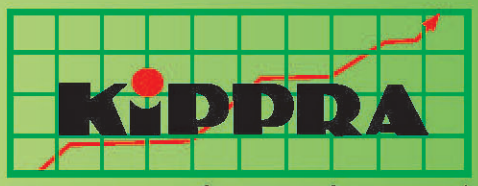
Discussion Paper Series



The KENYA INSTITUTE for PUBLIC
POLICY RESEARCH and ANALYSIS

Building Personal Data Sovereignty in Kenya

Humphrey Njogu

DP/320/2023

THE KENYA INSTITUTE FOR PUBLIC POLICY
RESEARCH AND ANALYSIS (KIPPRA)

Building Personal Data Sovereignty in Kenya

Humphrey Njogu

Kenya Institute for Public Policy
Research and Analysis

KIPPRA Discussion Paper No. 320
2023

KIPPRA in Brief

The Kenya Institute for Public Policy Research and Analysis (KIPPRA) is an autonomous institute whose primary mission is to conduct public policy research leading to policy advice. KIPPRA's mission is to produce consistently high-quality analysis of key issues of public policy and to contribute to the achievement of national long-term development objectives by positively influencing the decision-making process. These goals are met through effective dissemination of recommendations resulting from analysis and by training policy analysts in the public sector. KIPPRA therefore produces a body of well-researched and documented information on public policy, and in the process assists in formulating long-term strategic perspectives. KIPPRA serves as a centralized source from which the Government and the private sector may obtain information and advice on public policy issues.

Published 2023

Bishops Garden Towers, Bishops Road
PO Box 56445-00200 Nairobi, Kenya
tel: +254 20 2719933/4; fax: +254 20 2719951
email: admin@kippra.or.ke
website: http://www.kippra.org

ISBN 978 9914 738 07 0

The Discussion Paper Series disseminates results and reflections from ongoing research activities of the Institute's programmes. The papers are internally refereed and are disseminated to inform and invoke debate on policy issues. Opinions expressed in the papers are entirely those of the authors and do not necessarily reflect the views of the Institute.

Abstract

Personal data is an invaluable strategic resource for businesses and governments that drives economic growth and development. The ability to collect and use large volumes of personal data in an efficient manner has become an important component in today's data-driven world. However, in the digitally disruptive age of the Internet, involving unrestricted and unregulated processing of personal data outside a given jurisdiction popularly known as cross-border data transfers have raised concerns of privacy, trust, and sovereignty across many countries. Consequently, countries are seeking to reinstate their sovereignty over gaining control and use of personal data by embracing Data Localization measures. This paper seeks to appraise policy efforts for safeguarding the personal data sector against increasing privacy and security-related threats with a goal of building data sovereignty in Kenya. The paper applied exploratory approach guided by OECD data governance framework that comprised of three pillars: Strategic pillar; Tactic pillar; and Delivery pillar. A systematic review of secondary sources of information including policy and legal documents drawn from local and international scene was carried out. Overall, Kenya's data localization regulations are less strict, not fully implemented and are barely three years old.

Strategic pillar: The key policy issues include absence of a national comprehensive data management policy, and supporting strategies and procedures to provide a road map of how data localization initiatives are to be rolled out. Formulation and implementation of a national comprehensive data management policy framework is instrumental in providing strategic direction on processing of personal data. The framework covers quality, standards, security and sharing of personal data while taking considerations on the new risks being introduced by merging technologies, including artificial intelligence. Provision of resources to support key data localization activities, including awareness creation is necessary to steer the development of personal data economy. It is paramount to strengthen sectoral-based approach in personal data management and consider localizing certain categories of personal data for critical sectors such as health before embarking on massive data localization across all sectors.

Tactical pillar: There are inadequate professionals possessing advanced digital skills to support the growth of a vibrant personal data economy. Prioritizing building of essential digital skills on the emerging technologies, including artificial intelligence, data analytics and privacy enhancing technologies will facilitate a vibrant personal data economy. A comprehensive innovation framework is key to supporting nurturing, development and scaling up of innovations on personal data.

Delivery pillar: Key policy issues include digital divide, high Internet cost, costly devices, fewer certified data centres and increasing cyber threats. Other issues include low uptake of local data storage services and inadequate smart data centres to host local personal data. Building essential digital infrastructure, such as data centres, and Internet connectivity by partnering with private sector and tapping on the Universal Service Fund will support development of robust data sovereignty in Kenya. Other key considerations include fast-tracking the rolling out of the national digital superhighway and Digital Masterplan initiatives, and incentives to investors to access basic infrastructure services such as power and Internet to spur growth and development of the local data economy in Kenya.

Abbreviations and Acronyms

BETA	Bottom-up Economic Transformation Agenda
BPO	Business Process Outsourcing
BRICS	Brazil,Russia, India, China, and South Africa
CA	Communications Authority of Kenya
CIIs	Critical Information Infrastructures
CMCA	Computer Misuse and Cybercrimes Act
CSPs	Cloud Service Providers
DCs	Data Cooperatives
DLP	Digital Literacy Programme
DSPs	Data Sharing Pools
DPA	Data Protection Act
GCCN	Government Common Core Network
ICCPR	International Covenant on Civil and Political Rights
IoT	Internet of Things
ISPs	Internet Service Providers
ITU	International Telecommunication Union
KAIST	Kenya Advanced Institute of Science and Technology
KE-CIRT/CC	Kenya Computer Incident Response Team and coordination Centre
KENET	Kenya Education Network
KIPPRA	Kenya Institute for Public Policy Research and Analysis
KODI	Kenya Open Data Initiative
MICDE	Ministry of Information Communications and Digital Economy
NAS	National Addressing System
NPKI	National Public Key Infrastructure
NC4	National Computer and Cybercrimes Coordination Committee
NOFBI	National Optic Fibre Backbone
NRI	Network Readiness Index
NSA	National Security Agency
ODPC	Office of the Data Protection Commissioner
OECD	The Organisation for Economic Co-operation and Development
PDTs	Public Data Trusts
PDS	Personal data sovereignty
PDTP	Presidential Digital Talent Programme
SP-CMM	Security and Privacy Capability Maturity Model
TVET	Technical and Vocational Education and Training
USA	United States of America
VDI	Virtual Desktop Infrastructure
Wi-Fi	Wireless Fidelity

Abstract

Personal data is an invaluable strategic resource for businesses and governments that drives economic growth and development. The ability to collect and use large volumes of personal data in an efficient manner has become an important component in today's data-driven world. However, in the digitally disruptive age of the Internet, involving unrestricted and unregulated processing of personal data outside a given jurisdiction popularly known as cross-border data transfers have raised concerns of privacy, trust, and sovereignty across many countries. Consequently, countries are seeking to reinstate their sovereignty over gaining control and use of personal data by embracing Data Localization measures. This paper seeks to appraise policy efforts for safeguarding the personal data sector against increasing privacy and security-related threats with a goal of building data sovereignty in Kenya. The paper applied exploratory approach guided by OECD data governance framework that comprised of three pillars: Strategic pillar; Tactic pillar; and Delivery pillar. A systematic review of secondary sources of information including policy and legal documents drawn from local and international scene was carried out. Overall, Kenya's data localization regulations are less strict, not fully implemented and are barely three years old.

Strategic pillar: The key policy issues include absence of a national comprehensive data management policy, and supporting strategies and procedures to provide a road map of how data localization initiatives are to be rolled out. Formulation and implementation of a national comprehensive data management policy framework is instrumental in providing strategic direction on processing of personal data. The framework covers quality, standards, security and sharing of personal data while taking considerations on the new risks being introduced by emerging technologies, including artificial intelligence. Provision of resources to support key data localization activities, including awareness creation is necessary to steer the development of personal data economy. It is paramount to strengthen sectoral-based approach in personal data management and consider localizing certain categories of personal data for critical sectors such as health before embarking on massive data localization across all sectors.

Tactical pillar: There are inadequate professionals possessing advanced digital skills to support the growth of a vibrant personal data economy. Prioritizing building of essential digital skills on the emerging technologies, including artificial intelligence, data analytics and privacy enhancing technologies will facilitate a vibrant personal data economy. A comprehensive innovation framework is key to supporting nurturing, development and scaling up of innovations on personal data.

Delivery pillar: Key policy issues include digital divide, high Internet cost, costly devices, fewer certified data centres and increasing cyber threats. Other issues include low uptake of local data storage services and inadequate smart data centres to host local personal data. Building essential digital infrastructure, such as data centres, and Internet connectivity by partnering with private sector and tapping on the Universal Service Fund will support development of robust data sovereignty in Kenya. Other key considerations include fast-tracking the rolling out of the national digital superhighway and Digital Masterplan initiatives, and incentives to investors to access basic infrastructure services such as power and Internet to spur growth and development of the local data economy in Kenya.

Definition of Terms

Critical system: Any system whose 'failure' could threaten human life, national security or could cause huge economic losses. Such systems include but not limited to electric grid, manufacturing system, transportation system, financial institutions, water treatment facilities and water supply systems (Ministry of ICT Kenya, 2018).

Data controller: A person who either alone or jointly with other persons or in common with other persons or as a legal duty determines the purpose for and the manner in which data is processed or is to be processed (Ministry of ICT Kenya, 2018).

Data localization: An act of storing data on any device or a system that is physically present within the borders of a specific country where the data was generated (Technopedia, 2023).

Data processor: Refers to any person or entity (other than an employee of the data controller) that processes the personal data on behalf of the data controller (Ministry of ICT Kenya, 2018).

Data protection: Refers to implementation of appropriate administrative, technical, or physical means to guard against unauthorized intentional or accidental disclosure, modification, or destruction of data (Law Insider, 2023).

Data sovereignty: Refers to the jurisdictional control or legal authority that can be asserted over data because of its physical location is within jurisdictional boundaries (Macquarie Government, 2023).

Data subject: Means an identified or identifiable natural person who is the subject of personal data (Ministry of ICT Kenya, 2018).

Personal data: Means any information relating to an identified or identifiable individual (data subject) such as names, data of birth, location data, health data, among other data (OECD, 2015b).

Processing of personal data: Any operation performed on personal data, such as collecting, creating, recording, structuring, organizing, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data (Ministry of ICT Kenya, 2018).

Restriction of processing: The marking of stored personal data with an aim of limiting data processing in the future (Ministry of ICT Kenya, 2018).

Table of Contents

List of Tables and Figures

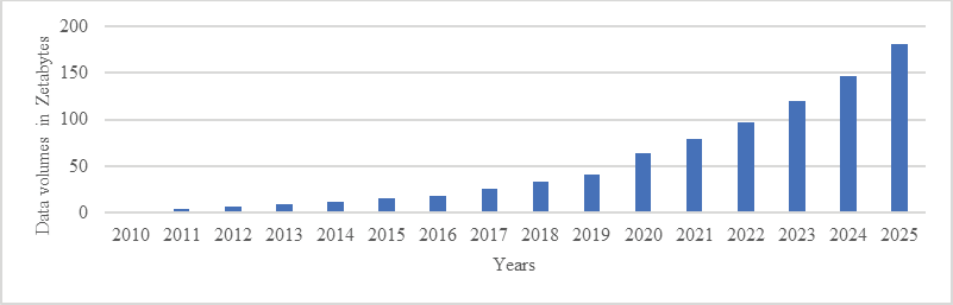
List of Figures

List of Tables

1. Introduction

The world is experiencing unprecedented growth in technological innovations, and this has significantly changed the traditional means of collecting, storing, analyzing, and sharing data. With increased digitization and digitalization supported by the development of the Internet, smartphones and mobile broadband and emerging technologies, countries have increased their capacity to generate and process data at a much higher rate (OECD, 2020). In today's digital economy era, data is an invaluable resource and lifeline supporting activities by government and business organizations. A United Nations quarterly report (United Nations, 2019) indicates that the digital age is producing a vast amount of data every second. Notably, devices and people actively share their data and leave behind rapid, real-time trails of data. Due to increased data-related activities supporting the digital economy, the amounts of data generated have exponentially increased in the last ten years as demonstrated through Figure 1.1. The world generates 2.5 quintillion bytes per day equivalent of 1,000 petabytes. About 90 per cent of the world's data was created in the last two years and every two years, the volume of data across the world nearly doubles in size. By 2025, global data creation is projected to grow to more than 180 zettabytes due to increased demand for data-driven activities. Further, it is expected that by 2030, nine (9) out of every ten (10) people aged six years and above will be digitally active (Vuleta, 2021).

Figure 1.1: Total amounts data generated globally



Source: Statistical (2022)

Personal data is one of the categories of data contributing to the highest size of data created, consumed, and stored globally (OECD, 2013). Personal data refers to any information relating to an identified or identifiable natural person such as name, email address, identification number and passport number (KenyaLaw, 2019). Due to its increased value, personal data is regarded as the new oil of the Internet and the new currency of the digital world (World Wide Web Foundation, 2017). Personal data is viewed as a social-economic asset generated by the identities and behaviours of individuals, and which is traded in exchange for higher quality services and products. For instance, businesses are using personal data to understand their consumers in designing customized products and

services (United Nations, 2019). Similarly, personal data facilitates government organizations in improving the efficacy of public policy, delivery of public services, transparency, and accountability. The increased value of personal data in the digital economy is driving rapid advances in technologies.

The adoption of mobile, Internet and other emerging technologies, including artificial intelligence and machine learning in organizations has impacted the capacity and pace of processing personal data. Consequently, the number of users interacting with digital platforms has significantly increased, thus generating huge volumes of personal data (OECD, 2020). Notably, various public and private organizations are increasingly relying on digital platforms supported by emerging technologies such as cloud computing and data analytics to process personal data in service delivery. For instance, public organizations use digital platforms for service delivery when issuing birth, death, and travel certificates to the public while private organizations rely on data such as names, addresses and billing information to monitor and support production, distribution and supply chain systems, marketing systems and workforce systems in real time.

While the use of personal data is yielding great social-economic benefits, the unregulated use and control of personal data brings new risks not only on breaching the privacy of individuals but also posing a national security threat (OECD, 2020). Personal data is increasingly used in ways that were not anticipated at the time of collection, with citizens not fully aware of how their personal data are captured, stored, used, and sometimes shared with third parties for various purposes. Various research studies indicate that organizations may use, share, or keep this data in unethical, illegal, or inappropriate ways and this may ultimately reveal consumers sensitive details such as names, date of birth, bank accounts, locations, income, race, ethnicity, religion, and health information. The IBM (2019) Security report indicates that the demand by data brokers for personal data held in foreign countries has driven up the value for personal data, and therefore posing a significant threat on personal data. Further, it is observed that the data broker business model involves accumulating personal data to build predictive models and profiles based on age, race, sex, weight, height, marital status, education level, politics, shopping habits, health issues and holiday plans and finally selling it for political campaigns and committing online frauds (Martin, 2020). Data brokers are known to collect information through foreign companies while data subjects are not aware and usually serve downstream firms who use the personal data in several ways, including targeted advertising, personalized pricing, product customization, and other marketing purposes (Gu, Madio and Reggiani, 2019). Interestingly, many data brokers often operate either on the brink of the law, or in countries without data localization policies or if present are not diligently enforced.

In the digitally disruptive age of the Internet involving the cross-border flow of personal data and unrestricted processing of personal data outside a given jurisdiction, various countries are reporting increased sovereignty concerns of their personal data (Deloitte, 2017). Internet provides an avenue that threatens lawful use of personal data, and this ultimately may compromise the sovereignty of a country and thus threaten national security and may cause economic harm (Banks,

2017). Since commercialization of the Internet in the early 1990s, governments around the world have struggled to address the wide range of privacy, business continuity and sovereignty challenges presented by the rapid growth of personal data and the borderless nature of the Internet (Hill, 2014). Edward Snowden and other intelligent sources have further revealed the presence of various foreign surveillance programmes that obtain information resident on or transiting through foreign-based systems and networks. Foreign surveillance and espionage involve State actors attempting to acquire secrets held by foreign governments, companies, and individuals (Banks, 2017). The act of foreign surveillance violates human rights based on the International Covenant on Civil and Political Rights (ICCPR) on Article 17(1). The mounting online theft of intellectual property, the growth of sophisticated malware and foreign surveillance, among other threats such as cyberwarfare, require the attention of governments to protect personal data and safeguard the national interests (Australian Government, 2017).

Evidently, there is growing interest among governments to control the processing of personal data (World Wide Web Foundation, 2017). Several governments around the world are now flexing their muscles and stepping up efforts to limit cross-border data flows to other jurisdictions with an aim of protecting personal data for privacy, business continuity, national security, and sovereignty reasons. Data localization is being embraced by less-developed countries to defend their national digital interests against aggressive surveillance by developed countries (Nigel, 2017). Digital localization is expected to continue gaining even more political currency in the years to come, given the broad deployment of highly invasive digital technologies ranging from artificial intelligence to the Internet of Things (IOT). Research studies observe a long history of disputes and conflicting policies regarding the transmission of information across national borders. In the beginning of the 21st century, some countries including China and Russia, started embracing the concept of data localization to control processing of personal data within their borders. Ever since, there is a steady global trend towards adopting data localization laws that require personal data to be processed within the geographic boundaries of its state of origin (Taylor, 2020). Nevertheless, countries have not been able to reach an international agreement on rules for cross-border data flows and, as a result, individual countries are enacting their data localization laws (Nigel, 2017). Data localization strives to limit the storage, movement, and processing of personal data in specific geographies and jurisdictions (Hill, 2014).

Debates around personal data and how to govern personal data have increased in the recent years as countries work to develop instruments to develop their local data economies (Azmeh, Foster and Rabuh, 2021). Research has shown that imposing restriction on processing of personal data within jurisdictions that personal data was collected from can significantly enhance data governance and, therefore, positively impact data localization. While data localization laws offer a quick way to build data sovereignty where governments gain control of personal data within their own borders, policy makers in developing countries are facing enormous challenges to gain control and protect personal data within their jurisdictions. The borderless nature of the Internet and widespread use of personal data has compounded the privacy and trust policy issues of personal

data. Generally, developing countries are poorly prepared to host local personal data due to challenges arising from inadequate infrastructure, limited human and technical skills and other capacity gaps, posing a challenge in realizing the benefits of data localization. Notably, developing countries have fewer local data centres due to the high cost associated in setting up such facilities and, therefore, may not effectively support the data localization policy initiative. The idea of restricting data flow may raise concerns, including acting as trading barriers with other countries in this era of digital economy.

Locally, the digital economy in Kenya continues to evolve at breakneck speed, driven by the ability to collect, use and analyze massive amounts of personal data. Kenya accounts for 7.7 per cent in the African Internet Economy based on e-Conomy Africa 2020 report (IFC, 2020). The report projects that Kenya's digital economy will account for 15.17 per cent in Africa by 2050. Because personal data is an ingredient for the digital economy, government and business organizations collect, use, and transfer personal data at an unprecedented scale and for multiple purposes. Notably, nearly every sector in the Kenyan economy, including the financial sector, processes personal data in foreign countries. As the size of personal data in the country grows, addressing the privacy, trust, business continuity and sovereignty concerns is of policy concern because of the unregulated and arbitrary use of personal data. To address this policy concern, the government recognizes the importance of protection of personal data and the right to privacy as stipulated in Article 31 of the Constitution of Kenya. Consequently, as an effort to further guarantee the same, Kenya has established policy, legal and regulatory frameworks to enforce the right to privacy and in particular protection of personal data. The Data Protection Policy, Data Protection Act of 2019, and the Data Protection Regulations of 2022 lay the foundations for data localization in Kenya.

Despite having relatively new legal and policy instruments for data localization in Kenya, there is need to assess the level of preparedness in the country and determine the key considerations in building data sovereignty for successful personal data governance in Kenya. With few to no research carried out in this relatively new policy arena in the country, Kenya is in dire need to address the growing privacy and sovereignty concern over personal data. The main objective of this study is to appraise policy efforts for safeguarding the personal data sector against increasing privacy and security-related threats with a goal of building data sovereignty in Kenya. The specific objectives of this study are to:

(i) Assess the current policy efforts towards data sovereignty in Kenya

(ii) Recommend a robust data governance policy framework for data sovereignty in Kenya based on the best practices and lessons

The study is guided by the OECD data governance pillars that include the strategic, tactical and delivery pillars to inform on the requirements for building data sovereignty for personal data in Kenya. The pillars consider the activities along the data value chain that includes roles, processes, and actors. The recommendations provided in this study will strengthen the control of processing of local personal data necessary for enhancing the privacy, continuity of services,

national security and encouraging the emergence of domestic digital firms and ultimately accelerating the digital economy in the country.

