean = 2.98, SD = 0.15), showing a clear link between resource management and strategic direction.

The results suggest that ISPs in Nairobi have established strong internal capacities in training, legal compliance, and strategic alignment of data resources, which are critical enablers for the effective implementation of data privacy regulations. However, the mixed views on the adequacy of security infrastructure investment highlight a potential vulnerability that could undermine compliance efforts and expose organizations to data breaches. Addressing this gap through enhanced funding and technology upgrades could strengthen regulatory adherence and consumer trust.

Table 2: Data Resources and Implementation of Data Privacy Regulations

Statement	Agree	Disagree	Neutral	Mean	Standard Deviation
ISPs staff receive regular training on data resources and management.	93.20%	6.80%	-	2.93	0.25
ISPs invest heavily in security infrastructure is adequate.	34.54%	35.74%	29.72%	1.99	0.84
ISPs ensures that legal compliance is strictly upheld.	91.16%	2.41%	6.43%	2.89	0.39
ISPs financial resources for data management are sufficient.	78.40%	11.60%	10.00%	2.67	0.67
ISPs ensure that data resources are used efficiently.	96.40%	1.60%	2.00%	2.95	0.29
ISPs data resources align with organizational goals.	98.80%	0.40%	0.80%	2.98	0.15

Implementation of Data Privacy Regulations among Internet Service Providers

The main objective of this section was to determine how the implementation of data privacy regulations affects compliance practices among Internet Service Providers (ISPs) in Nairobi City County, Kenya. In this study, implementation was measured by adherence to laws, enforcement of breach policies, employee training, and the role of privacy policies in building customer trust and confidence.

On whether ISPs follow all data privacy laws, 98.40% of respondents agreed, only 0.40% disagreed, and 1.20% were neutral (mean = 2.98, SD = 0.17), showing near-universal compliance. Similarly, 96.40% affirmed that data breach policies are enforced, 0.40% disagreed, and 3.20% were neutral (mean = 2.96, SD = 0.22), indicating strong operational safeguards. Employee training on data privacy rules was rated extremely high, with 98.80% agreement and only 1.20% disagreement (mean = 2.99, SD = 0.11). Likewise, the role of privacy policies in building customer trust was almost unanimously recognized—99.20% agreed, 0.40% disagreed, and 0.40% were neutral (mean = 2.99, SD = 0.14). Consumer confidence was similarly high, with 98.80% agreement (mean = 2.98, SD = 0.19).

The findings imply that ISPs in Nairobi demonstrate very strong compliance with data privacy regulations, underpinned by well-trained staff, clear enforcement policies, and robust privacy frameworks that enhance both customer trust and consumer confidence. This high level of

adherence suggests maturity in privacy governance, which can serve as a benchmark for other sectors handling sensitive data.

Table 3: Implementation of Data Privacy Regulations

Statement	Agree	Disagree	Neutral	Mean	Standard Deviation
ISPs follow all data privacy laws.	98.40%	0.40%	1.20%	2.98	0.17
ISPs ensure that data breach policies are enforced.	96.40%	0.40%	3.20%	2.96	0.22
I believe ISPs employees are trained on data privacy rules.	98.80%	1.20%	-	2.99	0.11
ISPs privacy policies build customer trust.	99.20%	0.40%	0.40%	2.99	0.14
ISPs privacy policies build consumer confidence	98.80%	0.80%	0.40%	2.98	0.19

Inferential Statistics

The significance of the relationship between the two components was evaluated by using correlation analysis to ascertain the correlation of the study variables. The two correlated variables move in the same direction when the correlation coefficient is positive, and in the opposite direction when it is negative. Essentially, correlation analysis reveals the strength of the association between one variable and another, but it does not imply a causal relationship. In this research, correlation analysis is conducted between the independent and dependent variables, with the results displayed in Table 4.

Correlation Analysis

The correlation analysis was done in order to ascertain the strength, direction, and significance of relationships between the study variables. The strength and direction of the correlation between the independent variables (Data Processing, and Data Resources), and the dependent variable (Implementation of Data Privacy Regulations) were measured using the correlation coefficient (r) of Pearson. The range of Pearson correlation coefficients is +1 to -1 in which closer to +1 is a strong positive relationship, closer to -1 is a strong negative relationship then closer to zero is the lack of linear relationship between two variables (Gujarati and Porter, 2016). A positive correlation means that the more a variable increase, the more another variable increases.

