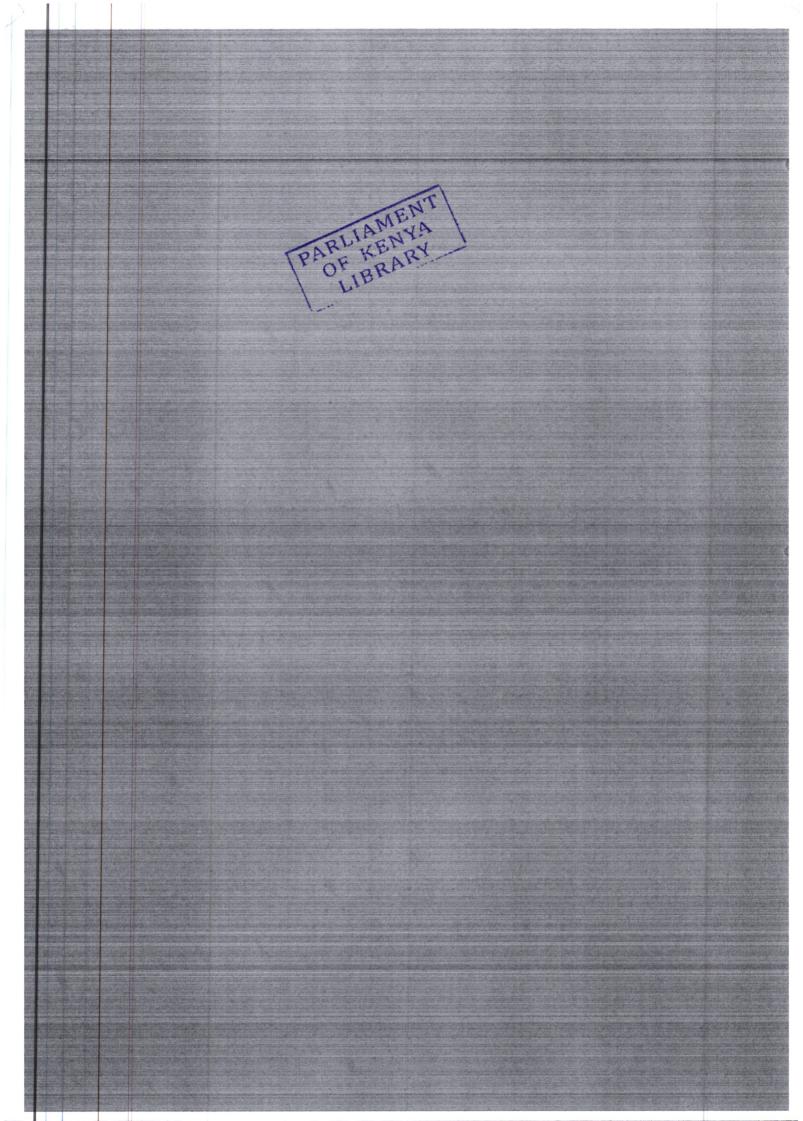


# Quarterly Economic and Budgetary Review

First Quarter, Financial Year 2021/2022 Period ending 30th September, 2021

**November 2021 Edition** 

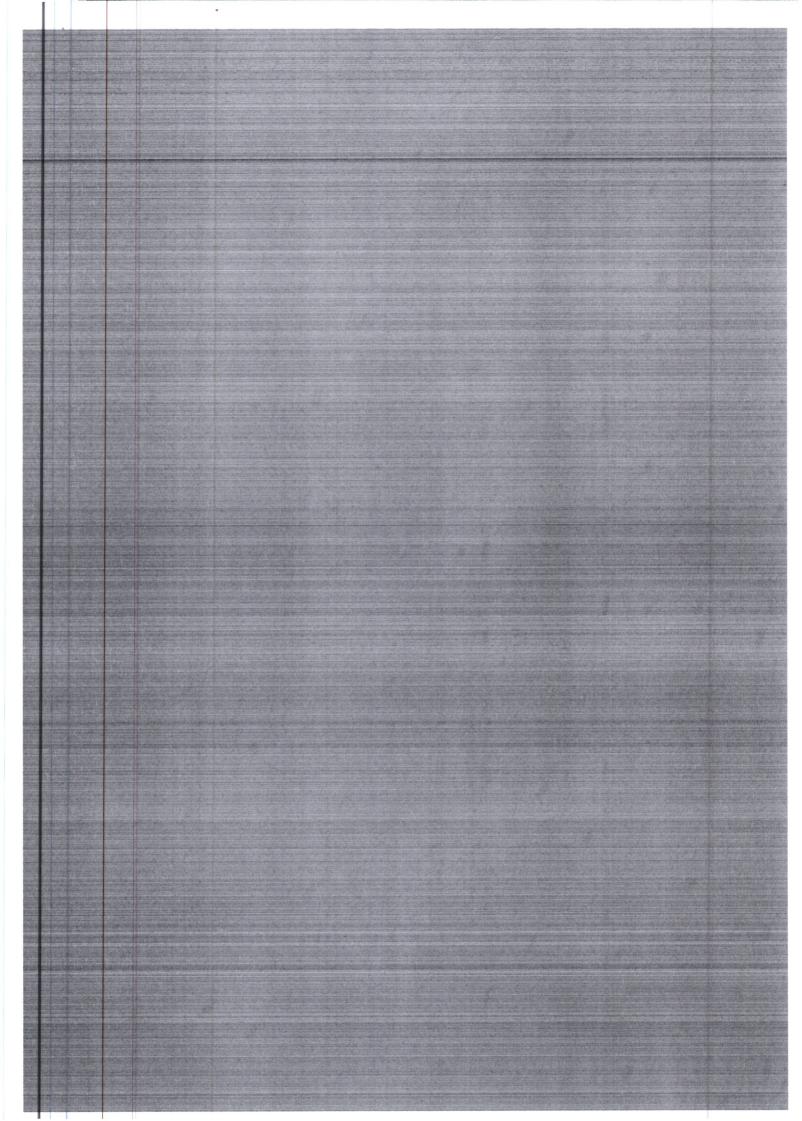


CON	TENTS						
1.0	STATEMENT BY THE DATA COMMISSIONER4						
2.0	INTRODUCTION6						
	2.1 Background Information						
	2.2 Vision, Mission and Functions of Office of Data Protection Commissioner7						
3.0	0 FINANCIAL STATEMENT FOR THE YEAR 2020/21						
	3.1 Budget allocation and Utilization9						
4.0	OFFICE OPERATIONAL PLAN1						
5.0	KEY ACHIEVEMENT/ DELIVERABLES11						
	5.1 Work Station - Office Space 11						
	5.2 Human Resource11						
	5.3 Financial Resource Mobilization 12						
	5.4 Stakeholder Engagements and Consultations Forums 12						
	5.5 Data Protection Regulations, 202112						
	5.6 Policies, Standards Operating Procedures (SOPs)& Manual 13						
	5.6.1 Map Data Controller/Processors13						
	5.6.2 Strategic Plan13         5.6.3 Data Protection Curriculum14						