Section 2 reviews related work on data localization, data sovereignty and data governance. Section 3 outlines the methodology adopted by the study. Section 4 provides analysis of relevant policy initiatives for personal data based on the data governance pillars and global trends and lessons for data localization in Kenya. Finally, section 5 provides conclusions and policy recommendations.

2. Literature Review

2.1 Introduction

This section provides an overview of the research works that were systematically reviewed in support of the study. First, the section gives a solid introduction of theoretical foundation on data governance and privacy of data. The section further provides literature on nexus between personal data and data sovereignty.

2.2 Data Governance framework

Data governance is the combination of processes, policies, standards, technologies, and systems that work together to ensure data is accurate, usable, secure, easy-to-understand, high-quality, integrated and preserved. Data owners use data governance to safeguard their data, control who has access and who is responsible for owning and managing it. According to Micheli et al. (2020), the dominant model of personal data is mainly characterized by the asymmetry of power of a few technology corporations and telecommunication companies that have established monopolies that contribute to biases in algorithmic decision-making, nudging and manipulation, and privacy violations.

Generally, global companies collect huge amounts of personal data from various countries, which is later transferred and stored in a few data centres, allowing a few countries to impose surveillance laws (Lee, 2014). Therefore, countries that host such data centres have more influence over personal data stored in their countries. Similarly, governments hosting data centres may have privileged position to abuse their Internet infrastructure leading to data breaches or surveillance of other countries. China has claimed that personal data stored in foreign countries is prone to foreign surveillance and espionage. Similarly, Russia has accused the United States of America and its allies of exploiting their dominant position in Internet infrastructure for geopolitical and economic objectives, including cybertheft (Mueller, 2010).

As data becomes essential to economic growth, data governance has become critical to policy makers. Because of the increasing importance of data localization, governments are seeking to regulate commercial use of personal data. Such countries strongly believe that the right to control the collection, ownership, and application of citizens' data should rest with national policy makers (Aaronson, 2021). The author argues that the best way to protect citizens' data while encouraging data-driven development is to ensure that data resides in local servers, under domestically determined rules, and the control of national authorities. An effective data governance model should support massive collection, use and sharing of personal data among multiple actors, such as small businesses, public bodies, and civic society. Micheli et al. (2020) define data governance as an evolving ecosystem with a plurality of actors having multiple interests, agendas, goals, and strategies, and interacting with an array of tools, mechanisms, systems, interfaces, and devices for governing data. Micheli et al. (2020) note that a personal data ecosystem should reflect on how data subjects

are governed, and how they can intervene in the data regimes by recognizing and claiming their rights and being active in the politics of data with their everyday acts. The authors identified four data governance models, namely: data sharing pools (DSPs), data cooperatives (DCs), public data trusts (PDTs) and personal data sovereignty (PDS) as illustrated in Table 2.1.

Table 2.1: Data governance models

Type of model	Description
Data Sharing Pools (DSPs)	Data is treated and exchanged as a market commodity to produce data-driven innovations, new services, and economic benefits for all the parties involved. DSPs are horizontal joint initiatives among data holders to aggregate data from different sources to create more value through their combination. Governance mechanisms for DSPs include technical architectures, such as data sharing platforms and Application Programming Interfaces (APIs), which facilitate a centralized data exchange in business ecosystems. A key mechanism is the contract, a legal and policy framework, that defines the modalities for data sharing and how data can be handled and data purposes.
Data Cooperatives (DCs)	DCs distribute data access/rights among actors providing higher involvement of data subjects guided by different goals. DCs enable a de-centralized data governance approach in which data subjects voluntarily pool their data together to create a common pool for mutual benefits. Participants of DCs share data while retaining control over it, having a say on how it is managed and put to value, and not submitting to the extractive logic of digital capitalism.

Public Data Trusts (PDTs)	PDTs refer to a model of data governance in which a public actor accesses, aggregates and uses data about its citizens, including data held by commercial entities, with which it establishes a relationship of trust. Several stakeholders might be involved in this model, including city administrators, managers of public institutions, platform companies, trusted data intermediaries, research institutions, start-ups, and SMEs. Public administrations may also invite third parties to access their data sources and develop data-driven services and/or to offer guidance on data sharing. A key goal of PDTs is to integrate data from multiple sources to inform policy making, promote innovation and address societal challenges, while adopting a responsible approach to the use of personal data. In PDTs, public actors assume the role of trustees that guarantee citizens' data is handled ethically, privately, and securely.
Personal Data Sovereignty (PDS)	The PDS model is characterized by data subjects that have greater control on their data, both in terms of privacy management and data portability. The model comes from the broader principle of technological sovereignty, which concerns subjects, public administrations, or governments regaining control of technology, digital content, and infrastructures, thus reducing the influence of IT commercial enterprises and of foreign States in which these companies reside. This model promotes a different and fairer data economy, echoing critical accounts of the dominant model of surveillance capitalism. Data subjects are envisioned as key stakeholders, together with digital service providers – which deliver the means for subjects to control, use and share their data – and re-users with whom data subjects decide to share their data. This governance model pursues two goals: it increases individuals' self-determination, granting more opportunities to access, share and use personal data, and engendering a more balanced relationship between users and digital platforms; and it is expected to foster a socially beneficial usage of data through the development of new data-driven services centred on user needs.

Source: Micheli et al. (2020)

2.3 Privacy Framework

Security and Privacy Capability Maturity Model (SP-CMM) is one of the popular frameworks to enhance privacy of personal data. SP-CMM was developed by the Secure Controls Framework Council (Secure Controls Framework, 2022) to guide organizations in the establishment and evaluation of their security and privacy controls, and it has three primary objectives:

- Provide chief level executives with a well-defined criterion for setting the expectations for an organization's cybersecurity and privacy programme;
- Provide internal security teams with a well-defined criterion for planning and implementing security practices; and
- Provide a baseline criterion for organizations to evaluate third-party service providers.

The model follows a nested approach, such that every succeeding level of maturity builds on its predecessor. It has a total of six levels that are represented from CMM0 to CMM5 as shown in Table 2.2.

Table 2.2: Levels of security and privacy capability maturity model

Level	Description
CMM0: Not performed	This maturity corresponds to non-existent practices in an organization. This means that the organization is not performing the relevant control or process, and thus no identifiable work products of the process.
CMM1: Performed informally	This maturity level corresponds to ad-hoc practices. The organization is performing the relevant controls, but they are inconsistent or incomplete. This level is associated with: • Base practices of the process area are generally performed • The performance of these base practices may not be rigorously planned and tracked • Performance depends on individual knowledge and effort • There are identifiable work products for the process

CMM2: Planned and tracked	This level of maturity is defined as "requirements-driven practices", where the expectations for controls are known (e.g., statutory, regulatory, or contractual compliance obligations) and practices are tailored to meet those specific requirements. This level is associated with: • Performance of the base practices in the process area is planned and tracked • Performance according to specified procedures is verified • Work products conform to specified standards and requirements CMM 2 focuses more on compliance than security. The performance is verified by the designated individual, and the given requirements are fulfilled.
CMM3: Well-defined	At this maturity level, the organization has enterprise-wide standards with well-defined processes. There is a standard documentation process in place that came into effect after approval. All such processes are planned and managed with a well-defined process. CMM3 practices focus more on organization-wide standards, unlike CMM2. This maturity level anchors the implementation of security practices, instead of merely fulfilling compliance obligations. Organizations at this maturity level generally have smaller security teams led by a competent security manager/director. Larger organizations at this maturity level may have dedicated specialists for security operations, risk management and privacy.

CMM4: Quantitatively controlled	This level of maturity is defined as "metrics-driven practices," where in addition to being well-defined and standardized practices across the organization, there are detailed metrics to enable governance oversight. This level entails: • Detailed measures of performance are collected and analyzed. This leads to a quantitative understanding of process capability and an improved ability to predict performance. • Performance is objectively managed, and the quality of work products is quantitatively known. CMM4 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control, and detailed metrics enable an objective oversight function. Metrics may be daily, weekly, monthly, or quarterly. For smaller organizations, it is unrealistic to achieve this level of maturity. For larger organizations, there is a C-level executive who leads the organization's security programme, and the top management is informed about cybersecurity status at regular intervals.

CMM5: Continuously improving	The highest level of maturity is analogous to having world-class security practices. Along with having standard processes and metrics about process execution, processes continuously improve at this maturity level. An organization sets a clear target for process effectiveness, in line with their business goals. There exists a continuous improvement process that incorporates previous experience, ideas, technologies, and quantitative feedback. In some cases, an organization may use artificial intelligence-based tools to improve their processes and procedures. For small and medium scale enterprises, it would be unrealistic to achieve CMM5.

Source: Secure Controls Framework (2022)

2.4 Necessity for Data Sovereignty in Personal Data Economy

The term sovereignty is derived from the Latin word superanus, which means "over" or "superior" (Taylor, 2020). Sovereignty is a political concept of the power enjoyed by a governing body to rule over itself, free from any interference by outside sources or bodies (Pohle and Thiel, 2020). Sovereignty refers to a State's supreme authority within a territory and over its population and it is commonly agreed that every State exercises sovereignty over digital networks and cross-border communications within its territory (Taylor, 2020). Some states also lay claim to extra-territorial extensions of such sovereignty through subpoenas, national privacy laws, and/or national security rationales (Turner, 1997). Studies show that sovereign power across many countries covers all communications modalities and are regarded as critical state mechanisms and thus require it to be licensed, regulated, and closely supervised for political, security and economic reasons. Communication sovereignty by different nations can be traced back to the beginnings of cross-border telegraphy. For instance, governments codified mutually exclusive control of their respective national telegraph networks and to limit international regimes to just the connections between them.

According to Taylor (2020), the principle of internal national communication sovereignty is universal, and should be embodied in the domestic laws of countries. However, the modern digital transformation due to development of the Internet presents a challenge to sovereignty. The cross-border nature of data transfer seems to defy the principles of territoriality and State hierarchy. The ever-growing nature of digital network and digital applications and communication practices have significantly reduced the legal governance and control by governments (Pohle

and Thiel, 2020). To counter these potential risks to their authority, countries are enforcing national laws and undertaking governmental interventions in the digital sphere.

Further, there are several examples where some countries extend sovereign access to, and control of, personal data beyond their national borders. This raises sensitive questions of jurisdiction, access, and control by some countries over other countries. This has accelerated the trend of several countries whose sovereignty is threatened to adopt data localization. For instance, the USA Patriot Act allows law enforcement to conduct electronic surveillance and communication interception to investigate many ordinary and non-terrorism crimes such as drug crimes, mail fraud, and passport fraud beyond the American physical boundary (Department of Justice, 2021). PRISM project, a surveillance programme, allows the United States' National Security Agency (NSA) to collect Internet communications from various US Internet companies (Wikipedia, 2021). Similarly, the Cloud Act of USA primarily allows service providers to disclose all data in their possession, custody, or control, pursuant to lawful process, regardless of the location of the data (Wu, 2021). Other laws that allow for surveillance and interception of communication beyond physical boundaries include the United Kingdom's "TEMPORA" project.

With the presence of various foreign surveillance programmes and revelations of top secrets by Snowden, many governments are aware of the need to control how their personal data is processed. Snowden revealed various surveillance programmes and tools used to gather and analyze personal data by intelligence agencies and tech companies in the United States and other Western countries (Sargsyan, 2016). For instance, there are policy concerns that demonstrate that the global technology companies such as Microsoft, Google and Apple agreed to compromise encryption standards and allow backdoor access to data, subjecting global users' privacy to unwarranted surveillance (Ball, 2013; Greenwald, 2014; and Greenwald and MacAskill, 2013).

According to Banks (2017), the traditional State-sponsored surveillance and espionage have been transformed into high-tech and high-stakes enterprises. The electronic surveillance is carried out for foreign intelligence purposes to uncover patterns of terrorist attacks, learning about the foreign policy plans of adversaries, and gaining advantage in foreign relations negotiations. Generally, surveillance operations encompass four elements that include gathering, analysis, verification, and dissemination of information of relevance to the decision-making process of a State. Surveillance is undertaken with secrecy and without consent of countries being spied on (UNODC, 2020). It is observed that governments and their agents have been exploiting Internet connectivity by penetrating the electronic networks of foreign companies for nearly a quarter century. According to Banks (2017), cyberspace remains a netherworld for intelligence activities that include surveillance, cyber spying by governments or other agencies and usually go beyond their national borders. Usually, surveillance and espionage may be conducted across borders and may involve perpetrators collecting the contents of electronic communications or metadata about them; watching government computer systems through cyber penetration; exfiltration of government data, including military or other national security secrets; malware distribution, social engineering

and denial of service penetrations that decrease the bandwidth for government websites. These cyber espionage perpetrators intentionally or unintentionally disclose confidential or sensitive information to countries or others linked in some way to foreign countries as part of their intelligence collection efforts (UNODC, 2020). Countries that have advanced Internet infrastructure are likely to carry out surveillance and espionage on other countries relying on such infrastructure (Banks, 2017).

Several accusations on foreign surveillance and espionage are made by countries and global companies. For instance, in 2010, Google claimed that China had stolen source code and used it to spy and to penetrate other companies' networks (Jacobs and Helft, 2010). Some global technology companies, including the Internet Service Providers (ISPs) tend to disregard the security and privacy of customers data and sell the browsing habits of their customers to third parties, including data brokers (Thielman, 2017). Further, various governments such as China, North Korea, Russia, Australia, and Iran have recruited young tech savvy persons with the goal of establishing cyber armies to protect their interests locally and in foreign countries.

The concept of data sovereignty, also known as data residency, has become a powerful term in political discourse that seeks to reinstate the sovereignty over the use of data in supporting social and economic activities. Data sovereignty is the idea that data, including personal information, is subject to the laws and governance structures of the nation within which it is collected. In a world where access to data is essential for the development of a local data economy but concerns are emerging around data breaches and cybersecurity, countries are increasingly demonstrating an appetite to secure local access to data and restrict international transfers of data. Data sovereignty is perceived as a gap-filling claim for authority and control over information assets, which would compensate for the progressive national disenfranchisement from virtualization in extraterritorial data processing (Taylor, 2020). According to Taylor (2020), data sovereignty is a concept being embraced by less-developed countries to defend their national digital interests against more developed countries. Less developed countries fear the efforts of promoting the free flow of information because it is a likely threat to their sovereignty due to heavy dominance of the US and its allies on Internet governance (Aaronson, 2015).

2.5 Adoption of Data Localization Measures to Data Sovereignty

According to Wu (2021), there are three forms of data localization. The first category means an obligation to locally manage data or a prohibition of international data transfer. This is the strictest type of localization policy and is more likely to be descriptive of nations seeking broader control over citizen activities. The second category requires companies to keep a copy of data in local servers or data centres. This allows for easier access to this data for regulation and law enforcement purposes. It is generally easier for local law enforcement agencies to access data stored locally than accessing data stored in another jurisdiction. The final category

specifies conditions of transfers of data outside a country and, therefore, such data transfers are only permitted if certain conditions are met by the transferee and/or by the recipient country. Other forms of data localization include defining the time and locations for storing data, requiring companies to relocate or build data centres in specific locations, requiring the local purchasing of digital equipment for government and private sector procurements, or mandatory local ownership of data storage equipment, limitations on foreign online retailers, and forced local hiring.

Data localization is a critical component for sovereignty towards building the national defense of a country. Data localization requires data to be stored and processed domestically, with the aim of enhancing sovereign control over citizens' data (Wu, 2021). Data localization laws are primarily driven by concerns about foreign government interference on data stored outside of their jurisdiction. Data localization laws can be broadly classified under data sovereignty (Taylor, 2020). The goal of these laws is to move data away from the geographically borderless world of cyberspace and plant such data directly under local jurisdictions. Countries are adopting data localization measures to restrict the storage, movement, and processing of data to specific areas and jurisdictions to enhance national security (Pohle and Thiel, 2020). According to Taylor (2020), the ability to wall off one's domestic Internet is believed to be a defense of its cyber assets. Several governments around the world wish to maintain the highest level of control over national data for domestic control to maintain political, social, and economic control of the State. The concept of digital sovereignty has become a central element in policy discourses on digital issues for centralized, authoritarian, and democratic countries alike (Pohle and Thiel, 2020).

Various actors have started to proclaim the need to establish sovereignty in the digital realm. The demand for national data sovereignty over personal data is invoked by actors who highlight the risks of foreign surveillance and national security (Pohle and Thiel, 2020). Some countries believe that they can offer better protection to their national data, including personal data by controlling its access, transmission, and use (Taylor, 2020). Several countries and in particular Brazil, Russia, India, China, and South Africa (BRICS), representing large percentages of the world's population, are supporting data localization policies. Further, some liberal democracies appear to embrace data sovereignty. For instance, in July 2020, the German government, in its official programme for its presidency of the European Council, announced its intention to establish data sovereignty. Similarly, the United Kingdom has begun to advocate for democratic governments doing more to confront cybersecurity threats. India, Japan, the European Union, and the United States are all considering how to effectively govern data flows (Taylor, 2020). Data sovereignty is expected to continue gaining even more political currency in the years to come, given the broad deployment of highly invasive digital technologies ranging from artificial intelligence to the Internet of Things.

Data localization is perceived as a symbolic assertion of national power and a rejection of "data colonialism" in support of indigenous principles and traditions (Taylor, 2020). Data localization offers an opportunity to protect national data of all kinds, related to national security, governmental functions, financial

functions, business and civil society, and personal data on citizens. When data is stored outside their borders, governments are not able to easily enforce data protection laws to enhance privacy and security of personal data without relying on intermediary companies' infrastructure. Similarly, data localization policies are also perceived to provide a "safe space" for the development of domestic digital businesses. Sargsyan (2016) studied data localization cases that store data on local servers and observed that the data localization regulations grant governments more jurisdictional control over personal data, and governments can increase their effectiveness of law enforcement. Other similar studies that cited national security as the main reason for adopting data localization laws are Deibert (2013), DeNardis (2014) and Fuchs (2010).

Sargsyan (2016) further observes that governments are increasingly recognizing the importance of critical infrastructure for processing personal data for national security, public safety, and other national strategic interests. To fulfil the national security goal, governments across the globe are keen in limiting the processing of personal data. Because of national security-related reasons, governments across the globe are prioritizing to develop their own infrastructure and invest in data localization initiatives to locally process personal data. According to Sargsyan (2016), data localization commonly encapsulates requirements that data be physically stored within a country's jurisdiction and/or not to be transferred abroad.

3. Methodology

3.1 Introduction

This section describes the methodology adopted to undertake this research study. The section provides details of study conceptualization, analytical framework, data, and data sources consulted in the study. The study relied heavily on secondary data from relevant sources.

3.2 Study Conceptualization

Globally, the privacy of personal data is an important focus area in the digital and intelligent economies (Acquisti and College, 2010). Technology facilitates the collection, storage, processing, and sharing of personal data. It reduces the cost of processing data, thus making it possible to capture, store and analyze data about individuals. Government and business organizations have invested in data processing tools, including websites and data aggregators, to collect personal data from multiple sources to create consumer profiles in this knowledge-based market (Acquisti and College, 2010). Further, Symons (2022) notes that most of today's data is controlled by a handful of global monopolies, a fact that makes governments and citizens where data was collected, and the developing countries lose control of their data and its privacy and autonomy.

As more organizations embrace digital technologies to process personal data, privacy and sovereignty concerns grow as well. Acquisti and College (2010) observe that hundreds of millions of individual data worldwide is collected and shared with advertising companies without the data subjects' consent. Despite the significant benefits that arise from the ability of organizations to easily share data across borders for various reasons, personal data could be exposed to various threats that carryout data breaches, online theft of intellectual properties, surveillance, and foreign surveillance. Individuals and organizations are facing a complex issue of balancing protection and sharing of personal data. For instance, individuals prefer security of their data while organizations want to understand their clients by tracking their transactions to offer personalized services. Personal data is therefore a critical asset that some countries often fail to govern, manage, and value in the same way other national assets are treated.