Pearson correlation matrix is presented in table 4.13. The correlation among the variables is high with all showing high positive correlation ranging between 0.751 and 0.950. The most significant correlations are noted between Data Resources (DR), and Implementation of Data Privacy Regulations (IDPR) whose coefficients are over 0.899 which implies a very high accuracy of interdependence. The data Processing (DP) presents a lower yet well-correlated value to the rest of the variables (r = 0.751-0.951), indicating that it could be affected by certain distinctive or independent variables.

Table 4: Pearson Correlation Matrix

	Data Processing (DP)	Data Resources (DR)	Implementation of Data Privacy Regulations (IDPR)
Data Processing (DP)	1		
Data Resources (DR)	.950	1	
Implementation of Data Privacy Regulations (IDPR)	.751	.799	1

Multiple Regression Analysis

The study carried out a multiple regression analysis to determine the nature of relationship of the model by predicting the dependent in terms of the independent variables using the following linear regression model.

Model Summary

The model summary shows how the rate of the independent variables explains the change in the dependent variable. The R value (.948) indicates an almost perfect positive correlation between the dependent variable (Implementation of Data Privacy Regulations) and the independent variables (Data Processing, and Data Resources). This means that changes in the independent variables are very strongly associated with changes in the dependent variable.

The R Square value (.898) reveals that 89.8% of the variation in Implementation of Data Privacy Regulations can be explained by the combined effect of Data Processing, and Data Resources. This is an exceptionally high explanatory power, leaving only 0.2% of the variation attributable to other factors not included in the model. The Adjusted R Square (.849) confirms the robustness of the model even after adjusting for the number of predictors.

The small Standard Error of the Estimate (0.146) further implies high accuracy in the model's predictions. Practically, this means effective management and improvement in data processing, and data resource allocation are almost certain to result in better compliance and execution of data privacy regulations. However, such high correlations may also indicate multi-collinearity, requiring careful statistical checks.

Table 5: Model Summary

Model	R	R Square	Adjusted R-Square	Std. Error of the Estimate
1	.948a	.898	.849	.14600

a. Predictors: (Constant), Data Processing, and Data Resources

b. Dependent Variable: Implementation of Data Privacy Regulations

ANOVA Test

The ANOVA was used to determine whether the model was a good fit for the data. According to statistical convention, the p-value of the F-ratio should be less than 0.05 for the regression equation to be statistically significant at the 5% level (Gujarat & Porter, 2016). In this analysis, the F-calculated value is 25,922.878, which is far greater than the typical F-critical value for (4, 285) degrees of freedom. The Significance F (p-value) is 0.000, which is less than 0.05, indicating the model is statistically significant. This means that at least one of the independent variables Data Processing, or Data Resources is a significant predictor of the dependent variable, Implementation of Data Privacy Regulations. The very high F-value reflects the model's exceptionally strong explanatory power, aligning with the earlier R^2 result (0.898).

This implies that improvements in any of the identified data management components are likely to produce meaningful and measurable enhancements in the implementation of data privacy regulations. However, such a high model fit also suggests the potential presence of multi-collinearity, which, while not diminishing predictive accuracy, may limit interpretability of individual predictor effects and should be addressed in further analysis.

Table 6: ANOVA Test

	Df	SS	MS	F	Significance F
Regression	4	2215.666	553.917	25922.878	0.000
Residual	285	5.256	0.021		
Total	289	2220.923			

Regression Coefficients

Findings from the regression analysis show that all beta coefficients for the independent variables were significant, with p-values less than the 0.05 significance threshold. This means that Data Processing (DP) and Data Resources (DR) are all significant predictors of the Implementation of Data Privacy Regulations. Data Processing ($\beta = 0.498$, $p = 0.000$) had the highest influence, indicating that for every unit increase in data processing effectiveness, there is a 0.498 unit increase in the implementation of data privacy regulations, holding other factors constant. This underscores the importance of efficient, accurate, and secure data processing systems in ensuring compliance. Portney et al. (2020) notes that well-structured processing workflow, reduce compliance risks and improve organizational accountability.