	5.6.3 Data Protection Curriculum14						
	5.6.4 Service Charter 14						
	5.6.5 Complaints Manual14						
	5.6.6 Guidance Notes14						
	5.6.7 Code of Conduct and Ethics15						
	5.6.8 Training Needs Assessment15						
	5.6.9 Standards Operating Procedures (SOPs) 16						
	5.6.10 ICT Policy and Strategy16						
	5.6.11 Media and Public Communication Strategy 16						
	5.6.12 Framework for Periodic Audits 16						
	5.6.13 Awareness Creation 16						
	5.6.14 Complaints Resolution 17						
	5.6.15 Data Protection Advisories 17						
	5.6.16 International Cooperation on Data Protection 17						
6.0	STATISTICAL INFORMATION ON DATA PROTECTION 21						
6.1	Data Protection Legislation21Data breach Complaints23						
6.2	Data breach Complaints						
6.3	Registration of Data Controllers and Data Processors						
7.0	LIST LESSONS LEARNT FROM SECTION 6. ABOVE AND PROPOSE RECOMMENDATIONS_						
8.0	IMPACT OF DATA PROTECTION LAWS 26						
9.0	CHALLENGES27						
	CALL FOR ACTION 30						
	CONCLUSION 30						
12.0	ANNEX: 32						