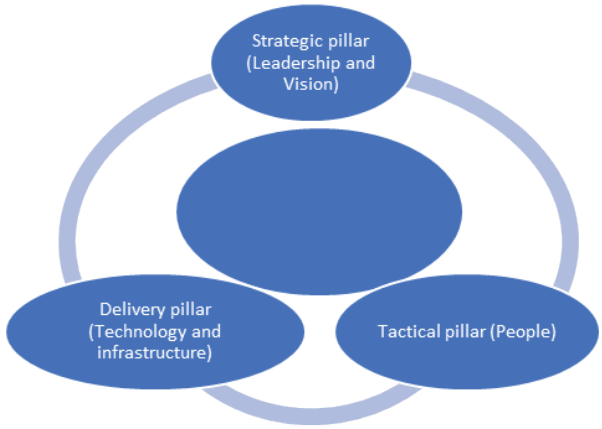
In recent years, personal data protection is a growing topical policy concern around the globe as countries seek to regulate collection, storage and processing personal data that is happening on an unprecedented scale. Countries are putting in place policy measures to restrict transfer of certain local personal data to other countries with a goal of gaining control over their local data and to encourage the emergence of domestic digital firms. Due to privacy, business and sovereignty concerns involving cross border processing of personal data, Kenya has recently put in place data localization instruments. To effectively respond to these policy challenges, Kenya requires a comprehensive assessment of personal data initiatives in relation to its data governance. Symons (2022) recommends investment in data

localization as a long-lasting solution to empower and gain control in processing of personal data within their jurisdictions for a thriving personal data economy.

3.3 Data Governance Pillars and Elements for Data Localization

Good data governance is synonymous with effective data localization that ultimately builds data sovereignty, promotes integration and systemic coherence in data management, and offers a robust foundation to enhance privacy and trust for personal data. An effective data governance model is a cornerstone for data-driven economy and consists of policies; people; and infrastructure and technology. These aspects can further be interpreted in terms of the following elements: Data strategy, policies, and laws; Data processes; Data standards; Data quality; Data security; Data literacy; Communication and collaboration; and Data technology. The OECD (2022) identifies a comprehensive analytical framework to build a strong foundation for data governance for data sovereignty that comprises of three pillars: Strategic pillar; Tactic pillar; and Delivery pillar as shown in Figure 3.1.

Figure 3.1: Building blocks for data sovereignty



Source: OECD (2022)

On the strategic pillar, leadership and vision are key in providing policy direction for data localization. The key data governance elements in this layer considered in the analysis include: Supervisory authority; Supporting resources (budget and staff); Data standards; Data architecture; Data quality; Data security; Data storage; and Data sharing. The conceptualization of this pillar supports the identification of strategic policy gaps that require to be addressed to build effective data sovereignty in Kenya.

The conceptualization was also guided by the requirements in the second layer, the Tactical layer, which defines the required human capacities for coherent

implementation of the data governance framework. The tactical layer enables the coherent implementation and steering of laws, regulations, data-driven policies, strategies, and related initiatives. The key aspects of this pillar include Training institutions; Human resources and support to skills development; and job opportunities.

Finally, the conceptualization reflected on the Delivery layer focused on technical requirements, reflected by Data generation and collection systems; Internet infrastructure; Cellular infrastructure or mobile network; Data centre; Spatial infrastructure; and Cybersecurity initiatives. The delivery layer allows for the day-to-day implementation (or deployment) of organizational, sectoral, national, or cross-border data localization policy direction. It covers different technical aspects of the data value cycle across its different stages (from data generation, processes, and storage), the role and interaction of different actors in each stage (such as infrastructure service providers, data producers, data providers and data processors), and the inter-connection of data flows across stages. The analysis of the requirements under this pillar is key in assessing the technical solutions that require to be re-engineered, retrofitted and customized to support effective implementation of data localization.

Table 3.1: Data governance policy elements

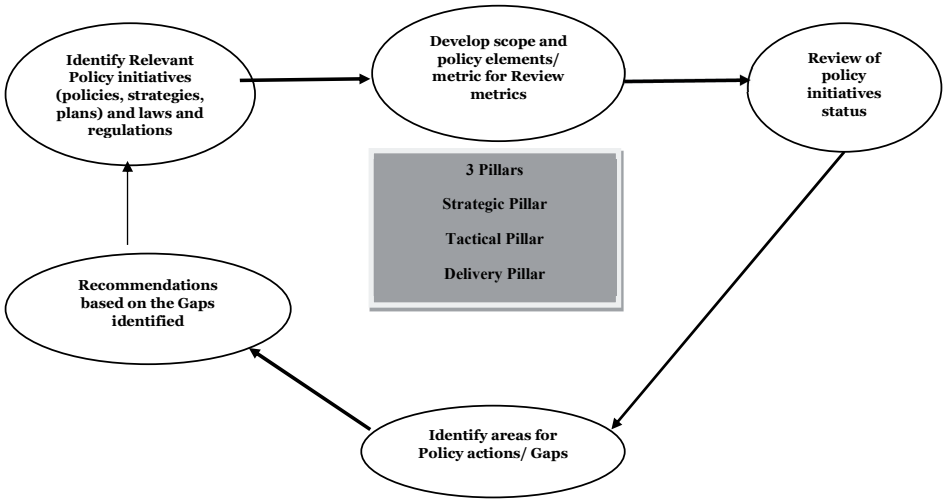
Pillar	Policy Element	Description
Strategic pillar	Supervisory authority	An independent public authority established by the State to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance
	Supporting resources (budget and staff)	Provision of essential resources including budget and staff to carry out strategic goals
	Data standards	Documented agreements on representation, format, definition, structuring, tagging, transmission, manipulation, use and management of data
	Data architecture	Blueprint that shows flow of data through systems. It describes the structure of logical and physical data assets and data management resources
	Data quality	Measures indicating how well a dataset meets criteria for accuracy, completeness, validity, consistency, uniqueness, timeliness, and fitness for purpose
	Data security	Practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire life cycle
	Data storage	Retention of information/data using technology specifically developed to keep that data and have it as accessible as necessary
	Data sharing	Practice of making data available for use in decision making, research or any other purposes
Tactic pillar	Training institutions	The available training institutions such as universities offering data protection-related programmes
	Human resources and support to skills development	The available human resources to undertake data protection related tasks. It also entails provision of facilitation to develop skills for data protection related tasks
	Job opportunities	Availability of jobs for trained graduates/ personnel in getting jobs

Delivery pillar	Data generation and collection systems	Systems to generate and collect personal data
	Internet infrastructure	Refers to the physical hardware, transmission, media, and software used to interconnect computers and users on the Internet. Internet infrastructure provides hosting, storage, processing and sharing of information
	Cellular infrastructure or mobile network	A telecommunication network where the link to and from end nodes is wireless and the network is distributed over land areas called cells
	Data centre	Facility that provides shared access to applications and data using a complex network, computer, and storage infrastructure
	Spatial infrastructure	It is a geospatial data infrastructure that implements a framework of geographic data, metadata, users, and tools that are interactively connected to use spatial data in an efficient and flexible way
	Cybersecurity initiatives	Policy efforts to protect, detect, respond, and recover from cyber-attacks including Computer Emergency Response Team, National Public Key Infrastructure (NPKI)

3.4 Analytical Framework

To answer the objectives of this study, the analysis considered the requirements of the three pillars while reflecting on the activities along the data value chain, such as data generation, data storage, data processing, data sharing and data applications (Azmeh, Foster and Rabuh, 2021). Guided by the requirements spelt out in the three pillars, the study reviewed the existing policies, laws, regulations, strategies, and guidelines to identify the achievements and gaps in building sovereignty in Kenya as shown in Figure 3.1. The study first identified the existing policies, laws, regulations, strategies, and guidelines on data sovereignty based on the three pillars. Kenya was compared against three countries, namely Uganda and Nigeria that served as comparator, while Australia served as comparator due to its robust personal data sector. The metrics listed in Table 3.1 served as the basis of comparison. The study provides recommendations based on the gaps identified. Figure 3.2 outlines the policy review framework adopted in the study.

Figure 3.2: Policy review framework



Source: Author's conceptualization

This study reviewed various secondary sources of information both at the local and global levels to understand the subject field of data sovereignty of personal data. Some of the key local policies and legal documents included Data Protection Act and Policy, and General data protection regulations. The study heavily relied on published reports from key institutions such as the Central Bank of Kenya, Kenya National Bureau of Statistics, Communications Authority of Kenya, Ministry of Information Communication and Digital Economy, World Bank, and International Telecommunication Union. Other local key reports included Economic Survey reports, National Digital Masterplan, Micro and Small Enterprises Survey, Communications Authority's quarterly reports, among other digital economy reports to understand the personal data landscape in Kenya. Key global reports such as Global Cybersecurity Index of 2020, UN E-Government Survey of 2020 and Symantec report 2020 were systematically reviewed to understand the current trends of privacy threats facing personal data. Further, this study explored data drawn from countries that have adopted data localization laws with an objective of tapping their experiences, lessons, and emerging opportunities in building data sovereignty.

4. Key Findings and Discussion

4.1 Introduction

This section describes the key findings and discussions guided by OECD's data governance pillars that include– Strategic, Tactical and Delivery pillars.

4.2 Strategic Pillar

This study has reviewed various elements in the strategic pillar that support leadership and vision to implement data sovereignty in Kenya. The key elements considered in the analysis under this pillar include establishment of Supervisory authority; Supporting resources (budget and staff); Data standards; Data architecture; Data quality; Data security; Data storage; and Data sharing elements. The study compares Kenya with other countries along the elements of the strategic pillar.

4.2.1 Establishment of Supervisory Authority

A review of the policy initiatives in Kenya indicates a positive effort towards defining a robust leadership and vision to implement data localization for personal data. To protect and mitigate threats such as privacy and sovereignty-related policy issues against personal data while harnessing the benefits of the digital economy, Kenya has made significant progress in fulfilling the requirements of the strategic pillar. Kenya is among the early countries in Africa to put in place a policy and legal framework for data protection. Notably, Kenya formulated a policy and legal framework that includes the Data Protection Policy of 2018 and Data Protection Act of 2019. The aim of the Policy and Act is to protect and safeguard personal data against any possible misuse, abuse, or breach. Both the Policy and Act lay the foundation of preserving privacy towards enforcing Article 31 of the Constitution of Kenya. The fundamental principles of the Policy and Act are largely informed by global practices and the need to bridge the gaps that exist in contextualizing privacy and data protection in a technological environment in Kenya.

Like other developed data economies, having an independent public authority is key in monitoring the application of data protection laws to protect the fundamental rights and freedoms of persons in relation to processing and facilitation of the free flow of personal data. Kenya's data protection policy and legal framework has established a supervisory authority to oversee all aspects of personal data. The Authority, known as the Office of the Data Protection Commissioner (ODPC), is an independent office mandated to ensure compliance to the Data Protection Policy and law. Specifically, ODPC regulates the processing of personal data; ensures that the processing of personal data of a data subject is guided by the data protection principles set; protects the privacy of individuals; establishes the legal and institutional mechanism to protect personal data; and provides data subjects with

rights and remedies to protect their personal data. The ODPC works closely with all entities processing personal data, including both public and private entities. To facilitate effective processing of personal data, institutional, administrative interventions and legal frameworks have been established, including the civil registrations and identity management with a focus on personal data.

4.2.2 Supporting resources (budget and staff)

As highlighted earlier, Kenya's Data Protection Act establishes the Office of the Data Protection Commissioner. The first Data Protection Commissioner was appointed in 2020 to serve a period of six years. The ODPC has four directorates, namely: Corporate Services Directorate; Data Protection Compliance Directorate; Complaints, Investigations and Enforcement Directorate; and Research, Policy and Strategy Directorate. The ODPC is in its formative stages in regulating personal data in Kenya as compared to some well-established authorities in countries such as China. The ODPC has a total establishment of ninety-two (92) staff comprising 57 officers for technical services cadres and 35 officers in the support services cadre (Office of the Data Protection Commissioner , 2021). Given its broad mandate, the ODPC has established 6 regional offices (Nyeri, Garissa, Eldoret, Kisumu, Mombasa and Nakuru) with a plan to open 10 more regional offices to serve both the public and private sectors, including all non-State actors. The ODPC has a budget allocation of Ksh 270 million based on budget figures for 2023.

4.2.3 Data standards

Development of standards for data processing is critical in supporting the maturity of the local data economy. Standards provide guidelines for data processing activities including creation, storage, and distribution of personal data. Kenya has put in place various policy initiatives to promote the development and enforcement of standards for the personal data economy. For instance, the ICT Authority, a public agency established in 2013 with a mandate of ICT standards, has developed the Government Enterprise Architecture Framework for Ministries, Counties and Agencies. The framework builds a blueprint for improving management of data and aligning Government's business processes, information flows, and technology consistently across and throughout the Government. The framework provides guidance on Enterprise Architecture Principles (EAP); Information/data architecture principles; Application Architecture Principles (AAP); Technology Architecture Principles (TAP); Security Architecture Principles (SAP); and Integration Architect Principles. Further, the Authority has formulated various ICT standards for public entities, including the following: Cloud Computing Standard; Data Centre Standard; Electronic Records and Data Management Standard; End-User Equipment Standard; ICT Human Capital and Workforce Development Standard; Information Security Standard; IT Governance Standard; ICT Network Standard; and Systems and Applications Standard. However, compliance levels

to the standards are low due to inadequate enforcement officers and low budget allocation to ensure enforcement.

4.2.4 Data architecture

Data architecture is the blueprint that shows the flow of data through systems. It describes the structure of logical and physical data assets and data management resources. Kenya established the Kenya Open Data Initiative (KODI) in 2011 to make data freely available in easy reusable formats by the public through a single online portal. This initiative is in support of the Government's drive to consistently inform and be accountable to its citizens. While the National and County Governments are encouraged to provide their developmental, demographic, statistical and expenditure data to various stakeholders and the public, the initiative has faced several challenges. For instance, the portal lacks up to date data because most government agencies are not willing to share their data in the portal. To help institutions to open and share their datasets, the KODI Initiative is placing data fellows who are experienced in data mining and presentation in institutions that include the Office of the Auditor General, Agriculture and Food Authority, Kenya Forest Service, Posta Kenya, and State Department for Housing and Urban Development, and in counties including in Kiambu, Kisumu, Nakuru and Embu County Governments (ICTA, 2021).

4.2.5 Data quality

Data quality measures how well a dataset meets the criteria for accuracy, completeness, validity, consistency, uniqueness, timeliness, and fitness for purpose. This policy element is not comprehensively incorporated in policies in Kenya. The Kenya Data Protection Policy has identified accuracy of personal data as one of its principles. The policy states that personal data must be correct, complete, and be kept up to date. However, Kenya does not have a comprehensive data quality management framework.

4.2.6 Data Security

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire life cycle. The Data Protection Act requires personal data to be collected and used fairly, stored securely and not disclosed to any other person unlawfully. Like other legal frameworks such as the Global Data Protection Regulation for the European region, Kenya's Data Protection Act defines two key categories of personal data: Personal data and Sensitive personal data as illustrated in Table 4.1

Table 4.1: Categories of personal data in Kenya

Categories of personal data	Description
Personal Data	Any information relating to an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly by reference to an identification number, passport number, birth certificate or to one or more specific factors such as physical or physiological
Sensitive Personal Data	Any data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the data subject

Source: Data Protection Act (2019)

Kenya's data protection policy and legal framework recognizes the need to protect personal data processed outside of the country, popularly known as cross border data flow of personal data. To this end, the Office of the Data Protection Commissioner has developed three sets of regulations in 2021 to further guide the operationalization and implementation of the Act, and in particular on the type of data to be restricted for cross border data transfer, among many other provisions, to protect personal data (Government of Kenya, 2021). Specifically, the Data Protection (General) Regulations of 2021 outline the requirements to be met prior to transfer of personal data outside the country. The key requirements include contractual agreements, obtaining of consent and countries meeting the adequate safeguards spelt out by the regulations. A summary of the regulations is provided in Table 4.2.

Table 4.2: Summary of data protection regulations of 2021

Name of regulation	Description of regulation
The Data Protection (General) Regulations of 2021	This set of regulations outlines the rights of data subjects that include right to object processing of personal data, right to be forgotten, right to data portability, right to rectification of personal data and right to data access. The regulations provide guidance on restrictions on the commercial use of personal data, obligations of data controllers and data processors and notification of data breaches. Further, the regulations provide guidance on the transfer of personal data outside Kenya, including rooting for data localization. Finally, the regulations guide on how to conduct data protection impact assessment.
The Data Protection (Complaints Handling Procedure and Enforcement) Regulations of 2021	This set of regulations facilitate fair, impartial, just, expeditious, proportionate, and affordable determination of complaints lodged with the Office of Data Protection Commissioner. The regulations provide for issuance of enforcement notices as guided by section 58 of the Data Protection Act. Further, the regulation provides for issuance of penalty notices guided by section 62 of the Data Protection Act. Finally, the regulations provide for procedures for hearing and determining of complaints and provide grounds for resolutions of complaints lodged with the Office of Data Protection Commissioner by means of alternative dispute resolution

The Data Protection (Registration of Data Controllers and Data Processors) Regulations of 2021	This set of regulations defines the requirements for registration by data controllers and processors as guided by section 18 of the Data Protection Act. The regulations spell out the registration process, payment of registration fees by public and private agencies, certificate of registration. The regulations guide on the renewal of registration, conditions for approval or declining registration and renewal of certificate. Further, the regulations provide guidance on exemptions from the mandatory registration, procedures for electronic registration and offences.

Source: Data Protection Regulations (2021)

Other policy initiatives on data security include: Kenya Information and Communication Act, which was enacted in 1998 to facilitate the development of the ICT sector and the digital economy. The Act has been repealed several times to accommodate the evolving nature of the ICT sector, including the revisions done in 2012, later in 2013, 2015 and 2019. Currently, the Act is undergoing legal review. The Act has created the Communications Authority (CA) of Kenya that regulates the ICT sector and processes huge amounts of personal data through telcos. To further contain the cybercrimes that target personal data, the enactment of the Computer Misuse and Cyber Crimes Act in 2018 has established a multi-agency collaboration framework known as the National Computer and Cybercrimes Coordination Committee (NC4) to advise the government on cyber security for a safer digital economy. Specifically, the Act was created to protect the confidentiality, integrity and availability of data and facilitate the prevention, detection, investigation, prosecution, and punishment of cybercrimes. The Act defines critical data and critical infrastructure as that one whose disruption would significantly interrupt life sustaining service, economy; and lead to massive casualties or fatalities or has adverse effect of national security. Further, there are draft cybersecurity regulations awaiting approval primarily for elaborating the provisions in the Act.

4.2.7 Data storage

Data storage refers to retention of information/data using technology specifically developed to keep that data and have it accessible, as necessary. Kenya's data protection regulations provide the basis for data localization in the country and therefore target processing of certain categories of personal data and critical systems. As noted earlier, like other countries, Kenya is restricting cross-border data flows of citizen data to safeguard national interests, including national security and privacy of individuals. The regulations require processing of personal

data of strategic interest to be affected through a server and data centre located in Kenya or a serving copy of such data should be stored in a data centre located in Kenya. The strategic personal data include data derived from the following systems as prescribed in section 26 of the General Data Protection Regulations:

- Civil registration and legal identity management systems;
- Electoral systems that facilitate the conduct of elections for the representation of the people under the Constitution;
- Any system for administering public finances by any State organ;
- Any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018;
- Any system offering any form of early childhood education and basic education under the Basic Education Act, 2013; and
- Any system facilitating provision of primary or secondary health care for a data subject in the country.

4.2.8 Data sharing

Data sharing is a practice of making data available for use in decision making, research or any other purposes. There are various policy efforts towards personal data sharing. For instance, Kenya has put in place data protection regulations in 2020 that outline data protection measures for safeguarding civil registration and identity management systems. The regulations provide the data protection framework to be followed by the civil registration entities when collecting, processing, storing, using, sharing and destroying personal data. A well-established and secure civil registration and identity management is critical for developing a robust digital economy in Kenya. Similarly, the Office of the Data Protection Commissioner has developed several guidance notes for secure processing of personal data. The guidance notes are important because of their role in increasing compliance to data collection and sharing by the data controllers and data processors to the data protection laws. A summary of the guidelines is provided in Table 4.3.