Data Resources ($\beta = 0.209$, $p = 0.000$) showed a positive and significant relationship, indicating that adequate technological, financial, and human resources directly enhance the capacity to meet privacy requirements.

These results imply that improving data privacy compliance requires a holistic approach. While data processing stands out as the strongest driver, success depends on strengthening all aspects of the data management chain from accurate collection, secure storage, and resource allocation, to processing efficiency. An integrated investment in these areas would certainly enhance adherence to data privacy regulations and reduce the risk of breaches or penalties.

Table 7: Regression Results

	Coefficients	Standard Error	t Stat	P-value	Lower 95%	Upper 95%	Lower 95.0%	Upper 95.0%
Intercept	.000							
Data Processing (DP)	.498	.048	10.367	.000	.404	.593	.404	.593
Data Resources (DR)	.209	.037	5.617	.000	.136	.283	.136	.283

CONCLUSIONS & RECOMMENDATIONS

Conclusions

The study concludes that data management practices have a significant and strong influence **on** the implementation of data privacy regulations among ISPs in Nairobi. The combined effect of Data Processing and Data Resources explains almost all variations in regulatory compliance, emphasizing the integrated nature of these practices. Accurate, ethical, and consent-based data collection significantly enhances compliance. However, weak tool usability may hinder efficiency and full compliance potential. Data Processing is the most critical driver of privacy regulation implementation. Efficient, accurate, secure, and standards-compliant processing systems ensure better adherence and reduced compliance risks. Secure storage systems strongly support compliance. However, sustainability concerns arise from low cost-effectiveness, which may affect long-term data governance. Adequate resources, financial, technical, and human, are essential to maintain high compliance levels. Gaps in security infrastructure investment could undermine otherwise strong compliance frameworks.

Recommendations

- Continue investing in staff training and secure, automated processing workflows.

- Ensure sustainable funding for data management operations to maintain long-term compliance.

Suggestions for Further Studies

- Investigate additional factors such as organizational culture, regulatory enforcement intensity, and emerging technologies that may influence data privacy compliance beyond the current four variables.

REFERENCES

Ademi, D. (2024). Digital Rights: A Critical Analysis of the Status of Online Freedom Of Expression In Kenya.

Ahmed, W., Shahzad, F., Javed, A. R., Iqbal, F., & Ali, L. (2021, April). Whatsapp network forensics: Discovering the IP addresses of suspects. In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-7). IEEE.

Akanfe, O., Valecha, R., & Rao, H. R. (2020). Assessing country-level privacy risk for digital payment systems. *Computers & Security*, *99*, 102065.

Barasa, F. A. (2023). *The Congruence of International Laws and Kenyan Laws about International Online Trade* (Doctoral dissertation, University of Nairobi).

Bock, K., Kühne, C. R., Mühlhoff, R., Ost, M. R., Pohle, J., & Rehak, R. (2021). Data protection impact assessment for the Corona app. *arXiv preprint arXiv:2101.07292*.

Cooray, M. A., Ahmad Rajuhan, I. S. B., & Binti Adnan, W. N. A. (2023). Industry approaches in handling online exploitation of children: A comparative study of the policy, guidelines and best practices in Malaysia, Singapore and Australia. *Cogent Social Sciences*, *9*(2), 2241713.

Erforth, B., & Martin-Shields, C. (2022). Where privacy meets politics: EU–Kenya cooperation in data protection. In *Africa–Europe Cooperation and Digital Transformation* (pp. 142-155). Routledge.

Fernandez Nieto, G. M., Kitto, K., Buckingham Shum, S., & Martinez-Maldonado, R. (2022, March). Beyond the learning analytics dashboard: Alternative ways to communicate student data insights combining visualisation, narrative and storytelling. In *LAK22: 12th international learning analytics and knowledge conference* (pp. 219-229).

Florido-Benítez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities*, *7*(1), 475-495.

Garcia, H. B. (2024). Mitigating Information Asymmetry in the 5G Era: unveiling practices that restrict users' Internet access.