25

9.8932 2.9500

Table of Contents





## 1.0 INTRODUCTION

#### 1.1 Background Information

The right to privacy is acknowledged as a basic human right under the Universal Declaration of Human Rights and, indeed, espoused in many Constitutions the world over, including in the Constitution of Kenya 2010. Article 31 of the Constitution states that every person has the right to privacy. Article 31 (c) and (d) goes further to include the right not to have their information relating to their family or private affairs unnecessarily required or revealed and the privacy of their communications infringed, respectively.

Kenya's Vision 2030 also calls for the development of a vibrant ICT sector that promotes socio-economic growth and drives productivity in other sectors.

The ICT sector is positioned as a critical driver and enabler to Kenya's socio-economic development. To this end the Government of Kenya has developed a number of policies and documents that emphasise the importance of technology and innovation in achieving Kenya's strategic goals. One of this being the Digital Economy blueprint, 2019 which recognises five key pillars that must exist in order to have a robust Digital Economy. The identified pillars are: (1) Digital Government; (2) Digital Business; (3) Infrastructure; (4) Innovation Driven Entrepreneurship and (5) Digital Skills and Values.

The Digital Economy Strategy, 2019 further recognizes that there are some cross-cutting issues that must be addressed in order for the five pillars to have strong foundations. One of those identified cross-cutting issues is the existence of a Data Protection Framework.

It is against this backdrop that Kenya enacted the Data Protection Act, 2019 to give effect to Article 31 (c) and (d) of the Constitution in November 2019. The object and purpose of this Act is to regulate the processing of personal data, ensure that the processing of personal data of a data subject is guided by the principles set out in Section 25 of the Act, protect the privacy of individuals, establish the legal and institutional mechanism to protect personal data and provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act. The enactment of the Act paved way for the establishment of the Office of the Data Protection Commissioner whose mandate is to operationalize and implement the purpose of the Data Protection Act, 2019.

Today, the issues on data protection have become more relevant in our increasingly data driven economy, with many nations and regional blocks enacting and adopting Data Protection legislation and Conventions. An example is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) which provides for electronic transactions, privacy and cybersecurity. With the establishment and operationalization of the Office of Data Protection Commissioner, Kenya is on the path to ratifying the Malabo Convention.

Technology is advancing at an exponential rate. This has resulted an increase in the processing of data, occasioned by the increased use of technologies reliant on the Internet of Things (IoT) and the move by institutions to undertake digital transformation. The constant challenge is to ensure that the institutions think ahead and put in place adequate data protection and security safeguards to protect personal data.

## 1.2 Vision, Mission and Functions of the Office

## 1.2.1 Vision

"To enhance trust and build transparency of data protection in Kenya"