Table 4.3: Summary of data protection guidelines

Name of guideline	Description of guideline
Guidance notes on Registration of Data Controllers and Data Processors	This guidance assists public and private entities in ascertaining if they are Data Controllers or Data Processors and understand their obligations with respect to mandatory registration. The guidance provides a checklist of description of data controllers and data processors, requirements for mandatory registration, amount of fees to be paid and other consideration for registration.
Guidance Notes for Electoral Purposes	This guidance note provides direction on processing of personal data for electoral purposes. The guidance note provides lawful basis for processing personal data, including legal obligation, public tasks, legitimate interests, consent, and sensitive personal data. The guidance note provides for registers of voters, register of members including duty to notify, rights of a data subject, privacy by design or default and data protection impact assessment.
Guidance Note on Data Protection Impact Assessment	This guidance note provides a framework to data controllers and data processors in risk identification and mitigation measures to protect personal data. A data protection impact assessment is meant to identify the least privacy intrusive way in processing personal data. The guidance notes provide procedures to be followed by data controllers and data processors when undertaking any project involving personal data.
Guidance Note on Consent	This guidance note outlines that consent is an essential element of data protection required during the collection, use and disclosure of personal data. The guidance notes assist data controllers and data processors understand their duties under the Data Protection Act and appreciate their obligations when obtaining consent.

Complaints Management Manual	This manual provides guidance on complaints management process focusing on inquiry or preliminary investigation only. The manual provides guiding principles to be followed when managing complaints. The manual provides steps to be followed when lodging a complaint, complaints reporting channels, forms of complaints, and information required while lodging a complaint. The manual provides process to be followed when screening complaints, resolving, and concluding a complaint.

Source: Office of Data Protection Commissioner (2023)

4.2.9 Comparison of Kenya and selected countries on various elements of the strategic pillar

The recent technological developments have strengthened the recognition of privacy and protection of personal data as a key pillar in the respect for human dignity globally. The growth of the digital economy and technological advances, which largely depend on personal data, requires reciprocal formulation and implementation of data protection laws and policies. Kenya has recently joined countries that enacted data localization measures that include Vietnam, Indonesia, Brunei, Iran, China, Brazil, India, Australia, South Korea, Nigeria, Ghana, and Russia. The landscape of legislative data localization requirements is highly diverse and the degree of restriction and their impacts on economies differ from country to another. Some countries are imposing local storage requirements; that is, only a copy of the data has to remain within the territory of the country. This is the case in Denmark, Germany, Greece, the Netherlands, New Zealand, Poland, Romania, Sweden, and Turkey. These measures are usually imposed on a specific set of data relating to corporate documents, and the local storage is usually imposed so that the authorities can easily access such documents. In other cases, countries are not only imposing local storage restrictions, but also local processing requirements. Kenya, like other countries such as Denmark, Germany, Greece, the Netherlands, New Zealand, Poland, Romania, Sweden, and Turkey is imposing local storage requirements; that is, having data stored in a local server or keeping a copy of the data within the territory of the country.

The analysis in Table 4.4 indicates that Kenya has significantly put in place various policy measures towards building data localization. For instance, Kenya has comprehensive policies in the establishment of Supervisory authority, Supporting resources (budget and staff); Data architecture; Data security; Data storage; and Data sharing. However, Kenya does not have a comprehensive policy document on data standards and data quality. The recent development in the emerging technologies such as artificial intelligence are posing new challenges to the collection, usage and sharing of personal data globally.

Table 4.4: Comparison of elements of strategic pillar across selected countries

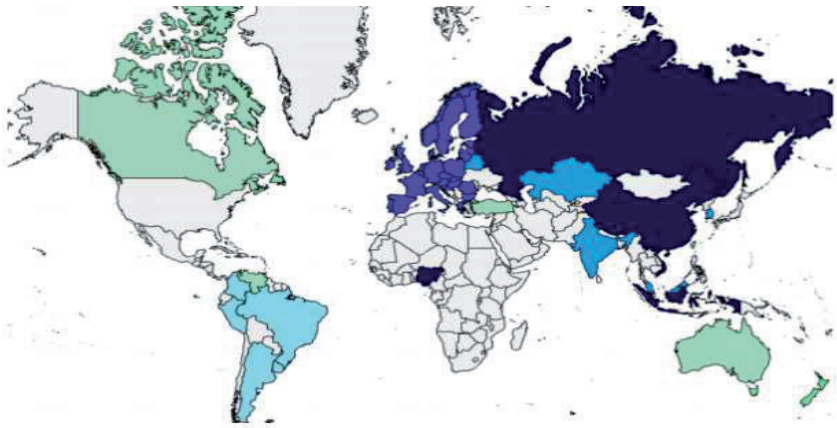
Policy Element	Policies				Acts/Laws/Regulations				Guidelines			
Countries	K	U	N	A	K	U	N	A	K	U	N	A
Establishment of supervisory authority	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Supporting resources (budget and staff)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Data standards	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
Data architecture	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
Data quality	N	N	N	Y	N	N	N	Y	N	N	N	Y
Data security	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Data storage	Y	Y	Y	Y	N	N	N	Y	N	N	Y	Y
Data sharing	Y	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y

NB: K=Kenya, U=Uganda, N=Nigeria, A=Australia Y=Yes N=No

4.2.10 Forms of data localization adopted by various countries

As highlighted earlier, data localization is still a thorny issue dividing policy makers across the globe. In the global policy arena, there are various forms of data localization, ranging from very strict regulations to less strict rules as shown in Figure 4.1 in processing of personal data.

Figure 4.1: Global spread of data localization



COLOR	STRENGH OF MEASURES	COUNTRIES
	Strong: Explicit requirements that data must be stored on servers within the country.	Brunei, China, Indonesia, Nigeria, Russia, Vietnam
	De Facto: Laws that create such large barriers to the transfer of data across borders that they effectively act as data localization requirements.	European Union
	Partial: Wide range of measures, including regulations applying only to certain domain names and regulations requiring the consent of an individual before data about them is transferred internationally.	Belarus, India, Kazakhstan, Malaysia, South Korea
	Mild: Restrictions on international data transfers under certain conditions.	Argentina, Brazil, Colombia, Peru, Uruguay
	Sector-specific: Tailored to specific sectors, including healthcare, telecom, finance, and national security.	Australia, Canada, New Zealand, Taiwan, Turkey, Venezuela
	None: No known data localization laws.	Remaining Countries

Source: Global Commission on Internet Governance, ourinternet.org

China's data protection laws require personal data concerning Chinese citizens be stored and processed locally. China restricts market access for cloud computing if the required data localization requirements are not met. The country introduced measures for keeping personal data relating to e-banking, health and medical information in servers located in China. Similarly, the Counter-Terrorism Law introduced in 2016 requires Internet and telecommunication companies and other providers of "critical information infrastructure" to store data on Chinese servers and to provide encryption keys to government authorities. China enacted a new cybersecurity law in 2016 that requires companies to store users' personal information and other important business data in China. China has successfully reduced data breaches arising from cross border data flows. Russia's strict data localization laws of 2015 mandate that data operators who collect personal data about citizens must "record, systematize, accumulate, store, amend, update and

retrieve" data using databases physically located in Russia. The laws require personal data to be transferred out of the country, but only after it is first stored in Russia. In Brazil, all Internet Services Providers such as Google and Facebook are required to store information relating to Brazilians on local servers. From 2016, the Brazilian government enforces data localization as a requirement for public procurement contracts involving cloud-computing services. In France, there are efforts to promote a local data-centre infrastructure, known as the sovereign cloud and therefore all public data should be considered as archives and stored and processed in France. Similarly, Germany introduced local data storage requirements for a type of telecommunications metadata in 2016. Venezuela has regulations requiring that IT infrastructure for payment processing be located domestically.

In Vietnam, the government has local server requirements for online social networks, general information websites, mobile telecoms, network-based content services and online games services and therefore organizations are required to establish at least one server inside the country from 2016. Vietnam forbids direct access to the Internet through foreign ISPs and requires domestic ISPs to store information for at least 15 days. Further, all over-the-top services (such as WhatsApp and Skype) are subject to data localization requirement in Vietnam. Iran has initiated various data localization initiatives in 2015, including the launch of its own search engines, which only show approved websites. Iran set up its first government-paid cloud data centre in 2016 and ordered foreign messaging apps, such as WhatsApp and Telegram, to store data of Iranian users locally. Similarly, since 2005, Kazakhstan has required all domestically registered domain names (i.e., ".kz" top-level domain) operate on physical servers within the country and companies collecting and using personal data to keep such data in Kazakhstan. Saudi Arabia has certain secular regulations passed by the government on data privacy/protection that contain specific provisions governing the right to privacy and data protection. Saudi Arabia has sectoral regulations with data protection obligations regarding organizations working in telecommunication, IT/cloud services, healthcare, and financial services industries. For instance, the country has established a Cloud Computing Framework based on international best practices and governs the rights and obligations of cloud service providers (CSPs), individual customers, government entities and businesses.

Australia has specific laws pertaining to instances of dataflows. For instance, the laws require telecommunication carriers to capture and retain certain information. Australia enacted the Personally Controlled Electronic Health Records Act that requires personal health records be stored only in Australia. South Korea has data localization requirements to protect local e-commerce and online payment operators. The rules require all cloud computing networks serving public agencies to be physically separate from networks serving the general public. The rules bar any company from using mapping data not stored in South Korea. Colombia laws stipulate that data processing centres should be in Colombia, since storing data overseas is considered too risky to network security and personal data. Cyprus has a directive requiring data operators to retain certain categories of traffic and location data for a period of six months to two years. Denmark's laws require companies

to store accounting data in Denmark for five years and may grant permission to preserve accounting records abroad in specific locations in the country. Poland requires e-commerce entities, including betting firms, to store customer details in Poland or in the servers in the EU. Sweden requires companies to store data about current company records and accounts in Sweden for seven years. Romania requires all data on gambling players and their activities to be stored in Romania. In 2016, Turkey enacted laws which limit the transfer of personal data out of the country and requires firms to store data on citizens in the country. In Canada, some provinces including British Columbia have implemented laws mandating personal data held by public bodies such as schools, hospitals, and public agencies to be stored and accessed only in Canada unless certain conditions are fulfilled. Taiwan's laws permit government agencies to restrict international transfers of data in the industries they regulate. Argentina prohibits the transfer of personal data to countries that do not have an adequate level of protection in place.

Other countries have introduced various forms of local requirements. India's data localization requirements require backups of financial information, if primarily stored overseas, to be stored in India. The Central Government determines the categories of personal data which are 'critical' with strategic interests and should be processed within India. All payment system providers are required to ensure that their payment data is stored in systems located in India. Further, India requires e-pharmacies to store data locally. India allows the transfer of other non-critical personal data subject by having one serving copy of it being stored in India. In Indonesia, datalocalization laws require e-money operators to store data locally and all over-the-top service companies (such as Skype and WhatsApp) to store data locally. The United States of America (USA) has data localization requirements to restrict the location of information systems that receive, process, store, or transmit federal tax information to areas within the United States territories, embassies, or military installations. In 2015, the US Department of Defense issued revised rules that require all cloud-computing service providers that work for the department to store data domestically. Similarly, some State and local governments impose data storage requirements in contracts. Finally, in the Africa region, there are some countries that have adopted data localization measures including Nigeria, South Africa, and Uganda. For instance, Nigeria's Central Bank introduced a measure in 2011 that requires all point-of-sale and ATM transactions to be processed locally. Nigeria introduced several restrictions on cross-border data flows in 2014 and mandated that all subscribers, government, and consumer data be stored locally.

Based on the analysis of various forms of data localization adopted by countries along the elements of the strategic pillar, Kenya's data localization regulations are less strict, not fully implemented and are barely two years old. The budget allocation for Kenya's data protection regulator is significantly less as compared to other jurisdictions. Moreover, there several gaps that require policy interventions, such as lack of National Data Governance policies and strategies that are necessary for personal data economy. Further, based on the requirements spelt out in the strategic pillar, Kenya has a well-defined strategic model within the Security and Privacy Capability Maturity Model. This is further demonstrated by various indicators, including the ITU ranking on data policies for data protection. As

noted earlier in Table 4.4, the country still faces challenges that include absence of a national comprehensive data management policy to provide a road map of how data initiatives are to be rolled out in the data economy. In some countries such as Australia, India and Germany, there are comprehensive data localization frameworks that indicate the sector and scope of personal data, time, location, systems, and contracts associated with personal data. The Office of the Data Protection Commissioner in Kenya is yet to adequately put in place mechanisms to support data localization in the country. Currently, the Office is focusing on creating awareness on the Data Protection Act, and registration of entities (data controllers and data processors) dealing with personal data. So far, about 3,000 have been registered as at end of 2023. Further, there are many actors across all sectors dealing with personal data spanning from the public sector, private sector to community-based organizations and these require a robust mechanism to ensure effective application of the data localization measures in the country. Finally, most of the personal data is being processed outside of the country because of superior data products offered at a lower cost, hence favourable for most businesses. There is need to build adequate local infrastructure such as data centres to support local processing of data, which is key in building sovereignty for personal data.

4.3 Tactical Pillar (People)

This study reviewed elements in the tactical pillar supporting the capacity for coherent implementation of Kenya's vision on data protection for the growth of personal data sector. The key elements include training institutions, Human Resources and Support to Skills Development and Job opportunities. These elements provide critical skills for data protection to implement adequate quality controls for processing personal data.

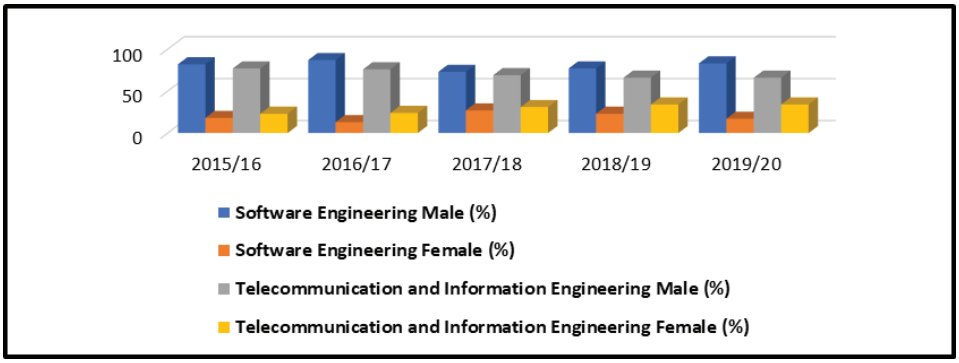
4.3.1 Training institutions

This policy element refers to the available training institutions such as universities offering data protection related programmes. Kenya recognizes the importance of data in the growth of its digital economy. Consequently, data protection is growing in importance as Kenya adopts digital services to enhance data privacy and compliance. As demonstrated by the discussion on the strategic pillar, Kenya has initiated significant efforts to build capacity to support the implementation of the Kenya's vision on data protection. In building the necessary capacity to implement the strategic interventions for data protection, Kenya has invested in various initiatives to develop digital skills required in the data economy. For example, the Ministry of Information Communications and Digital Economy is implementing a Digital Literacy Programme (DLP) popularly known as DigiSchool. The programme aims to prepare every pupil for today's digital world. The programme introduces primary school children, beginning with those in lower primary, to the use of digital technology and communications in learning. DLP is targeted at learners in all public primary schools in Kenya covering more

than one million class 1 pupils in all the 23,951 primary schools. The programme has developed infrastructure, content, trained teachers and provided learning digital devices to schools. A total of 1,148,160 digital devices had been installed in 21,232 schools (97.7%) as of 19th September 2019. About 201,811 devices were assembled by local universities - Moi University and Jomo Kenyatta University of Agriculture and Technology. Over 22,259 schools have been connected to power (19,023 schools connected to the power grid supply and 3,236 connected to the solar power supply). Further, over 228,000 teachers have been trained on the use of technology in learning and over 47000 teacher's devices distributed in primary schools.

Locally there are 22 public universities and 14 chartered private universities offering ICT degree programmes for graduates with skills in telecommunication; software engineering; cybersecurity; software development; hardware design and implementation of network systems. In addition, there are various tertiary training institutes including Technical and Vocational Education and Training (TVET) institutions across counties that equip students with technical skills and soft skills with an aim of making the youth employable. However, there are various challenges faced in the development of the prerequisite digital skills for data economy. For instance, most of the digital jobs are dominated by males. According to the Kenya Economic Report of 2020, female enrolment in ICT-related university programmes is less than 40 per cent as shown in Figure 4.2.

Figure 4.2: Enrolment of computer related university programmes (%)



Data source: KNBS Economic Survey (various)

4.3.2 Human resources and support to skills development

This policy element refers to the provision of facilitation to develop skills for data protection-related tasks. To further develop digital skills for personal data economy and support the implementation of DigiSchool, the government through the Kenya Institute of Curriculum Development has approved a new curriculum

for secondary and primary school students for computer coding. It is expected that the country will require innovative digital products to support the growth of the data economy. To actualize this dream, Kodris Africa, an online publishing company that specializes in equipping learners with 21st century skills, will offer the syllabus with support from other partners. The curriculum will include practical lessons that will equip more 20 million children with relevant digital skills necessary for the digital economy. Students will develop coding skills so that Kenya can be a producer of digital products in the 21st century digital age. Kenya is the first country on the African continent to implement such a curriculum.

Similarly, the Presidential Digital Talent Programme (PDTP), also known as DigiTalent, is being implemented by the Ministry of Information Communications and Digital Economy. Digitalent is a strategic intervention to develop and sustain high-end ICT talent by bridging the gap between industry requirements and the capabilities of the local workforce. This is in line with the National Digital Master Plan (2022-2032), which underscores the need to develop a critical mass of high-end ICT skills and to develop an ICT-ready workforce to meet the needs of the digital economy. The participants are placed both in the Government Ministries (for 10 months) and in the private sector (for 2 months) during the programme, giving them a holistic understanding of how ICT works both in the public and private sectors. The programme provides participants with an excellent opportunity to gain workplace experience, expand knowledge, mentorship, refine career goals and build professional networks in the areas of: Network and Infrastructure, Application Development, Graphic Design, Information Security, and Project Management. Further, participants are mentored on leadership skills and innovative thinking required in the data economy. After the programme, the participants emerge as talented and well-rounded individuals with a clear career progression path in the digital economy, and make valuable additions in protecting personal data. The programme has benefited over 2,100 ICT graduates.

The Ajira Digital Programme is a government initiative to empower over one million young people to access digital skills and job opportunities. The programme seeks to position Kenya as a choice labour destination for multinational companies and encourage local companies and the public sector to create digital work. The main objectives are to raise the profile of digital work; promote a mentorship and collaborative learning approach to finding digital work; provide Kenyans with access to digital work; and finally promote Kenya as a destination for online workers. The components of the Ajira digital programme have been designed to address the main challenges that hinder the youth from benefiting from digital job opportunities. The programme promotes access to dignified work, build skills and awareness and promotes access to infrastructure as data economy grows. The Government has built capacity of 92,000 youths under the Ajira initiative and, currently, over 1.2 million are working on digital and digitally enabled jobs, and further over 15,000 civil servants have been trained on digital technologies.

The Konza Technopolis is one of the national flagship initiatives in Kenya. The initiative offers a strategic opportunity to invest in the growth of the digital economy in Kenya and the country's overall economy. When completed, Konza Technopolis will offer digital infrastructure such as data centres that support the growth of

the data economy. Other benefits include personal data-related job opportunities in Konza's world-class technology hub that will be home to leading companies in education, life sciences, telecom, and Business Process Outsourcing (BPO). Commercial space for these uses will be complemented by diverse residential neighbourhoods, hotels, a variety of retail offerings, community facilities, and other public amenities. So far, local engineers and artisans are involved in the horizontal development of the project. Mega infrastructure including establishment of the Kenya Advanced Institute of Science and Technology (Kenya KAIST) to foster elite human resources for personal data are underway. With establishment of Konza Technocity, Kenya could potentially create more than 200,000 technology-related jobs and make the country a model for other African countries in technological solutions. Konza will support the Business Process Outsourcing (BPO) initiatives in Kenya. Currently, there are only five globally competitive BPO service providers in Nairobi, employing more than 3,000 youths and contributing about Ksh 2 billion into the country's revenue.