Hartzog, W., & Richards, N. (2020). Privacy's constitutional moment and the limits of data protection. *BCL Rev.*, *61*, 1687.

Hersi, M. (2022). *Challenges Affecting Adoption of Big Data Analytics in Telecommunication Firms in Kenya* (Doctoral dissertation, University of Nairobi).

Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Frontiers in Computer Science*, *2*, 36.

Juma, C. W. (2022). *Examining Nairobi Internet Users' Attitudes Towards Newspaper Paywalls in Kenya* (Doctoral dissertation, University of Nairobi).

Kabata, V., & Garaba, F. (2020). The legal and regulatory framework supporting the implementation of the Access to Information Act in Kenya. *Information Development*, *36*(3), 354-368.

Karale, A. (2021). The challenges of IoT address security, ethics, privacy, and laws. *Internet of Things*, *15*, 100420.

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean Journal of Anesthesiology*, *72*(6), 558-569.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610.

Krishnamurthi, R., Gopinathan, D., & Kumar, A. (2021). Wearable devices and COVID-19: state of the art, framework, and challenges. *Emerging Technologies for Battling Covid-19: Applications and Innovations*, 157-180.

Kuner, C., Bygrave, L., Docksey, C., & Drechsler, L. (2020). *The EU general data protection regulation: a commentary*. Oxford University Press. Available at: https://global. oup. Com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826491.

Lancieri, F. (2022). Narrowing data protection's enforcement gap. *Me. L. Rev.*, *74*, 15.

Laurer, M., & Seidl, T. (2021). Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet*, *13*(2), 257-277.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*, *39*(4), 571-591.

Maina, D. K. (2021). *The Learning Curve: An exploration of the digital literacy dimension to ISPs* (Doctoral dissertation, Massachusetts Institute of Technology).

Mukuki, A., & Assenga, A. (2024). Comparative study of data protection legislation frameworks across the East African community. *D4D ACCESS*.

Munyendo, C. W., Acar, Y., & Aviv, A. J. (2023, May). "In Eighty Percent of the Cases, I Select the Password for Them": Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 570-587). IEEE.

Musole, T. M., & Rwabashi, J. P. M. (2021). Digital surveillance and privacy in DRC: Balancing national security and personal data protection.

Mutua, S. N. (2023). Exploring Public Perceptions towards Online Content Regulation in Kenya. *Multidisciplinary Journal of Technical University of Mombasa*, *2*(2), 37-51.

Nairobi City County. (2023). *County annual development plan (CADP) 2023/2024*. Nairobi City County Government.

Okesola, J. O., Adebiyi, M., Osi-Okeke, T., Adewale, A., & Adebiyi, A. (2020). Internet service providers' responsibilities in botnet mitigation: a Nigerian perspective. *International Journal of Electrical and Computer Engineering*, *10*(4), 4168.

Portney, B. A., Arad, M., Gupta, A., Brown, R. A., Khatri, R., Lin, P. N., ... & Zalzman, M. (2020). ZSCAN4 facilitates chromatin remodeling and promotes the cancer stem cell phenotype. *Oncogene*, *39*(26), 4970-4982.

Singh, A., & Shanker, N. (2024). Examining the Role of Internet Service Providers in Cyberspace: A Comparative Analysis of the Current Legal Landscape in India and the USA. *Educational Administration: Theory and Practice*, *30*(5), 7377-7390.

Story, D. A., & Tait, A. R. (2019). Survey research. *Anesthesiology*, *130*(2), 192-202.

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer law & security review*, *43*, 105614.

Wanekeya, E. (2023). *Effectiveness of Domestic Data Protection Laws in African Countries: A Case Study of the Data Protection Law in Kenya* (Doctoral dissertation, University of Nairobi).

Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. (2022). Data governance

through a multi-Cloud architecture in view of the gdpr. *Cluster Computing*, *25*(6), 4515-4542.

Ziwa, C. (2021). The Effectiveness of Legal Framework on Personal Data Protection in E-Commerce in Kenya. *Available at SSRN 4403156*.

Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: A classification of personal data misuses. *Available at SSRN 3887097*.