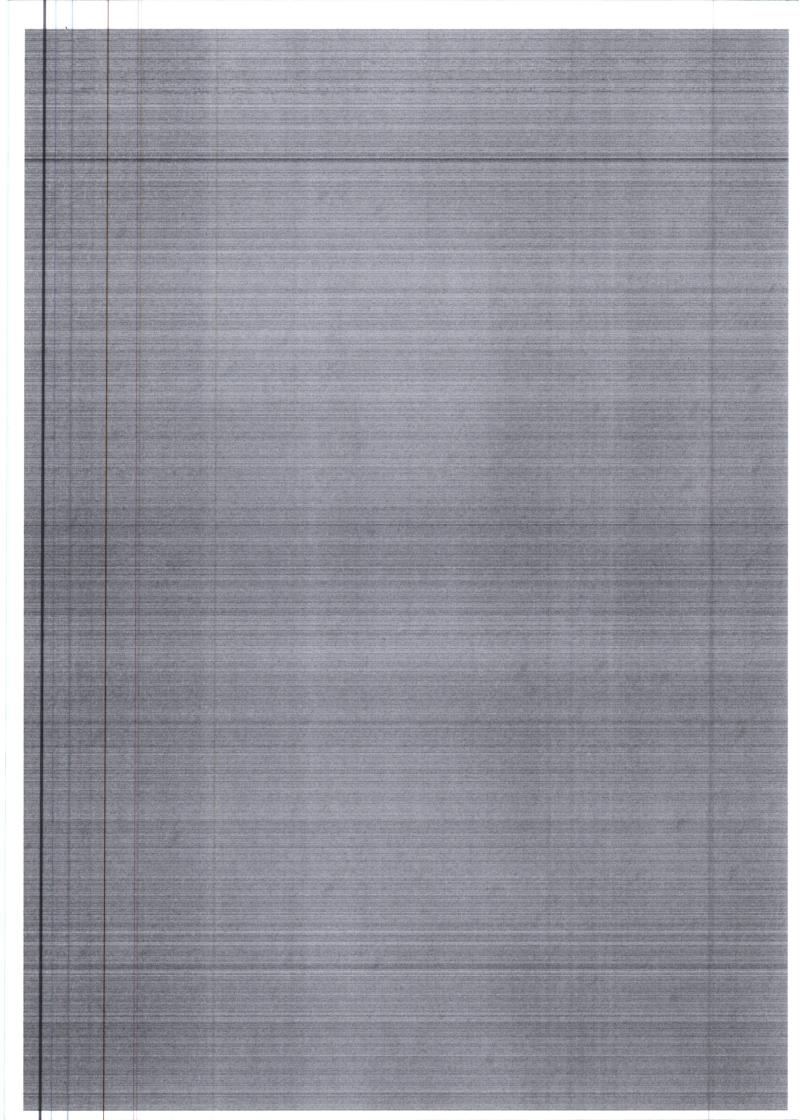
## 1.2.2 Mission

"Protect personal data in Kenya through compliance, enforcement, public awareness and institutional capacity development"

## 1.2.3 Mandate

The Mandate of the Office of Data Protection Commissioner as derived from the Data Protection Act 2019 and includes;

- regulating the processing of personal data;
- 2) ensuring that the processing of personal data of a data subject is guided by the principles set out in section 25 of the Act;
- 3) protecting the privacy of individuals;
- 4) establishing the legal and institutional mechanism to protect personal data; and
- 5) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.



## 3.0 OFFICE OPERATIONAL PLAN

The Office of Data Protection Commissioner used the funds allocated by the National Treasury and financial support from the Communications Authority of Kenya to implement the Office Operational Plan which had the following key components;

- Work Station -Office Space 1)
- 2) Human Resource Policy Documents
- 3) Financial Resource Mobilization
- 4) Stakeholders' Consultations
- 5) 6) 7) **Data Protection Regulations**
- Policies, Standards Operating Procedures (SOPs)& Manual
- Alternative Disputes Resolution Framework
- 8) Framework for Periodic Audits
- 9) Awareness Creation

## 4.0 KEY ACHIEVEMENT/ DELIVERABLES

#### Work Station -Office Space 4.1

During the 2020/21 financial year, the Office of Data Protection Commissioner was hosted by the Communications Authority of Kenva at the Communication Centre, Ground Floor Boardroom. The Office has identified future Office Space at Britam Towers in consultation with the State Department of Housing and Urban Development and Ministry of ICT, Innovation and Youth Affairs which we hope to acquire and occupy once legal processes have been undertaken.

In order to ensure seamless communications with stakeholders, the Office created an interactive website, website, website, developed our brand logo and opened postal address to enhance its visibility and accessibility. Further the Office functional email account info@odpc.go.ke and social media accounts such as face book, twitter and LinkedIn were operationalized.