Other initiatives that have potential to create job opportunities and build capacity in terms of digital skills in the data economy include the Jitume programme managed by the Konza Technopolis, which encourages the youth to access digital devices and opportunities to learn, become certified on digital skills and to access digital jobs. This programme is line with the Kenya National Digital Master Plan (2022-2032), which envisages upskilling of over one million youth who enter the job market annually with ICT skills. The Jitume programme aims to address the main challenges in accessing digital devices and Internet connectivity, training, and knowledge and opportunities that can result in decent and dignified income. So far, the programme has created 88 Jitume laboratory centres supporting about 13,000 users. Each Jitume Centre will have 100 Virtual Desktop Infrastructure (VDI) with broadband connectivity, reliable power and security. Other programmes include digital inclusion projects such as Constituency Digital Innovation Hubs and Studio Mashinani. The objective of the Constituency Digital Innovation Hubs is to support entrepreneurs access free Wi-Fi in all the 290 constituencies countrywide. The initiative enhances awareness and uptake of online platforms for employment and business opportunities in the data economy. The Studio Mashinani project aims at enhancing availability of accessible recording studios and enhancement of self-employment opportunities for artists in the robust digital economy.

4.3.3 Job opportunities

Job Opportunities refer to the availability of jobs for trained graduates/personnel in getting jobs. The data economy jobs and all the digital jobs in general require technical competencies ranging from low level of computer literacy to advanced competence in manufacturing of hardware and software development skills to support personal data products and services. Universities, innovation hubs and ICT training institutions provide support through robust training programmes, mentorship, capacity building and partnerships. For instance, innovation hubs not only offer employment but also facilities, financial or in-kind support to create

products. Kenya has about 50 tech hubs, making Kenya the heart of East Africa's technology ecosystem (GSMA 2019). Similarly, the number of tech hubs in Africa has grown from 314 in 2016 to 618 in 2019. According to GSMA report (2014), Kenya had about 40,000 ICT startups that created about 160,000 jobs. Unlike developed businesses, startups do not have the resources to employ the qualified personnel, and thus get less experienced employees who are mentored and trained on the job.

Development of personal data sector has potential to generate jobs along the data economy value chain that includes the core, intermediary and end user levels. For instance, at the core level, digital jobs are created by the telecommunication firms, Internet service providers, computer manufacturers/assemblers; content providers; software producers; hardware manufacturers; technology research labs; and technology innovation hubs. Some of the jobs include engineers for telecommunication, networks, software and hardware. A summary of technical skills for core level is listed in Table 4.5, and these skills are generally offered by the universities and specialized ICT training institutions. At the intermediary service level, digital jobs are created by financial service providers, enterprises offering e-commerce, distributors; agents; and government e-services such as Huduma services. A summary of technical skills for intermediary level is listed in Table 4.5, and these skills are generally offered by the universities and specialized ICT training institutions. Finally, at the end user service level, digital jobs are created by services rendered by intermediary service providers. Some of the jobs include data clerks, customer care officers, operational officers and technical field officers. These jobs involve registering and supporting the users/subscribers. In addition, these jobs involve running one's business to offer data protection products and services. The low skilled digital jobs normally associated with the lowest level require the basic digital skills to perform the jobs. A summary of technical skills for end user level is listed in Table 4.5, and these skills are generally offered by tertiary training institutions.

Table 4.5: Summary of technical skills required in the data economy

Data Value Chain	Types of Jobs	Technical Skills requirements	Non-Technical Skills requirements	Level of Training
Core level	Telecommunication Engineers, Network Engineers, Computer Engineers, Satellite engineers, software engineers, hardware engineers, GIS engineers	• Computer engineering • Telecommunication engineering • Electrical engineering • Mechatronic engineering • Remote sensing • Geographic information science • Software engineering	• Project management • Communication skills • Analytical skills • Business skills • Marketing skills	• Universities • Specialized ICT training institutions
Intermediary level	Software engineers, GIS officers, Database engineers, mobile bank agents, ecommerce specialists	• Software engineering • Geo-spatial engineering • Surveying • Mapping • Database management • Mobile technologies • Ecommerce	• Project management • Communication skills • Analytical skills • Business skills • Marketing skills	• Universities • Specialized ICT training institutions
End Users level	Data clerks, Digital clerks, Bank Clerks, Customer care, sales representatives	• Basic use of ICT tools	• Customer care skills • Business skills • Sales and marketing skills	• Tertiary training institutions

Source: Author's construction

4.3.4 Comparison of elements of tactical pillar across selected countries

Kenya is regarded as the Silicon Valley of Africa because of its robust digital economy that is supported by enabling policy and legal framework. Mainstreaming digitization into the realization of the national development goals is a driving force for the digital economy in Kenya, and thus a government priority as outlined in the various strategic documents including the Kenya Vision 2030, Digital Economy Blueprint and National Digital Masterplan. Digitalization is a critical determinant of economic growth, national security, and competitiveness. In the recent years, the digital economy primarily driven by data is among the fast-growing sectors at a rate of 9.9 per cent in 2022 with potential to significantly contribute to Kenya's growth and development. The sector contribution was 6.3 per cent of the national growth in 2022 based on the Economic Survey (2023). The growth of the digital technology in Kenya is mainly driven by mobile innovations in some cases showcasing leadership across the globe. Kenya is home to leading mobile innovations such as M-Pesa, which is a global innovation supporting mobile money transfer services. Interestingly, personal data is a key ingredient in the innovations. Based on four fundamental dimensions (Technology, People, Governance and Impact), Kenya is rated third best performing African country behind South Africa and Mauritius in embracing the digital transformation, and is ranked 77 globally by the Network Readiness Index (NRI) 2022. Similarly, Kenya is ranked 58 globally based on availability, affordability, relevance and readiness of Internet by the Inclusive Internet Index (2022). Kenya is rated among the top 5 African countries for thriving Internet economies based on the Inclusive Internet Index (2019). Similarly, Kenya is ranked 88 by the Global Innovation Index 2022 and position 2 on mobile money by the Boston Consulting Group (BCG) 2022. Kenya is among the top 5 countries in Africa with more than 50 active tech hubs to support the growth of digital innovations. Further, according to the Digital Skills Readiness by Wiley (2021), Kenya is ranked 70 globally and 2nd in Africa.

Table 4.6: Comparison of elements of tactical pillar across selected countries

Policy Element	Policies				Acts/Laws/ Regulations				Guidelines			
Countries	K	U	N	A	K	U	N	A	K	U	N	A
Training institutions	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Human resources and support to skills Development	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Job opportunities	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y

NB: K=Kenya, U=Uganda, N=Nigeria, A=Australia Y=Yes N=No

Based on the analysis on Table 4.6 in the tactical layer, Kenya has put in place various initiatives to build the capacity required to support the implementation of data localization in the country. As a result, Kenya has demonstrated better performance at the global level in the development of digital skills as compared to other African countries. Notably, Kenya recorded impressive performance in terms of availability of scientists and engineers, Government success in ICT promotion and the ease of finding skilled employees in the job market, which are key in the development of the prerequisite digital skills for building a successful data economy. However, there are several gaps in developing the necessary capacity that requires policy interventions. As noted in Table 4.6, Kenya did not perform well in having a workforce with global science and technology skills, which is a barrier in progressing the data economy. Further, the National Digital Masterplan notes that Kenya has low and intermediate digital skilled experts with few professionals possessing advanced digital skills. High-end digital skills are essential and therefore building digital skills is key for leveraging on the emerging technologies to facilitate a vibrant personal data economy. The World Bank Enterprise Survey (2018) shows that skills constraints in the personal data, mainly those associated with technological upgrading, is a strong indication of more specialized skills requirements. To address the technical skills in the country, most firms prefer sourcing the skills outside the country. Further, most graduating students who complete their formal education do not receive practical skills that are required when joining employment in public and private entities, including the startups and innovations for personal data economy. The root cause of this is linked to the failure to align the curriculum to the industry needs, and poor integration of theory into practical scenarios by learning institutions. This implies that the graduating students from educational institutions lack market-oriented skills required in the job marketplace. To build more skills to the students, universities, innovation hubs and ICT training institutions should provide skills development support through robust training programmes, mentorship, capacity building and partnerships for a successful data sovereignty in Kenya.

4.4 Delivery Pillar (Technology and Infrastructure)

This section provides analysis on the delivery layer, which includes data generation and collection systems; Internet infrastructure; cellular infrastructure; data storage/data centres, spatial infrastructures, and cybersecurity initiatives to support the day-to-day implementation (or deployment) of organizational, sectoral, national, or cross-border data strategies.

4.4.1 Data generation and collection systems

Data generation and collection systems refer to systems to generate and collect personal data. Kenya is regarded as the Silicon Valley of Africa because of its robust software industry. Evidently, there are various local firms and startups boosting Kenya's capacity in building data localization. Local software firms develop various data products for government and businesses in form of

computer systems and applications that support provision of critical services, including finance, national security, transportation, water supply, blood supply and health. These systems and applications support processing of personal data in terms of creation, storage, and dissemination of personal data. As mentioned earlier, personal data is a key asset in critical systems, and thus demand better protection. Any breach on critical systems targeting personal data is detrimental to the provision of essential services. Consequently, the Government of Kenya has recognized the importance of software development in supporting the achievement of the national development goals. Among the relevant flagship programmes is the establishment of two major software factories that will employ over 100,000 software engineers to develop software/systems for the region and for the global market. One of the software factories will be based in Bomet County under the public-private partnership arrangement. These upcoming projects are expected to create employment opportunities for the youth and spur the country's data economy growth. The initiatives will further boost the number of software engineers who are above 60,000 as at 2020 compared to Nigeria, which leads in Africa with more than 85,000 software engineers.

As discussed earlier, the Data Protection (General) Regulations (2021) have outlined that strategic personal data processed by certain systems must be kept within the Kenyan border. These systems include: Civil registration and legal identity management systems; Electoral systems that facilitate the conduct of elections for the representation of the people under the Constitution; Any system for administering public finances by any State organ; Any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018; Any system offering any form of early childhood education and basic education under the Basic Education Act, 2013; and any system facilitating provision of primary or secondary health care for a data subject in the country. For instance, Civil registration and legal identity management systems are key to reinforce the right to identity and in realization of citizenship and participation in any formal economy.

Generally, there are two major categories of systems, namely: Digital business applications and Digital government applications as indicated in Table 4.7. A large segment of local information systems processing amount of personal data are owned by either public or private actors. Some public systems such as IFMIS are heavily used to support financial transactions by the National and County governments. Unfortunately, due to inadequate local data centres, huge amounts of strategic personal data are processed outside Kenya through foreign digital platforms. Table 4.7 shows a list of selected computer systems and applications in Kenya with the type of personal data being processed.

Table 4.7: Selected computer systems and applications in Kenya

Category	Sector/function	Name of the computer system/software	Description of personal data processed
Digital Government	Data storage	• Konza National Data Centre and Smart City facilities including other data centres in selected areas	Hold critical data including personal data for citizens
Digital Government	Identity management	• National Integrated Identity Management System (NIIMS/Huduma card Database)	Holds personal data for citizens
Digital Government	Civil registration	• Civil registration database	Holds personal data for citizens (Births and Death)- used for issuing passports, National IDs, Death Certificates
Digital Government	Elections	• Kenya electoral system	Holds database of all Kenyan registered voters
Digital Government	Government	• National Education Management Information System (NEMIS)	Holds education-related database
Digital Government	Human resources	• Government Human Resource Information System (GHRIS)	Online payslip platform where government employees can now view and download their payslips
Digital Government	Education	• Kenya National Examination Systems	Systems for managing marks/certificates for students at primary, secondary and tertiary colleges
Digital Government	Financial management	• Financial Management Information System (IFMIS)	System for financial management
Digital Government	Tax	• iTax system	Holds data for taxpayers in Kenya
Digital Government	Customs Management	• Integrated Customs Management System	Holds data for exporters and importers
Digital Government	Transport	• Transport Information Management System Read	Hold data for vehicle owners and drivers
Digital Government	Data Storage	• Open Data Initiative	Holds datasets for public consumption

Digital Government	Transport	• Airport Management System	Holds airport and flight details
Digital Government	Energy	• Energy systems	Holds personal data for subscribers, e.g. KPLC database
Digital Government	Health	• National Health Systems	Holds personal medical information
Digital Government	Water	• Water systems	Holds personal data for subscribers, e.g. Nairobi Water and Sewerage Company database
Digital Government/ Digital Business	Agriculture	• Agriculture and Food Systems	Holds personal data for producers, distributors and consumers
Digital Government	Land	• Land Information Management System	Holds personal data for landowners
Digital Business	Telecommunication	• Money transfer systems such as M-Pesa • Telecommunication equipment database • Hold personal data for subscribers	Subscribers for cellular services
Digital Business	Financial services providers	• Fintech systems	Hold personal data for subscribers for financial services
Digital Business	Insurance services providers	• Insurance systems	Hold personal data for subscribers for insurance services
Digital Business	E-commerce	• E-commerce platforms	Hold personal data for subscribers for Ecommerce services

Source: Author's construction

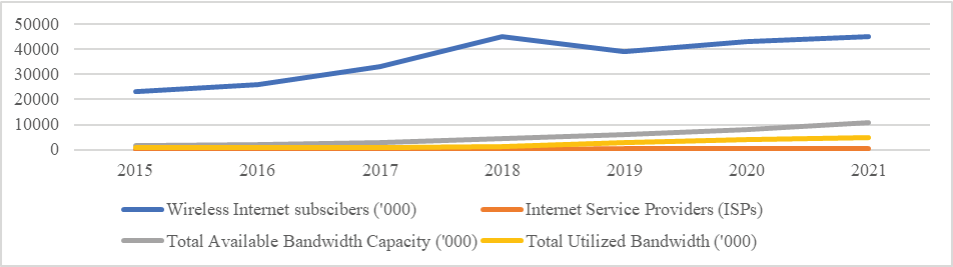
4.4.2 Internet infrastructure

Internet infrastructure refers to the physical hardware, transmission, media and software used to interconnect computers and users on the Internet. Internet infrastructure provides hosting, storage, processing and sharing of information. Various research shows that a well-connected and robust Internet infrastructure is critical to unlock the opportunities of the data economy. This means that a country served by adequate infrastructure supports the growth and development of data economy. Kenya has put in place various Internet connectivity initiatives to enhance connectivity for communication and collaboration required to support the

the development of personal data economy. The Internet connectivity initiatives aim to ease communication across counties and improve government service delivery to the citizens, such as issuance of national identity cards, passports and registration of birth and death certificates. For instance, the National Optic Fibre Backbone (NOFBI) is a project aimed at ensuring connectivity in all the 47 counties of Kenya. Under NOFBI, the country has put in place about 30,000km of fibre linking more than fifty-seven (57) towns within the country and has connected all the forty-seven (47) county headquarters. Further, the country plans to have over 100,000km of high-speed fiber optic infrastructure under the National Digital Superhighway programme as envisaged in the Bottom-up Economic Transformation Agenda (BETA). The programme aims to provide Internet to all schools, government institutions/offices, metro-cities, health facilities, rural businesses, homes, and public space. Similarly, based on the National Digital Masterplan, the government has prioritized establishing 25,000 Internet hotspots for Internet access across the country to innovators, youth, and entrepreneurs. So far, the government has put in place about 1,000 public Internet-hotspots.

Due to robust Internet infrastructure for the data economy in the country, the number of Internet subscriptions and consumption of mobile data have continued to grow due to increased demand for digital services for teleworking, e-learning and e-commerce as shown in Figures 4.3. In the last five years, the number of licensed Internet Services Providers (ISPs) has significantly increased. Similarly, fiber networks in urban residential and commercial areas have increased largely due to new partnerships between telecommunications and power companies. The increased service availability of infrastructure has spurred the growth of the data economy sector in the country.

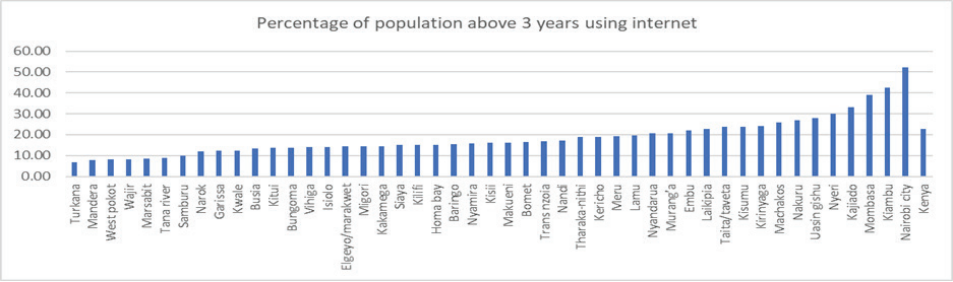
Figure 4.3: Internet services



Source: Communications Authority reports

However, a relatively huge population has limited access to affordable and high-speed Internet services. Even though the number of connections for the broadband Internet services at offices and homes levels has increased, access to Internet services remains a serious challenge due to limited coverage by service providers and high cost of the services. Based on Kenya Census data (2019), Nairobi County registered the highest percentage of population using Internet while Turkana County had the lowest (see Figure 4.4).

Figure 4.4: Percentage of population above 3 years using the Internet



Source: KNBS (2019), Population Census

In terms of web hosting capacity, Kenya has significantly developed its capacity for domestic hosting and domains, which is a key component for data economy as demonstrated by Table 4.8. Over the years, the number of registered Kenyan domains have increased from 85,744 in 2021 to 100,420 in 2022. The use of .go.ke especially for government websites has increased in the last six years due to strong advocacy for government entities to use the domain. The growth of Kenyan-registered domains is attributed to reduced domain renewal fees. However, there are many Kenyan entities relying on international domains largely due to lower cost and quality services as compared to Kenyan domains, and therefore this may hamper the efforts to build localization in data economy.

Table 4.8: Registered Kenyan domains, 2017-2022

Year	.ac.ke	.co.ke	.go.ke	.info.ke	.me. ke	.mobi.ke	.ne.ke	.or.ke	.sc.ke	.ke	Number of Kenyan Registrars	Total number of registered Kenyan domain
2017	768	68340	414	374	386	126	466	1981	1027		372	73,972
2018	891	77820	502	443	345	180	277	1976	1212	2098	382	85,744
2019	889	87243	565	155	219	40	96	1831	902	2226	203	94,166
2020	962	93776	606	156	182	43	51	1930	838	2579	190	101,123
2021	1026	85536	615	144	298	38	48	1895	1002	3924	194	94,526
2022	1,079	90,000	656	131	1,325	32	48	1,846	931	4,372	183	100,420

Source: KNBS (Various), Economic Survey

In terms of Internet traffic, the Internet Exchange Points (IXPs) are key Internet infrastructure that allow local exchange of traffic among access providers, and between content providers and access providers. IXPs enable the exchange of local traffic and access to content, and it can deliver benefits to local Internet subscribers and organizations. Therefore, IXPs support local hosting providers, increase digitalization of services, and promote the development of skills and businesses to meet the growing demand for local hosting. Generally, local traffic exchange has better latency for speed and performance. The Internet Society has

established a three-stage development scale based on the percentage of localized Internet traffic as shown in Table 4.9.

Table 4.9: Stages of Internet Exchange Points (IXPs)

Stage 1	IXP is mainly used to exchange local traffic between local access providers. The benefits include lower costs for the access providers, lower latency of traffic exchange, and greater network resilience from not relying on international connections for local traffic exchange. Stage 1 localizes up to approximately 30% of total traffic, as it does not involve significant amounts of content
Stage 2	International content is made available locally, attracted by the IXP. The benefits include increased cost savings, lower latency when accessing content, and greater resilience. The decreased latency results in an increase in usage of that content, which increases the revenues of those ISPs that sell data packages. In addition, the lower cost of accessing content may be passed on to end users. Stage 2 localizes approximately 30% to 70% of total traffic.
Stage 3	Local content is hosted locally, rather than in data centres located abroad. The benefits include the gains of locally hosting international content and help promote a digital economy for local content developers. Stage 3 localizes 70% or more of total traffic

Source: Kende (2020)

Kenya passed IXP stage 1 in 2012 because about 30 per cent of Kenya's Internet traffic was localized. Currently, Kenya is in stage 2 with more 70 per cent of Internet traffic localized and is progressing to Stage 3. Kenya is experiencing an increased exchange of traffic locally rather than using expensive international transit, thus reducing the Internet cost. Notably, the capacity of Kenya's IXP grew from carrying a peak traffic of 1 Gigabit per second (Gbps) in 2012 to 19 Gbps in 2020, with cost savings quadrupling to US$ 6 million per year. Further, the majority of the large international content providers such as Google added at least one edge cache in the country, and many also added a point of presence (PoP). The recent adoption of data protection legal and policy framework has reinforced an environment of local-content hosting. According to the Internet Society's report (Kende, 2020), Kenya requires to address various policy issues to progress to stage 3 that requires 80 per cent of traffic being locally accessed. Among the issues faced by Internet service providers include low awareness of the benefits of local content hosting and peering at the IXP among key stakeholders, including content providers and poor accessibility at the last mile point by content users. A review by the Internet Society reveals that of all the countries in Africa with IXPs, the most developed Internet ecosystem in Africa is South Africa, which has achieved 80 per cent of localized traffic, followed by Kenya and Nigeria (Kende, 2020).

At the continental level, Africa imports more than 99 per cent of the Internet content consumed and, therefore, creating an Internet Transit Deficit (Internet Society, 2017). Internet Transit Deficit is where significantly less traffic is

generated locally than accessed internationally. However, Africa has registered terrestrial and submarine fiber infrastructure developments in the region that could support Internet traffic exchange in the region. In 2010, the Internet Society's team in Africa launched the organization's Interconnection and Traffic Exchange (ITE) programme with the goal of "80/20 by 2020"; in other words, that 80 per cent of Internet traffic would be locally accessible by 2020 against 20 per cent international traffic. This programme is meant to make Africa not just an 'Internet Consumer' but an 'Internet Creator' (Internet Society, 2017). Despite the ITE programme having been established for more than 10 years, Africa still relies on legacy Internet business strategies and policies that are still predominant. As African countries continue investing in the Internet infrastructure, most countries have recognized data protection as critical for growth and development of modern economies. Consequently, African countries are adopting data protection laws to protect huge personal data that is processed within and outside the continent.

4.4.3 Cellular infrastructure

This is a telecommunication network where the link to and from end nodes is wireless and the network is distributed over land areas called cells. Telecommunication companies are one of the largest holders of personal data globally. Kenya has numerous service providers running on modern cellular infrastructure to offer cellular services. The government has licensed various telecommunications operators to roll out 4G and 5G network services for data economy. Safaricom launched the fifth-generation network services on 26th March of 2021. It is observed that the number of fourth generation-based subscribers is steadily growing as compared to third generation-based subscribers. To offer secure communication services in the telecommunication sector, it is a requirement under the Kenya Information and Communication Act (2013) for all the mobile service subscribers to register their personal data with the service providers. Kenya is one of the African countries with the highest levels of mobile phone penetration. The demand for cellular services has grown steadily over the years as Kenya adopts the data economy as shown in Figure 4.5. Further, the government has continued to promote the use of e-government services, adoption of mobile money services, working from home, e-health programmes, and e-learning as part of the efforts to contain the spread of the pandemic. In the last seven years, the number of mobile subscribers who have registered has significantly grown from 37.7 million in 2015 to 65.7 million in 2022. The local mobile voice traffic has significantly grown from 39.1 billion minutes in 2015 to 78.2 billion minutes in 2022. Although the number of SMS sent has increased from 28.3 billion in 2015 to 51.2 billion in 2022, it has significantly been affected by the preference of the users, particularly on WhatsApp.

In terms of data on mobile money, the number of mobile money transfer service subscribers and mobile money agents has increased from 26.7 million and 318,607 in 2015 to 38.6 million and 292,301 in 2022, respectively. Similarly, the number of total transactions and value of mobile commerce transactions has increased

from 1.5 billion and Ksh 1.7 trillion in 2016 to 2.2 billion and Ksh 20.2 trillion in 2022, respectively.

The digital divide between rural and urban areas and across counties has widened, as shown in Figure 4.5. Based on the Kenya Census data for 2019, rural areas recorded higher ownership of mobile phones compared to urban areas. Further, most of the mobile owners are between 15 and 54 years.

Figure 4.5: Percentage of population owning mobile phones by counties

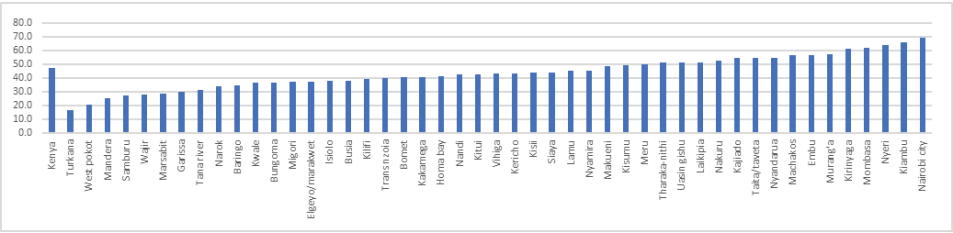
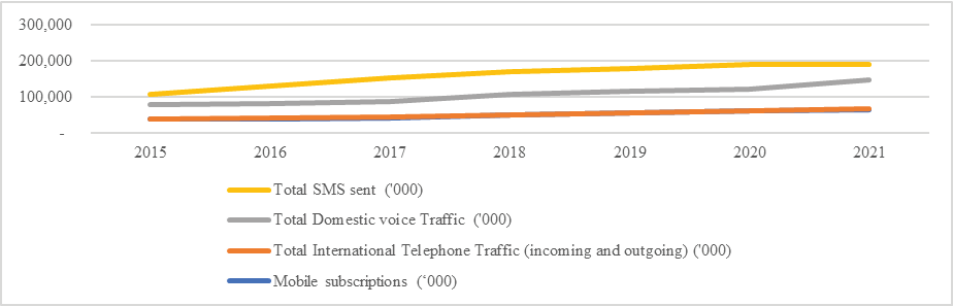
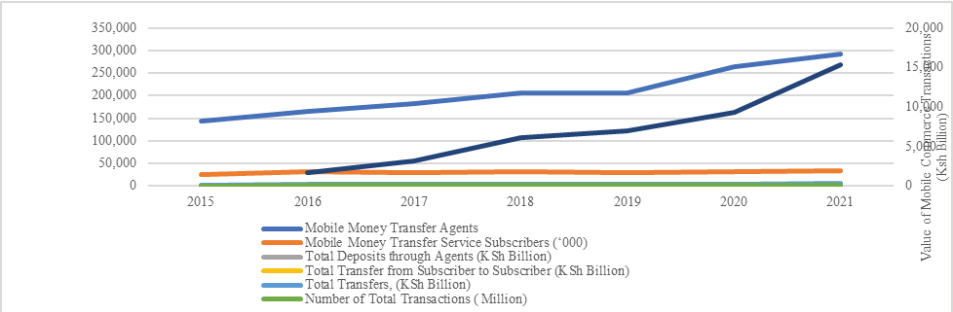


Figure 4.6: Cellular services subscriptions



Source: KNBS (Various), Economic Survey

Figure 4.7: Mobile money services



Source: KNBS (Various), Economic Survey

4.4.4 Data centres

A data centre is a facility that provides shared access to applications and data using a complex network, computer, and storage infrastructure. A data centre is a lifeblood of the digital economy and consists of large groups of networked computer systems and servers used by governments, companies, and individuals to remotely store, process, and distribute vast amounts of data. Domestic storage aims to increase control over citizen data by bringing decision making and access rights within jurisdictional boundaries. According to the Kenya Data Centre market research report (Research and Markets, 2021), Kenya is a major data centre market in Africa and is considered the gateway to the East African region. Kenya has 9 existing data centres spread across Nairobi (6) and other cities (3). Further, there are 2 upcoming data centre facilities.

The government has established a Tier-2 Government Data Centre to ensure the security of Government data, applications, and hosting of government critical data. The Government Data Centre houses the power, storage, and applications of the most critical and sensitive data and information necessary to support government services. Through this centralization, Government data is easy to access and is protected from natural or man-made disasters that may occur at the primary service sites/Government offices. Notably, the Government Data Centre is connected to the Government Common Core Network (GCCN) with high-speed connection links for faster access. In addition, the Government has established the National Data Centre at Konza Technopolis, a cloud-based, tier 3 data centre that is set to play a key role in the digital government agenda. The National Data Centre is worth US$ 30 million investment, expected to support the digital economy by offering storage capacity to the massive data in Kenya. The National Data Centre is connected to all major optic cables and strategically positioned as the first Data Centre from the landing station in Mombasa. The construction and equipping of the National Data Centre at Konza for phase 1 is complete and the Data Centre has not only started hosting services for some government agencies but is also playing a key role of an offsite DR site. The national Data Centre has established linkages with most service providers to power both public and private corporation's data centre needs.

Overall, the data centre market size in Kenya is expected to grow at 12 per cent during the period 2020-2026. The key factors contributing to the growth of data centres include the presidential directive to all ministries to digitize their public services, increased adoption of 3rd, 4th and 5th Generation services, increased fibre connectivity at home and office, wide adoption of cloud services and emerging technologies such as big data and Internet of Things (IoT), and the shift from on-premises to co-location and managed facilities by many organizations. Kenya's data market is dominated by global operators that have acquired or partnered with the local operators, for instance, icolo.io (Digital Realty), Africa Data Centres (Liquid Telecom), Pan African IX (PAIX) Data Centres, Safaricom, and Telkom Kenya. Notably, Huawei Technologies have modular data centre space with multiple efficient and reliable deployments. In addition, the Kenya Education Network (KENET) operates three cloud data centres that host the network

equipment that provide broadband connectivity and community cloud services to the KENET member institutions. These services include co-location services, storage as a service and hosting services on dedicated virtual private servers such as hosting of e-learning systems (KENET, 2021).

Some data centre vendors such as IXAfrica, PAIX, Teraco Data Environments, and Wingu have taken precautionary measures to reduce disruptions in their supply chain operations and use rack and blade servers from Cisco Systems, HPE, Dell Technologies, IBM, and Lenovo (Research and Markets, 2021). Kenya has only four facilities certified by Uptime Institute as Tier III standard facilities. Some of the key issues in the data centre space include that most facilities are based in Nairobi, leaving many cities and towns without data centre services. Other issues include: costly services offered by data centres, low number of certified data centres, low human capacity in data centre management, and costly and unreliable sources of power for data centres. Further, the development of local data centres is hampered by high cost of digital, electrical and mechanical infrastructure and construction costs.

4.4.5 Spatial infrastructure

Spatial infrastructure refers to a geospatial data infrastructure that implements a framework of geographic data, meta data, users, and tools that are interactively connected to use spatial data in an efficient and flexible way. Kenya has initiated efforts to strengthen the adoption of digital economy, which stands at US$ 7.42 billion based on e-conomy Africa report of 2020 by International Finance Corporation as shown in Figure 4.8. For instance, the government is implementing a National Addressing System (NAS) to guide the naming and numbering of streets and properties to facilitate easy identification and location on the ground. The addresses generated by the NAS system are part of personal data that require protection. NAS system guides the development of digitized maps for use in the management of settlements and urban communities. The potential benefits of NAS to citizens and businesses include unlocking economic value, job creation, and improved navigation. NAS system will accelerate the growth of e-commerce and associated industries with a commensurate positive impact on the economy by enabling easier geo-location for various service providers such as taxi, mail and home delivery of goods and services.

The implementation of NAS started in 2014 and the following milestones have been achieved: Drafting of NAS policy, National and County NAS bill and drafting of the NAS database framework. However, the implementation of the NAS system has been slow due to various reasons. Some of the key challenges that could impede the implementation of the NAS system include the protection of personal data. Further, a nationwide NAS implementation will require the coordination of actors at the national, county, and sub-county levels. Other challenges include outdated and scarce datasets, inadequate funding, and lack of formalized policies to manage spatial data. Implementation in rural and informal settlement areas will pose a more significant challenge compared to urban areas given the difficulty of access,

long distances, unnamed roads, uneven settlement patterns, and temporary settlements in some counties. Existing challenges also provide opportunities to Kenya's innovative talent to develop homegrown solutions that leverage on technology and crowdsourcing capacities to fast-track the implementation process and thus support the development of the data economy.

Figure 4.8: iGDP in Africa

iGDP Potential

Country	2020 ($B)	2020 (%)	2025 ($B)	2025 (%)	2050 ($B)	2050 (%)
Kenya	7.42	7.70%	12.84	9.24%	51.07	15.17%
Morocco	7.80	6.82%	12.09	7.84%	48.06	12.88%
South Africa	21.55	6.51%	31.45	7.86%	125.08	12.92%
Senegal	1.51	6.22%	2.92	7.11%	11.61	11.68%
Nigeria	24.59	5.68%	36.53	6.86%	145.28	11.27%
Algeria	9.02	5.60%	11.92	6.16%	47.39	10.12%
Cameroon	2.06	5.39%	3.27	6.19%	13.00	10.16%
Côte d'Ivoire	3.18	5.27%	5.53	6.04%	21.98	9.92%
Egypt	15.41	4.98%	25.97	5.99%	103.29	9.83%
Rwanda	0.52	4.98%	0.97	5.96%	3.85	9.79%

Source: e-conomy Africa report (2020)

4.4.6 Cybersecurity initiatives

Cybersecurity initiatives refer to policy efforts to protect, detect, respond, and recover from cyber-attacks, including Computer Emergency Response Team, National Public Key Infrastructure (NPKI). The dynamic and expansive nature and application of digital technologies in processing personal data has created a wide range of challenges in cyberspace. As a result, Kenya's personal data sector now faces constant cyberattacks attributed to well-organized and determined adversaries that continuously produce new tools and tactics of launching attacks. These attacks include but are not limited to phishing, Denial of Services (DoS), sabotage attacks on critical infrastructure, malware distribution, identity theft, electronic fraud, and other forms of cyber espionage activities. To address cyber threats that pose a challenge to the development of the data economy, Kenya has made significant efforts to secure personal data. The efforts include various policy and technical cybersecurity initiatives to deter and mitigate against all forms of cyber-attacks. For instance, the government has developed and enacted various policy, legal and regulatory frameworks aimed at leveraging the opportunities of digital transformation to improve Kenya's economic development while ensuring digital safety of its people, businesses, and interests. Some of the key policies, legal and regulatory frameworks include: Kenya Information and Communications Act of 1998; Computer Misuse and Cybercrimes Act (CMCA) of 2018; Data Protection Act (DPA) of 2019; National Cybersecurity Strategy of 2022; National Broadband Strategy of 2018; National ICT Policy Guidelines of 2020; and National Digital Master Plan of 2022.

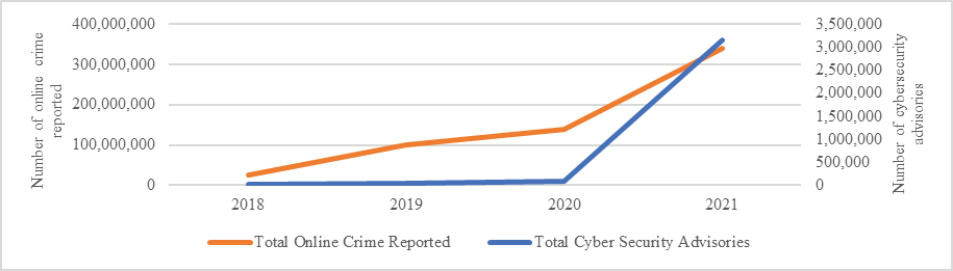
The current National Cybersecurity Strategy of 2022 roots for development of a robust local data economy. Among the national cybersecurity priorities identified

in the Strategy include enhancing the cybersecurity governance; protection of critical information infrastructure; enhancing cybersecurity capability and capacity building; building cybersecurity risks and cybercrime management; and strengthening of cooperation and collaboration. Other key policy initiatives supporting the protection of personal data include the establishment of National Computer and Cybercrimes Coordination Committee (NC4) and its Secretariat that act as the national body to spearhead and coordinate cybersecurity matters. The Committee comprises of the Principal Secretary in charge of internal security, Principal Secretary in charge of ICT, Attorney-General (AG), Chief of the Kenya Defence Forces (CDF), Inspector General of the National Police Service, Director-General of the National Intelligence Service, Director-General Communications Authority, Director of Public Prosecutions (DPP), Governor Central Bank of Kenya, and Director NC4 Secretariat. In addition, Kenya has established the Kenya Computer Incident Response Team and coordination Centre (KE-CIRT/CC) and the National Digital Forensics Laboratory at the National Police Service under the Directorate of Criminal Investigations (DCI). Further, the Communications Authority is implementing the National Public Key Infrastructure (NPKI) to enhance cybersecurity for digital transactions, which is critical for the data economy.

To protect the critical data systems as provided by the Computer Misuse and Cybercrimes Act (CMCA) of 2018 and Data Protection Act of 2019, the Government has designated sectors and critical systems that facilitate the provision of essential services and any other system that is strategic to the national security as Critical Information Infrastructures (CIIs) vide the Gazette Notice No. 1043 of 31st January, 2022. These are systems whose disruption would result in: interruption of life sustaining service; an adverse effect on the economy of the country; an event that would result in massive casualties or fatalities; failure or disruption of money market of the country; and adverse and severe effect on the security of Kenya including intelligence and military services. This affirms Kenya's commitment to safeguard and protect Kenya's sovereignty on data systems.

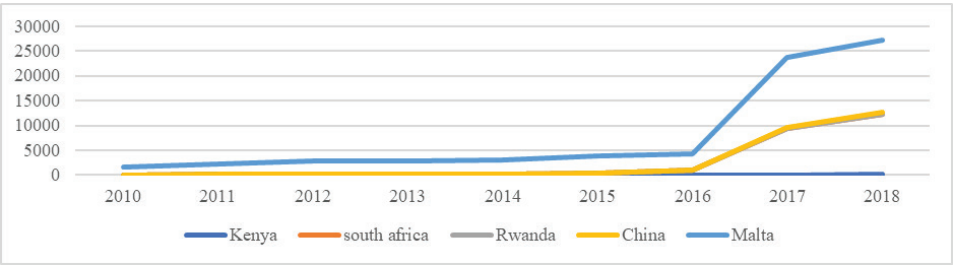
Despite the above policy progress, statistics from the KE-CIRT Coordination Centre cybersecurity indicate that the number of cyber threats detected in Kenya has significantly increased in the last few years. For instance, 339,066,637 cyber threats were detected in 2021 as compared to 25,475,013 threats detected in 2018 (see Figure 4.9). It is noted that Kenya does not have adequate capacity to offer cybersecurity advisories to increased number of threats detected in the recent years. Similarly, Figure 4.10 shows that Kenya is still lagging other leading digital economies in cybersecurity.

Figure 4.9: Total cyber threats in Kenya



Source: Communications Authority reports (various CA sector statistics)

Figure 4.10: Number of secure Internet servers



Source: World Bank dataset

The analysis of the delivery pillar indicates that Kenya has seen increased number of data subjects in form of subscribers of digital services and, consequently, the amount of personal data has significantly increased. Similarly, the number of data handlers including data controllers, data processors and data distributors have increased due to demand for digital services. To create a conducive environment at the delivery layer, Kenya has put in place policy, legal and technical initiatives to support the development of the data economy. This is key to making Kenya meet the goal of 80 per cent of Internet traffic locally accessible against 20 percent international traffic. This would make Kenya accelerate its path towards data localization since Kenya will not just be an 'Internet Consumer' but an 'Internet Creator' (Internet Society, 2017). Some of the remarkable efforts put in place include the formulation of Data standards, Data architecture, Data technology, Local systems, Data infrastructure, and Data security to support the building of data sovereignty in Kenya. As noted earlier, Kenya has the biggest digital economy in Africa with projection that it will account for over 15 per cent of Africa's digital economy by 2050. This presents an enormous opportunity for the country to strengthen the delivery pillar in supporting the growth of the data economy. Although much progress has been made, Kenya still faces several challenges in its delivery pillar; these include inadequate digital infrastructure due to limited coverage of national fibre infrastructure and limited Internet penetration,

especially in the rural areas. The existing capacity of the digital network is not able to serve all the government needs and the private sector.

Other challenges that may hamper the building of data localization under the delivery pillar include frequent fibre cuts and destruction of telecommunication infrastructure, limited last mile infrastructure connectivity leading to limited and high-cost Internet access by government institutions, homes, schools, and social centres. Further, the delivery pillar is associated with challenges that include low uptake of ICT standards and some organizations have not invested in the necessary controls to protect personal data. In terms of data storage, Kenya has only four facilities certified by Uptime Institute as Tier III standard facilities, and this leaves many cities and towns without quality data centre services. Other issues associated with data centres include costly services offered by local data centres, low number of certified data centres, inadequate human capacity in data centres, and costly and unreliable sources of power for data centres. Further, the development of local data centres is hampered by the high cost of digital, electrical, and mechanical infrastructure and construction costs. Finally, cybersecurity challenges continue to threaten personal data through banking/finance frauds, sim swaps and online scams such as digital Ponzi schemes, job scams, fake websites and lotteries, crypto and forex scams, "Tuma kwa Hii Namba" syndicates, among others.