In order to ensure that the Office operates smoothly, the Ministry of ICT, Innovation and Youth Affairs and the National Treasury has temporally deployed eight staff in legal services, Planning, Human Resource, Accounts, Procurement and Office Administration. In addition, the Office has recruited on contractual terms, a Personal Assistant and a driver for the Data Commissioner consequent to approval by the Public Service Commission(PSC) and the Salaries and Remuneration Commission bringing the total staff to thirteen (13) as at 30th September, 2021.

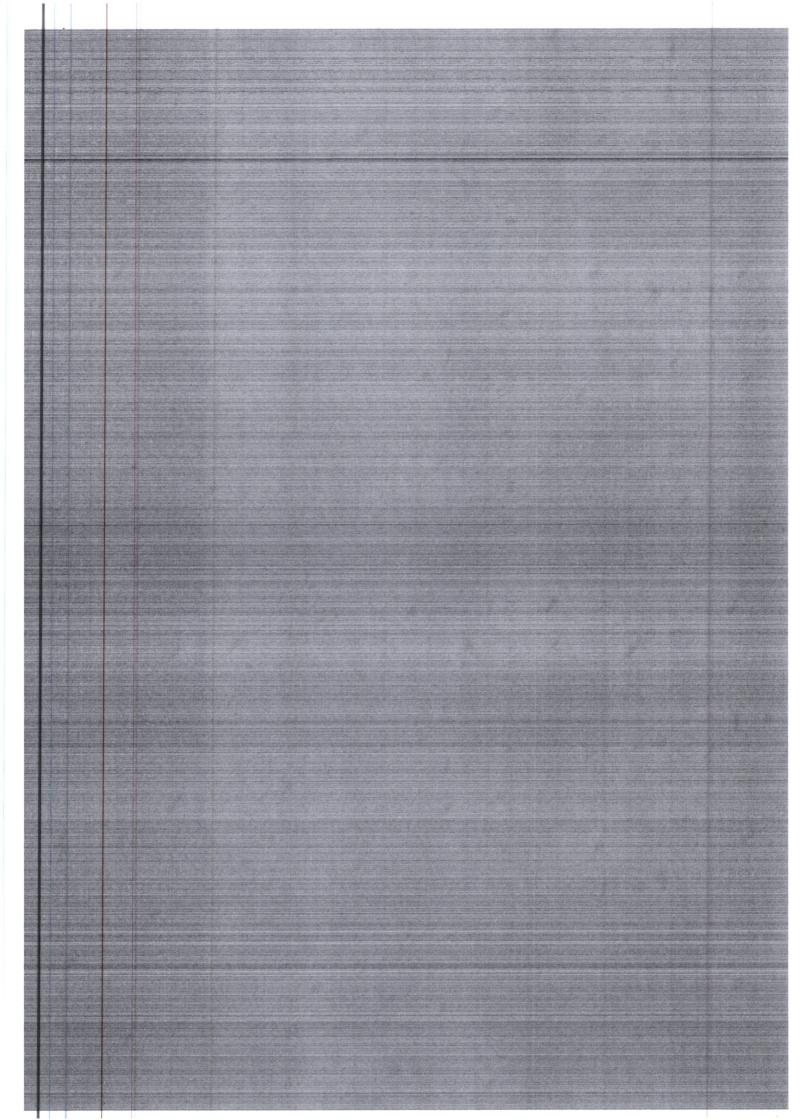
In order to facilitate staff recruitment, the Office through a multi-agency committee developed Four (4) Human Resource Policy documents. These are:

- Organization Structure and Staff Establishment; 1)
- Career Guidelines: 2)
- 3) Human Resource Manual
- 4) Job Description for Data Commissioner and Seventy Eight (78) for the Staff.

The Organizational Structure and Staff Establishment Policy document was approved by the Public Service Commission(PSC) in March, 2021. In addition, the Salaries and Remuneration Commission approved the grading and salary structure for the Office of Data Protection Commissioner in September, 2021 following job evaluation clinics and will be seeking authority to recruit from the Head of Public Service and the National Treasury in accordance with Government Policy on staff recruitment in the Public Service.

#### 4.3 **Stakeholder Consultations**

During the year under review, the Office of Data Protection Commissioner in actualization of its mandate of creating public awareness on Data Protection, held 36 virtual and Physical awareness creation and consultation forums with various stakeholders both from the Public, Private sectors and development partners.





#### 4.5.4 Complaints Manual

The Office of Data Protection Commissioner has developed and launched a Complaint Manual to provide a step by step simplified guide to promote efficiency & effectiveness in complaint's management and; provide clarity in the management of complaints starting from lodging of complaints, preliminary enquiries, investigations and resolution of complaints.

The Draft Complaints Manual will be finalized once the Data Protection Regulations are approved and gazetted.

#### 4.5.5 Guidance Notes

The Office of Data Protection Commissioner has developed and issued the following guidance notes;

- Conducting Data Protection Impact Assessment
- Seeking Consent from Data Subjects
- Processing Personal Data for Electoral Purposes

These Guidance Notes seek to provide further clarity on processing of personal data to ensure compliance with the provisions of the Data Protection Act, 2019 and Data Protection Regulations.

#### 4.5.6 Code of Conduct and Ethics

The Office of Data Protection Commissioner developed and submitted for approval the Code of Conduct and Ethics. This Code provides a clear framework within which the staff are expected to conduct themselves. The Code specifically seeks to:

- Increase the staff satisfaction, trust and self-identification with the ODPC;
- Increase the organizational resilience, and improve the functionality, efficiency and performance of the staff through preventing ambiguity and creating clear behavioural codes;
- Increase accountability, transparency and good governance in service delivery thus continually contributing to the Office's image, boosting public confidence and protect the integrity of the Office;
- Establish a moral foundation of values that raise the level of awareness of ethical standards required of all the staff to improve their decision making process and also to reflect in personal behaviour and standards of conduct;
- Ensure discipline, commitment, honesty, objectivity and impartiality in decision making and in the execution of the Office's duties;
- Provide mechanisms for consensus building on ethical issues, registration and management of gifts and conflicts of interest, decision making, and ethical dialogue;
- Provide a framework and mechanisms for reporting of misconduct, whistle blowing, and investigation procedures, processing of disciplinary matters arising from breach of this code and enforcement and sanctions for breach of the code or other Policies of the Fund.

The Code of Conduct and Ethics was approved by the Ethics and Anti-Corruption Commission and is currently in force.

#### 4.5.7 ICT Policy and Strategy

The Office of the Data Protection Commissioner developed the ICT policy and Strategy to guide the use of ICT resources within the Office of the Data Commissioner and to ensure that ;

- Acceptable use of ICT resources,
- Compliance with all standards, legislative and regulatory requirements during the acquisition and disposal of ICT equipment,
- Assure confidentiality, integrity and availability of the information used and produced in the Agency,
- Users are equipped with the necessary skills to properly utilize ICT resources.
- Security of data and information within the ODPC,
- Improve the quality of services through the application of ICT in service delivery and,
- Provide policy guidelines on acquisition, implementation, acceptable use and maintenance of ICT resources within the ODPC.

#### 4.5.8 Media and Public Communication Strategy

The Office of Data Protection Commissioner developed and adopted a Media and Public Communications Strategy to enhance both internal and external communication to enhance service delivery. In addition, the Office developed and uploaded on the website the frequent Asked Questions in respect to Data Protection.

#### **4.5.9 Framework for Periodic Audits**

The Office developed a System Audit Framework to guide in conducting periodic systems audits for Data Controllers and Data Processors to ensure compliance with the Data Protection Act, 2019 and promote self- regulation.