4.4.7 Comparison of Kenya and selected countries on various elements of the Delivery Pillar

Table 4.10: Comparison of elements of delivery pillar across selected countries

Policy Element	Guidelines				Policies				Acts/Laws/ Regulations			
Countries	K	U	N	A	K	U	N	A	K	U	N	A
Data generation and collection systems	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
Internet infrastructure	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Cellular infrastructure or mobile network	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Data centre	Y	Y	Y	Y	Y	N	N	Y	N	Y	Y	Y
Spatial infrastructure	Y	Y	Y	Y	Y	N	Y	Y	N	N	N	Y
Cybersecurity initiatives	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y

NB: K=Kenya, U=Uganda, N=Nigeria, A=Australia Y=Yes N=No

Based on the analysis on Table 4.10 in the Delivery layer, Kenya has put in place various initiatives to build digital capacity in terms of data management systems; Internet infrastructure; Cellular infrastructure; Data centres, Spatial infrastructures; and Cybersecurity initiatives. As a result, Kenya has demonstrated better performance at the global level in the development of digital capacity to support the implementation of data localization as compared to other African countries as demonstrated by high rankings across various indices on digital initiatives. For instance, Kenya has higher number of secure servers, data centres, high mobile and Internet penetration rates, indicating a strong foundation for building data localization in the country. Based on the Internet Privacy Index score, Kenya and Australia scored 25 each, indicating a promising data ecosystem in Kenya while Estonia is ranked first with 37 points out of 40. However, as noted earlier, Kenya still experiences challenges such as digital divide, high Internet cost, costly devices, fewer certified data centres and increasing cyber threats. Kenya not only has low uptake of local data storage services but also lacks smart data centres to host local and international Internet Exchange and Content Delivery Networks (CDN). Unlike developed data economies such as Australia and Estonia, Kenya does not have a comprehensive data localization framework on digital infrastructure to protect national critical sovereign data and hosting arrangements that store, protect and manage personal data. For instance, Australia has established a data localization framework for its digital infrastructure that ensures data centres are only controlled and accessed by the Australian government security-cleared personnel. Further, all data facilities are required to continually measure up against rigorous global certification standards in terms of mechanics, engineering and build to host critical information. Australia has prioritized local cloud and data storage service providers to provide world-class security for Australia's sovereign data. Estonia has established a Data Embassy to provide the server space for a data-storage cloud. Estonia has demonstrated the technical capability to not only host but also build and operate a variety of complex high-tech systems. The country maintains a robust system of servers within its territory, meant to support its e-governance operations in case one or several are knocked out by either a cyber- or physical attack. Finally, some countries including the UAE offer incentives for digital infrastructure such as creation of special economic or sector free zones such as Dubai International Financial Centre, the Abu Dhabi Global Market (ADGM) and the Dubai Health Care City.

4.5 Possible Effects of Data Localization in Kenya

As Kenya implements the data protection regulations particularly on data localization, it is expected that there are possible effects on the economy ranging from regaining sovereignty over its data to creating job opportunities. Research studies show that data localization measures may affect the cross-border data flows and thus impact on an array of economic sectors such as finance, transport, communication, automotive, energy, health, commerce, and entertainment businesses and public service organizations (Summer, Rene, 2013). These data localization measures cast a shadow on many sectors and players and therefore

data localization measures such as the one in Kenya is likely to reduce cross-border data transfer. Data protection laws not only effect the processing of personal data of all companies practicing business globally but also impact pure-play technology companies that are involved in production and innovation, thus impacting the competitiveness of such technology companies (Matthieu Pelissie du Rausas et al., 2011). Kenya's data protection regulations require strategic personal data to be processed in the local data centres or copies of certain data be preserved in local servers without prohibiting such data from moving out of the country. The data protection laws may bring uncertainties, operational difficulties, and increased costs in processing personal data. If not well implemented, data localization regulations may raise the costs of doing business and make transferring of data across borders unattractive or at times impossible, therefore acting as a trade barrier. Therefore, there is need to put in place a well thought out data localization framework to ensure data localization measures serve as incentives to build robust local data economy.

4.6 Lessons for Kenya

Globally, there is a growing interest in carrying out comprehensive research on data localization and its impact on businesses, legal and compliance professionals. This section highlights some key lessons Kenya can learn from various countries that have adopted data localization measures.

- One of the benefits arising from data localization regulations is the achievement of data sovereignty since the critical personal data can only be collected, used, and stored locally. This is a step forward from being trapped in data colonialism. Kenya would be a better position to control how critical personal data is created, used, and stored. Investing in data localization regulations to restrict processing of data would give Kenya an absolute sovereignty over its personal data. Data localization offers an opportunity to protect national data of all kinds, related to national security, governmental functions, financial functions, business and civil society, and personal data on many citizens. The available literature is not adequate to firmly conclude that data localization is the best option to safeguard personal data. However, the available literature indicates there has been success in eliminating data breaches that will involve personal data kept in vulnerable data storage systems located in foreign countries. As noted earlier, many companies globally do not adequately invest in cyber security and hence restricting cross border data flow reduces the exposure of such data in foreign countries. Additional complimentary cyber security solutions would strengthen local cyber defense against data breaches.
- With revelations of various foreign surveillance programmes and other secrets by Snowden, many governments are aware of the need to control how their critical data is shared and stored. Snowden revealed the mostly unconstrained exercise of hegemonic power and the enormous possibilities for data gathering, data analysis and data control by intelligence agencies and tech companies in the United States and other Western countries. The existence of surveillance

programmes has triggered the need to adopt data localization measures. Research has shown that imposing restriction on transfer of personal data to other jurisdictions can significantly reduce exposure to cross border threats. Further, a requirement to store personal data locally would facilitate the law enforcement agencies' efforts to easily access information required for the detection of crime and in gathering evidence for prosecution as compared to waiting for responses to requests made to foreign entities storing data abroad. Mutual Legal Assistance Treaty (MLAT) is applied to request data kept in a different jurisdiction and is often slow and cumbersome. Kenya made its last request under the Mutual Legal Assistance Treaty (MLAT) for evidence stored in the US servers in 2017. The long delays witnessed in getting evidence from foreign countries has delayed the finalization of several cybercrime cases in the Kenyan courts.

- Implementation of data localization measures will promote the investment of local digital infrastructure to collect, process and store personal data. For instance, Iran, Vietnam, and China require all data processing to happen locally and therefore entities are compelled to build local data centres. Data localization is an effective and convenient strategy for gaining a competitive advantage in domestic digital economy long dominated by developed countries. For instance, data localization in Germany presents clear economic benefits with adoption of "email made in Germany" system, the "Schengen area routing" arrangement and cloud computing. Brazil, South Korea, Indonesia, and India are also benefiting economically from data localization laws. In the long run, data localization will promote growth of local industries, hire more people, bring in more innovations and build data sovereignty.
- Emerging technologies such as Artificial Intelligence are increasingly being used to process personal data globally. Artificial Intelligence has given rise to intelligent tools that generate and process personal data across multiple business applications. If not well controlled, generative Artificial Intelligence poses a significant risk to the privacy of personal data. This has seen various countries including the USA, EU and China formulate and implement policy and legal frameworks to guide ethical use of generative Artificial Intelligence. Kenya does not have a policy and legal framework to steer the development of the data economy.
- Although data localization has many benefits, it may increase the cost of doing business in the early years. Data needs to flow to maximize value, which means policies that limit such flows across borders will reduce the economic growth and social value. At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on digital services. Companies are likely to pay more for data storage services, especially those in smaller countries (which will not naturally be home to a data centre). The reviewed research strongly indicates that there is considerable negative impact of data localization on overall domestic investments, causing lower economic growth and reduced exports. Restrictions on cross-border data flows harm both the competitiveness of the country implementing the policies and other countries. Every time one country erects barriers to data

flows, another country that relies on these data flows is also affected (Badran, 2018).

- Data localization is normally termed as Digital Protectionism and this is meant to protect domestic businesses from foreign competition. Technology firms from developed countries stand to lose customers and contracts because of data localization policies. Foreign companies will eventually shy away from entering markets where data localization laws apply to avoid additional costs and taxation.
- Data localization policies could have the effect of fragmenting the Internet, thus turning back the clock on the integration of global communication and e-commerce, and putting into jeopardy the myriads of societal benefits that Internet integration has engendered. Further, some countries seem to believe that personal data will be safer at home; however, countries with isolated or outdated technology are less able to protect locally stored data against foreign military and criminal threats. Furthermore, an isolationist mentality around cybersecurity can undermine access to state-of-the-art solutions.
- Data localization has been used in China, Iran, Egypt, and other authoritarian States to ease the technical burdens required to exert control over Internet platforms, such as Facebook, which those governments find to be hosting unwanted political speech, or facilitating political dissent (Hill, 2014).

5. Conclusion and Recommendations

The ever-growing nature of digital network and digital applications and communication practices have significantly reduced the legal governance and control of data by governments. Further, with revelations of various foreign surveillance programmes and other secrets by Snowden, many governments are aware of the need to control how their personal data is processed. Snowden revealed the mostly unconstrained exercise of hegemonic power and the enormous possibilities for data gathering, data analysis and data control by intelligence agencies and technology companies in the United States and other Western countries. As a result, data localization is a common term in political discourse to reinstate the sovereignty over the use of data in supporting social and economic activities. In a world where access to data is essential for a thriving digital economy, concerns are emerging around privacy, national security, business continuity and data breaches, thus countries are increasingly demonstrating an appetite to restrict the processing of personal data. Data localization is perceived as a gap-filling claim for authority and control over personal data.

Although data localization measures are often seen as protectionist, countries such as Kenya could still harness many benefits if Kenya develops a comprehensive data localization framework along the three pillars (Strategic, Tactic and Delivery), which are the cornerstone of data sovereignty. As noted in the study, Kenya has made significant efforts in formulating and implementing policy, legal and technical initiatives to support the development and growth of the data economy. While the prerequisites for data localization have been established in the country, there are various gaps that require to be addressed.

At the tactic pillar, Kenya has low digital skilled experts possessing advanced digital skills for the data economy. High-end digital skills are essential and, therefore, building digital skills is key to facilitating a vibrant data economy.

While at the delivery pillar, Kenya still faces several challenges that largely include inadequate digital infrastructure that contributes to the digital divide manifested by low Internet penetration in unserved and underserved areas. The capacity of the digital network is not adequate to serve all the digital needs for the public and private sectors. Other issues include costly services offered by local data centres, low number of certified data centres, inadequate human capacity in data centre, costly and unreliable sources of power for data centres.

5.1 Conclusions

- Strategic pillar

Kenya's data localization regulations are less strict, not fully implemented and are barely two years old. The budget allocation for Kenya's data protection regulator is significantly less as compared to other jurisdictions. There are also several gaps that require policy interventions such as absence of a national comprehensive data management policy and supporting policies, strategies, and procedures to provide a roadmap of how data initiatives are to be rolled out in the data economy. It is

also noted that the office of the Data Protection Commissioner is yet to enforce mechanisms to support data localization in the country. Currently, the Office is focusing on creating awareness on the Data Protection Act and registration of entities (data controllers and data processors) dealing with personal data. Further, there are many actors across all sectors dealing with personal data, spanning from public sector, private sector to community-based organizations and therefore would require a robust mechanism to ensure effective application of the data localization measures in the country. Finally, most of the personal data is being processed outside of the country because of superior data products offered at a lower cost, and therefore favourable for most businesses. There is need to build adequate local infrastructure such as data centres to support local processing of data to build sovereignty for personal data.

- **Tactical pillar**

Based on the analysis on the Tactical layer, Kenya has put in place various initiatives to build the capacity required to support the implementation of data localization in the country. As a result, Kenya has demonstrated better performance at the global level in the development of digital skills as compared to other African countries. Notably, Kenya recorded impressive performance in terms of availability of scientists and engineers, Government success in ICT promotion as well as ease of finding skilled employees in the job market, which are key in the development of the prerequisite digital skills for building a successful data economy. However, there are several gaps in developing the necessary capacity that require policy interventions. Kenya did not perform well in having workforce with global science and technology skills, which is a barrier in progressing the data economy. Kenya has low and intermediate digital skilled experts with few professionals possessing advanced digital skills. High-end digital skills are essential, and therefore building digital skills is key to leveraging on the emerging technologies to facilitate a vibrant personal data economy. To address the technical skills in the country, most firms prefer sourcing the skills from outside the country. Further, most graduating students who complete their formal education do not receive practical skills that are required when joining employment in public and private entities, including the startups and innovations for personal data economy.

- **Delivery pillar**

Kenya has put in place various initiatives to build digital capacity in terms of data management systems; Internet infrastructure; Cellular infrastructure; Data centres, Spatial infrastructures, and Cybersecurity initiatives. As a result, Kenya has demonstrated better performance at the global level in the development of digital capacity to support the implementation of data localization as compared to other African countries, and as demonstrated by high rankings across various indices on digital initiatives. However, as noted earlier, Kenya still experiences challenges such as digital divide, high Internet cost, costly devices, fewer certified data centres and increasing cyber threats. Kenya not only has low uptake of local data storage services but also lacks smart data centres to host local and international Internet Exchange and Content Delivery Networks (CDN). Unlike developed data economies such as Australia and Estonia, Kenya does not have a

comprehensive data localization framework on digital infrastructure to protect national critical sovereign data and hosting arrangements that store, protect and manage personal data.

5.2 Recommendations

For data localization and sovereignty to thrive in Kenya, it is critical to make careful considerations along the three pillars. A well thought out data sovereignty framework would spur growth and development of the local data economy. The following are the key recommendations:

- **Strategic pillar**
  - Formulate and implement a national comprehensive data management policy framework to provide strategic direction on processing of data
  - Formulate supporting data sovereignty policies and procedures to guide the processing of personal data
  - Enhance awareness among data controllers, data processors and data subjects on the importance of privacy and data protection
  - Strengthen sector-based approach to protect and safeguard data privacy
  - Prioritize to localize certain categories of personal data for critical sectors before embarking on massive data localization across all sectors
  - Formulate a national strategy and guidelines for application of emerging technologies such as artificial intelligence on personal data for a thriving data economy
  - Provide more resources to support key data localization activities including creating awareness
- **Tactical pillar**
  - Build digital skills on the emerging technologies to facilitate development of a vibrant personal data economy
  - Support learning institutions to align their curriculum to industry needs to produce well prepared graduates for the data economy
  - Partner with professional bodies to mentor students
  - Develop and implement a comprehensive policy framework to support identification, nurturing and scaling up of startups and innovations for the data economy
  - Fast-track the development of two software development firms as indicated in the National Digital Masterplan
- **Delivery pillar**
  - Fast-track the full completion of the National Data Centre

- Partner with the private sector to build more data centres across the country
- Tap on the Universal Service Fund to support the development of key infrastructure connectivity projects in the unserved and underserved areas
- Provide incentives such as basic infrastructure and economic special zones for digital infrastructure providers – power, water, and road to encourage investors build more data centres
- Fast-track the establishment of 25,000 Internet-hotspots across the country to provide Internet services to innovators, youth and entrepreneurs
- Effective campaigns for Kenyan data platforms, products, content, and services including .KE
- Roll out programmes to accelerate generation and uptake of local content through the creative economy

References

Aaronson, S. (2015), "Why are trade Agreements not setting information free: The lost History and reinvigorated Debate over cross-border data flows, Human rights, and national security?" World Trade Review.

Aaronson, S.A. (2021), Data is disruptive: How data sovereignty is challenging data governance. Heinrich Foundation.

Acquisti, A. and College, H. (2010), The economics of personal data and the economics of privacy. The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines. OECD Conference Centre.

Australian Government (2017), Strengthening the national security of Australia's critical infrastructure. Australia: Critical Infrastructure Centre.

Azmeh, S., Foster, C. and Rabuh, A.A. (2021), *The rise of the data economy and policy strategies for digital development*. Oxford: Digital Pathways at Oxford Paper Series.

Badran, M.F. (2018), "Economic impact of data localization in five selected African countries". *Digital Policy, Regulation and Governance*, 337-357.

Ball, J. (2013), NSA's Prism surveillance program: How it works and what it can do. Retrieved from The guardian: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

Banks, W.C. (2017), "Cyber espionage and electronic surveillance: Beyond the media coverage". *Emory Law Journal*, 513-525.

Barkan, S. (2006), *Criminology: A sociological understanding (3rd ed)*. Upper Saddle River, NJ: Prentice Hall.

Bauer, M., Ferracane, M. and Marel, E. (2016), Tracing the economic impact of regulations on the free flow of data and data localization. Global Commission on Internet Governance.

Bhutia, J. (2015). Isis 'Cyber Caliphate' Hacks More than 54,000 Twitter Accounts. Retrieved from International Business Times: http://www.ibtimes.co.uk/isis-cyber-caliphate-hacks-more-54000-twitter-accounts-1527821.

Boos, E., Givens, C. and Larry, N. (2014), "Damages theories in data breach litigation". SSRN.

Bosslera, A. M. and Berenblum, T. (2019), "Introduction: New directions in cybercrime research". *Journal of Crime and Justice*, 495-499.

Budanović, N. (2020), The largest battlefield in history – 30 Cyber warfare statistics. Retrieved from Dataprot: https://dataprot.net/statistics/cyber-warfare-statistics/.

Buguroo (2020), Opportunity makes the cybercriminal. Retrieved from Buguroo: https://www.buguroo.com/en/blog/opportunity-makes-the-cybercriminal.

CheckPoint (2020), *Cybersecurity Report 2020*. Tel Aviv: Checkpoint.

CNN (2015), CNN Staff, CENTCOM Twitter Account Hacked, Suspended, CNN Politics. Retrieved from CNN: http://www.cnn.com/2015/01/12/politics/centcom-twitter-hacked-suspended/.

Crowdstrike (2020), Global Threat Report. United States of America: Crowdstrike.

Cybersecurity Ventures (2019), 2019 Official Annual Cybercrime Report. Herjavec Group.

Das, S. and Nayak, T. (2013), "Impact of cyber crime: Issues and challenges". *International Journal of Engineering Sciences and Emerging Technologies*, Vol. 6, Issue 2: 142-153.

Davis, M. (2020), Damaging after-effects of a data breach. Retrieved from Cybint: https://www.cybintsolutions.com/4-damaging-after-effects-of-a-data-breach/

Deibert, R. (2013), *Black code: Inside the battle for cyberspace*. Toronto: McClelland and Stewart.

Deloitte (2017), *Privacy is paramount: Personal data protection in Africa*. Johannesburg: Deloitte.

DeNardis, L. (2014), *The global war for Internet governance*. New Haven, CT: Yale University Press.

Department of Justice (2021), The USA PATRIOT Act. Retrieved from The USA PATRIOT Act: https://www.justice.gov/archive/ll/highlights.htm.

European Union (2021), GDPR. Retrieved from GDPR: https://gdpr.eu/

FBI (2016), Cyber's most wanted. Retrieved from Federal Bureau of Investigation: https://www.fbi.gov/wanted/cyber.

Filkins, B., McMillan, R. and Carson, B. (2017), "Effective cybersecurity begins with identifying and prioritizing critical data assets". Basingstoke, UK: Intellsecure, Inc.

Fuchs, C. (2010), "Web 2.0, prosumption, and surveillance". *Surveillance and Society*, 288-309.

Government of Kenya (2021). Data Protection Regulations. Kenya Gazette.

Great (2019), APT trends report Q1 2019. Retrieved from Securelist: https://securelist.com/apt-trends-report-q1-2019/90643/.

Greenwald, G. (2014), *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. New York, NY: Metropolitan Books.

Greenwald, G. and MacAskill, E. (2013), NSA Prism programme. Retrieved from *The Guardian*: NSA Prism programme taps into user data of Apple, Google, and others: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Gu, Y., Madio, L. and Reggiani, C. (2019), Data brokers co-opetition. Working Paper No. 7523 Category 14: Economics of Digitization. CESifo.

Haber, E. and Zarsky, T. (2017), Cybersecurity for infrastructure: A critical analysis. Florida State University Law Review, Florida State University Law Review.