#### 4.5.10 Awareness Creation

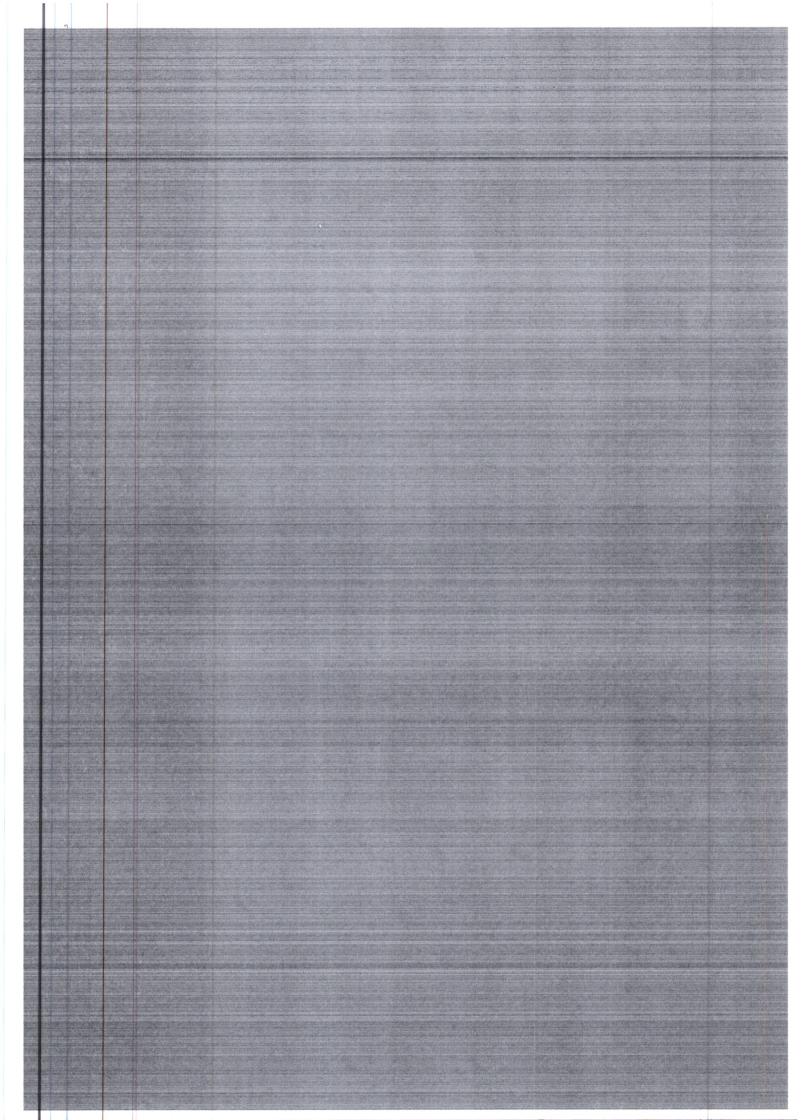
In order to enhance the effectiveness in the implementation of the Data Protection Act, 2019 and the three (3) sets of the Data Protection Regulations, the Office of Data Protection has undertaken stakeholders' awareness through virtual platforms owing to the implementation of Covid 19 pandemic Containment Measures. A robust awareness campaign targeting all the forty seven counties will be rolled out through print ,electronic and social media.

### 4.5.11 Complaints Resolution

The Office of Data Protection Commissioner has received a total of 352 Complaints from data subjects. Out of the received Complains, 291 have being investigated and resolved. However, 61 complaints remain active and investigations are ongoing.

#### 4.5.12 Data Protection Advisories

During the period under review, the Office received requests for advisories in relation to implementation of the Data Protection Act, 2019, and has subsequently issued 9 advisories to Data Controllers and Data Processors in public and private sector on the provisions of the Act to ensure compliance with the provisions of Data Protection Act, 2019. These institutions are Maina & Onsare Partners Advocates