Haley, C. (2013), "A theory of cyber deterrence". *Georgetown Journal of International Affairs*.

Hill, J. (2014), The growth of data localization post-Snowden: Analysis and recommendations for US policy makers and business leaders. Conference on the Future of Cyber Governance. The Hague, Netherlands: The Hague Institute for Global Justice.

IBM Security (2019), Cost of a data breach report. Michigan: Ponemon Institute LLC.

IFC (2020). e-Conomy Africa 2020. e-Conomy Africa 2020.

Internet Society (2017), *Interconnection and traffic exchange*. Geneva: Internet Society.

ITU (2019). *Global Cybersecurity Index (GCI)*. Geneva: International Telecommunication Union.

Jacobs, A.J. and Helft, M. (2010), Google, citing attack, threatens to exit China. Retrieved from The New York Times: http://www.nytimes.com/2010/01/13/world/asia/13beijing.html.

Karuppannan, J. (2008), Space transition theory of cyber crimes. Pearson.

Kaspersky (2020), What is a data breach? Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/data-breach.

Kende, M. (2020), Anchoring the African Internet ecosystem: Lessons from Kenya and Nigeria's Internet exchange point growth. Internet Society. Retrieved from https://www.internetsociety.org/resources/doc/2020/ixp-report-2020/

KENET (2021), Data centre cloud services. Retrieved from KENET: https://www.kenet.or.ke/content/data-centre-cloud-services.

Kenya Law (2019), The Data Protection Act. Nairobi: Kenya Gazette.

Law Insider (2023), Data protection. Retrieved from Data Protection definition: https://www.lawinsider.com/dictionary/data-protection.

Lee, T.B. (2014). 40 maps that explain the Internet. Retrieved from Vox: https://www.vox.com/a/internet-maps#list-28.

Leukfeldt, E. R. and Yar, M. (2016). "Applying routine activity theory to cybercrime: A theoretical and empirical analysis". *Deviant Behaviour*, 263-280.

Lis, P. and Mendel, J. (2019), "Cyberattacks on critical infrastructure: An economic perspective". *Economic and Business Review*, 24-47.

Macquarie Government (2023), Data sovereignty. Retrieved from Data Sovereignty: https://macquariegovernment.com/data-sovereignty/.

Mandelcorn, S., Modarre, M. and Mosleh, A. (2013), An explanatory model of cyber-attacks drawn from rational choice theory. Proceedings of the American Nuclear Society Meeting on Risk Management for Complex Socio-Technical Systems (RM4CSS). Washington, DC: Transactions of the American Nuclear Society.

Markets and Markets (2020), Cloud computing market. Retrieved from https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html.

Martin, B.A. (2020), "The unregulated underground market for your data: Providing adequate protections for consumer privacy in the modern era". "IOWA Law Review", 865-900.

Micheli, M., Ponti, M., Craglia, M. and Suman, A.B. (2020), "Emerging models of data governance in the age of datafication". *Big Data and Society*.

Ministry of Children, Community and Social Services Ontario (2020). Rational Choice and Routine Activities Theory. Retrieved from Literature Review: http://www.children.gov.on.ca/htdocs/English/professionals/oyap/roots/volume5/chapter03_rational_choice.aspx#!

Ministry of ICT Kenya (2018), Data Protection Policy. Nairobi: Ministry of ICT Kenya.

Moher, D., Liberati, A., Tetzlaff, J., Altmen, D. and Group, T.P. (2009), "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement". *Plos Medicine*.

Mueller, M. (2010), *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Nigel, C. (2017), Cross-border data flows: Where are the barriers, and what do they cost? Information Technology and Innovation Foundation.

OECD (2013), Exploring the economics of personal data: A survey of methodologies for measuring monetary value. OECD Digital Economy Papers.

OECD (2020), Personal data use in financial services and the role of financial education: A consumer-centric analysis. www.oecd.org/daf/fin/financial-education/Personal-Data-Use-in-Financial-Services-andthe-Role-of-Financial-Education.pdf.

OECD (2022), OECD iLibrary. Retrieved from The Path to Becoming a Data-Driven Public Sector: https://www.oecd-ilibrary.org/sites/9cada708-en/index.html?itemId=/content/component/9cada708-en.

Office of the Data Protection Commissioner (2021), Office of the Data Protection Commissioner of Kenya: Strategic Plan 2022/23-2024/25.

OWASP (2017), OWASP Top 10 vulnerabilities. OWASP.

Piquero, L., Lyn, E. and Simpson, S. (2005), "Integrating the desire-for-control and rational choice in a corporate crime context". *Justice Quarterly*, 252-280.

Pohle, J. and Thiel, T. (2020), "Digital sovereignty". *Journal on Internet Regulation*.

Research and Markets (2021), "Kenya data centre - Investment analysis and growth opportunities 2021-2026". *Research and Markets*.

Richardson, V., Smith, R. and Watson, M. (2019), "Much ado about nothing: The (lack of) economic impact of data privacy breaches". *Journal of Information Systems*, 227-265. Retrieved from Data Breach hurt the economy but not so much the average company: https://blogs.lse.ac.uk/businessreview/2019/10/24/data-breaches-hurt-the-economy-but-not-so-much-the-average-company/.

Sanger, D.E. (2014), With spy charges, US draws a line that few others recognize. Retrieved from *The New York Times*: http://www.nytimes.com/2014/05/20/us/us-treads-fine-line-in-fighting-chinese-espionage.html.

Sargsyan, T. (2016), "Data localization and the role of infrastructure for surveillance, privacy, and security". *International Journal of Communication*, 2221-2237.

Secure Controls Framework (2022), Secure controls framework. Retrieved from Security and Privacy Capability Maturity Model (SP-CMM): https://www.securecontrolsframework.com/sp-cmm.

Serianu (2018), Kenya Cyber Security report. Nairobi: Serianu Limited.

Singer, P.W. and Friedman, A. (2014), *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

Stallings, W. (2006), *Cryptography and network security*. New Jersey: Pearson Hall Press.

Statistica (2022), Amount of data created, consumed, and stored 2010-2025. Retrieved from https://www.statista.com/statistics/871513/worldwide-data-created/.

Strech, D. and Sofaer, N. (2011), "How to write a systematic review of reasons". *Journal of Medical Ethics*, 121-126.

Swinhoe, D. (2020), The 15 biggest data breaches of the 21st century. Retrieved from CSO: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Symanovich, S. (2020), Data breaches: What is a data breach and how do I handle one? Retrieved from Lifelock: https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html.

Symantec (2019), Internet security threat report. California: Symantec Corporation.

Symons, T. (2022), Me, my data, and I: The future of the personal data economy-2018. Retrieved from Europa: https://ec.europa.eu/jrc/communities/sites/default/files/24oct_02_symons_1.pdf.

Taylor, R.D. (2020), “Data localization: The Internet in the balance". *Telecommunications Policy*.

Technopedia (2023), Data localization. Retrieved from What Does Data Localization Mean? https://www.techopedia.com/definition/32506/data-localization.

The AME Group (2020), Data security breach: 5 consequences for your business. Retrieved from Security Breach: https://www.theamegroup.com/security-breach/.

Thielman, S. (2017), Tim Berners-Lee: selling private citizens' browsing data is 'disgusting'. Retrieved from The Gurdian: Technology: https://www.theguardian.com/technology/2017/apr/04/tim-berners-lee-online-privacy-interview-turing-award.

Turner, S. (1997), "Transnational corporations and the question of sovereignty: An alternative theoretical framework for the information age". *Southeastern Political Review*.

United Nations (2019), "Data economy: Radical transformation or dystopia?" *Frontier Technology Quarterly*.

UNODC (2020), Cyberespionage. Retrieved from UNODC: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html.

Vuleta, B. (2021), How much data is on the Internet + More stats: Editor’s choice. Retrieved from seedscientific: https://seedscientific.com/how-much-data-is-created-every-day/.

Wikipedia (2020), Cyberwarfare. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Cyberwarfare.

Wikipedia. (2021, April 14). CLOUD Act. Retrieved from CLOUD Act: https://en.wikipedia.org/wiki/CLOUD_Act

Wikipedia (2021), PRISM (surveillance program). Retrieved from PRISM (surveillance program): https://en.wikipedia.org/wiki/PRISM_(surveillance_program)

Wood, R. (2014), Ireland corks double Irish tax deal, closing time for Apple, Google, Twitter, Facebook. Retrieved from Forbes: http://www.forbes.com/sites/robertwood/2014/10/14/ireland-corks-double-irish-tax-deal-closing-time-for-apple-google-twitter-facebook/.

World Wide Web Foundation (2017), Personal data: An overview of low and middle-income countries. Washington: World Wide Web Foundation.

Wright Hassal (2020), Cyber security and data protection: Two sides of the same coin. Retrieved from wrighthassall: https://www.wrighthassall.co.uk/knowledge-base/cyber-security-and-data-protection-two-sides-of-the-same-coin.

Wu, E. (2021), *Sovereignty and data localization*. Massachusetts: Havard Kennedy School.

Appendix

Appendix A: Overview of legislative measures for the countries

Country	Law	Scope
Indonesia	• Law No. 11 regarding Electronic Information and Transaction of 2008 • Government Regulation No. 82 of 2012 regarding the Provision of Electronic System and Transaction • Draft Regulation with Technical Guidelines for Data Centres • Circular Letter of Bank Indonesia No. 16/11/DKSP of 2014 regarding E-money Operations	• Regulation 82 states that the storing of personal data and performing a transaction with the data of Indonesian nationals outside the Indonesian jurisdiction is restricted. This requirement would appear to apply particularly to personal data and transaction data of Indonesian nationals that is used within Indonesia and/or related to Indonesian nationals. • Regulation 82 requires "electronic systems operators for public service" to set up a data centre and disaster recovery centre in Indonesian territory for the purpose of law enforcement and data protection. • In the Annex of Circular Letter of Bank Indonesia No. 16/11/DKSP Year 2014 regarding E-money Operations, there is a requirement for all operators of e-money to localize data centres and data recovery centres within the territory of Indonesia.
Korea	• Regulations on Financial Institutions' Outsourcing of Data Processing Business and IT Facilities' approved in June 2013 • Spatial Data Industry Promotion Act	• Despite provisions in its free trade agreements with EU and US to allow sending financial data across borders, Korea still prohibits outsourcing of data-processing activities to third parties in the financial services industry. Banks can therefore only process financial information related to Korean customers in-house, either in Korea or abroad, and offshore outsourcing is restricted to a financial firm's head office, branch or affiliates. • Since June 2015, financial services institutions are allowed to offshore data processing to professional IT companies whose infrastructure is located outside of Korea. • Korea imposes a prohibition to store high-resolution imagery and related mapping data outside the country and justifies this restriction on security grounds.
Russia	• Federal Law No. 152-FZ "On Personal Data" as amended in July 2014 by Federal Law No. 242-FZ "On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks" • New provisions in the federal law on information, information technologies and protection of information (known as Blogger's Law) • Federal Law No. 319-FZ "On Amendments to the Federal Law on the National Payment System and Certain Legislative Acts of the Russian Federation"	• In accordance with the amendments to Federal Law No. 152-FZ of July 2006, an operator is required to ensure that the recording, systemization, accumulation, storage, clarification (updating, modification) and retrieval of Russian citizens' personal data is to be conducted only in databases located within Russia. • The law affects all business practices that involve the processing of personal data of Russian citizens, irrespective of whether companies have a physical presence in Russia. • Blogger's Law requires organizers of information distribution in the Internet (it is not clear which operators fall under this definition) to store on Russian territory information on facts of receiving, transfer, delivery and/or processing of voice information, texts, images, sounds and other electronic messages and information about users during 6 months from the end of these actions. • The amendments to the National Payment System Law require international payment cards to be processed locally.
Vietnam	• Decree No. 72/2013/ND-CP of July 15, 2013, on the Management, Provision and Use of Internet Services and Online Information	• The Decree No. 72/2013 entered info force in September 2013 establishes local server requirements for online social networks, general information websites, mobile telecoms network-based content services and online games services. • All these organizations are required to establish at least one server inside the country "serving the inspection, storage, and provision of information at the request of competent state management agencies."

Country	Law	Scope
Brazil	• Law No 12.965 (Macro Civil), passed in March 2014	• The Brazilian government considered requiring Internet Service Providers to store information regarding Brazilian users only on local servers. • The provision did not make it to the final version of Marco Civil.
China	• Various laws and guidelines, including Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems • Standing Committee of the National People's Congress in China Decision on Strengthening Protection of Online Information • Non-binding national standards related to personal information published by the Standardization Administration and the General Administration of Quality Supervision, Inspection, and Quarantine • People's Bank of China Notice to Urge Banking Financial Institutions to Protect Personal Financial Information (Notice) • China's Management Measures for Population Health Information	• A plethora of complex data privacy laws has made compliance very difficult for companies that collect personal information. • Cross-border data transfer restrictions are imposed by various industry guidelines for the information-services sector. These guidelines may serve as a "regulatory baseline" for law enforcement authorities to assess whether or not a business is in compliance with Chinese data privacy laws. • Banks and financial institutions are prohibited from storing, processing or analyzing any personal financial information outside China that has been collected in China. • Population health information needs to be stored and processed within China. In addition, storage is not allowed overseas. • Licensing system for online taxi companies that requires them to host user data on Chinese servers. • Online maps are required to set up their server inside of the country and must acquire an official certificate.
India	• Information Technology Act 2000 • Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 • National Security Council Secretariat proposal for data localization of email services	• With its "Reasonable Security Practices and Procedures," the Indian government introduced a strict consent requirement that only allows for sensitive personal data to be transferred abroad that is necessary for the performance of a lawful contract between the body corporate (or any person acting on its behalf) and the provider of information or such transfer has been consented to by the provider of information. • In February 2014, media reported on a leaked internal note from the National Security Council Secretariat, which shows that a three-pronged strategy with strong elements of data localization is being considered. The proposal included mandating all email providers to set up local servers for their India operations such that "all data generated from within India should be hosted in these India-based servers and this would make them subject to Indian laws" (Thomas 2014).

Source: Global Commission on Internet Governance, ourinternet.org

Appendix B: Overview of subjects targeted by data localization requirements (by country)

	Light (Only Copy)	Medium (Copy and Processing)	Strong (Ban to Transfer)
Australia			health data
Brunei		all data generated within the country	
Bulgaria		Gaming data	
Canada			data of public bodies
China		all data generated within the country, taxi users data, online maps, electronic media	financial information, health data, state secrets
Denmark	Financial records		
France		Systems for interception of electronic communication	
Germany	Tax records, accounting documents and business letters, invoices		
Greece	Data on 'traffic and localisation'		
Indonesia		financial data	personal data
Korea			financial data, high resolution imagery and related mapping data
Luxembourg		Financial data	
Netherlands	Public records		
New Zealand	Business records		
Nigeria		Subscriber and consumer data, financial data	Government Data
Pakistan			Certain countries
Poland	Gambling data		
Romania	Gambling data		
Russia	Users information	Personal data	
Sweden	Certain corporate documents, certain public data		
Taiwan			China
Turkey	Online payments		
Vietnam		Online social networks, general information websites, mobile telecoms network based content services and online games services	

Source: Global Commission on Internet Governance, ourinternet.org

Appendix C: Detailed analysis of Policy Elements in the Strategic Pillar

Country	Establishment of an independent supervisory authority	Supporting data localization policies, laws and regulations	Form of localization	Number of data subjects (population in million) Source: https://worldpopulationreview.com/countries	Number of registered data controllers and processors	Supporting resources (budget and staff)	Existence of data standardization framework	Existence of data architecture standard	Existence of data security strategy	Existence of data governance policies and strategies (data sharing, quality, analysis and storage)
Kenya	Office of the Data Protection Commissioner in 2020	• Kenya Data Protection Policy of 2018 • Kenya Data Protection Act of 2019 • General regulations • Complaints Handling Procedure and Enforcement) regulations • Registration of Data Controllers and Data Processors) regulations •	Processing of personal data of strategic interest to be affected through a server and data center located in Kenya or a serving copy of such data should be stored in a data centre located in Kenya	55	*2473	Budget: Ksh 250 million Total number of Staff: 92	Yes (ICT Standards)	Yes (Government Enterprise Architecture Framework for Ministries, Counties and Agencies)	Yes (National cybersecurity Strategy of 2022)	No National Data governance policies and strategies
Nigeria	Nigeria Data Protection Bureau in 2022	• National Information Technology Development Agency (NITDA) Act of 2007 • Nigeria Data Protection Regulation 2019 • Nigeria Data Protection Draft Bill	Restrict processing of personal data based on having adequate level of protection by foreign countries	223.7	NA 500,000 Potential members	Number of Staff: 15	Yes (Ownership Data Standard)	Yes (Data Exchange Architecture for the National Data Repository)	Yes (National cybersecurity policy and Strategy)	Draft National Data Strategy
Uganda	National Information Technology Authority - Uganda (NITA-U) in 2021	• Data Protection and Privacy Act, 2019 •	Restrict processing of data in foreign countries based on consent	48.5	112 data processers and controllers registered	Budget: Ksh 5.3 billion	Yes (Open Data Policy)	Yes (Uganda Enterprise Architecture and Interoperability Framework)	National Cybersecurity Strategy of Uganda of 2022	Open Data Policy
Australia	Office of the Australian Information Commissioner ("OAIC") - 2010	• Australian Information Commissioner Act 2010 • The Freedom of Information Amendment (Reform) Act 2010[	Data residency framework to protect national critical sovereign data, and the infrastructure and hosting arrangements that store, protect and manage personal data	26.4	NA	Budget: Ksh 4.6 billion Number of staff: 135	Yes (National Data Standards)	Yes (Australian Government Architecture)	Yes (Cybersecurity strategy)	Yes (Australian Data Strategy)

*Provisional statistics NA: No Official Statistics available

Source: Author's construction

Appendix D: Detailed analysis of policy elements in the tactical pillar

NA: Not Available

Country	Number of universities	Overall performance		Staff training		Availability of scientists and engineers		Digital skills among populations		Global science and technology skills		Government success in ICT promotion		Tertiary graduates (IT)		Ease of finding skilled employees	
		Overall Value range 0-10	Overall Global Ranking	Scores	Ranking	Scores	Ranking	Scores	Ranking	Scores	Ranking	Scores	Ranking	Scores	Ranking	Scores	Ranking
Kenya	48	4.8	70	5.3	55	6.1	38	6.2	49	0.8	105	6.5	22	3.4	44	8.2	21
Nigeria	170	3.6	103	3.6	101	4.2	79	2.9	119	NA	118	3.2	102	3.2	48	4.6	95
Uganda	43	3.7	100	4.0	91	57	5.0	2.9	118	NA	118	5.0	51	2.8	74	6.6	48
Australia	43	33	6.1	7.2	24	7.1	16	7.6	23	7.2	27	4.9	54	85	2.7	7.1	40

Source: Digital Skills levels- index – Wiley 2021

Appendix E: Detailed analysis of Policy Elements in the Delivery Pillar

Country	Size of digital economy (Billion Ksh)	Individuals using the Internet (% of population) Source: World Bank	National total available bandwidth (million Mbps)	Network readiness index score (Technology, People, Governance and Impact) Source: https://networkreadinessindex.org/	Internet Privacy index score (out of 40) Source: https://online.stevens.edu/info/countries-ranked-by-internet-privacy/	Number of Data centers Source: https://www.datacentermap.com/africa/	Mobile cellular subscriptions (per 100 people) Source: World Bank	Number of Secure Internet servers (per 1 million people) Source: World Bank	Global Cybersecurity Index 2020 score Source: ITU
Kenya	742	29	11.9	46.9	25	9	123	248	81.7
Nigeria	3,405	55		36.6	17	11	91	73	84.7
Uganda	139	10		33.3	19	1	66	35	69.98
Australia	16,402	96		72.8	25	287	105	39,853	97.4
Estonia	NA	91		69.7	37	15	149	112,151	99.48
China	987,000	73		68.8	NA	443	122	948	92.53

NA: Not Available * estimates

Source: Author's construction

ISBN 978 9914 738 07 0

Kenya Institute for Public Policy Research and Analysis
Bishops Garden Towers, Bishops Road
PO Box 56445, Nairobi, Kenya
tel: +254 20 2719933/4, 2714714/5, 2721654, 2721110
fax: +254 20 2719951
email: admin@kippra.or.ke
website: http://www.kippra.org