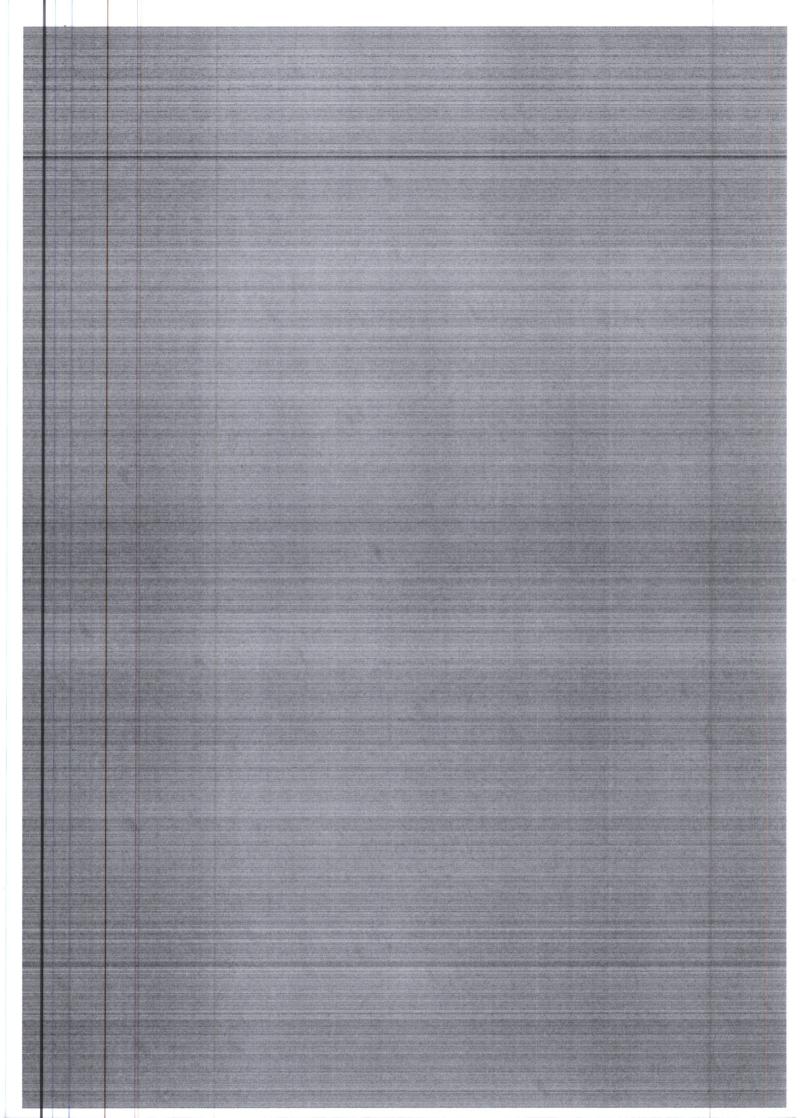
LLP, the Teachers Service Commission (TSC), Huduma Namba Secretariat, Law Society of Kenya, Isuzu Kenya, Ministry of Foreign Affairs, World Athletics U20 championships Nairobi 21, Munyaka Advocates and Peek Vision Limited.

#### 4.5.13 International Cooperation on Data Protection

In order to promote International Cooperation in matters relating to data processing of personal data and ensure that there is no significant risk or adverse effects of any development on the privacy of the individual, the Office of the Data Protection Commissioner applied and joined two International Associations on Data Protection; Commonwealth Common Thread Network and African Network of Data Protection Authorities to build capacity of the Office to safeguard personal data.

## 4.6 Summary of Key Milestones

Programme	Key Output	Key Performance Indicators	Planned Targets 2020/21	Achlevements 2020/21	Remarks
Compliance and Enforcement	Personal Data Pro- tection Services	Sets of Data Protection Regulations	3	3	3 Sets of Draft Data Protection Regulations developed awaiting review by National Assembly.
					<ul> <li>Data Protection (General) Regula- tions, 2021;</li> </ul>
					These regulations set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the du- ties and obligations of the data controllers and data processors.
					• Data Protection (Compliance and En- forcement) Regulations, 2021
					These regulations outline the compliance and enforcement provisions.
					• Data Protection (Registration of Data Controllers and Data Processors) Regu- lations, 2021.
					These regulations set out the procedure that will be adopted by the office of the data commissioner in registering data controllers and data processors as per the Data Protection Act.
		No. of Guidelines and Manuals developed	3	3	<ul> <li>The Office has developed the following Data Protection Policy documents;</li> <li>a. Guidelines on Data Protection Impact Assessment,</li> <li>b. Guidelines on Seeking Consent from</li> <li>c. Data Subjects and Manual on Complaints</li> </ul>
		No. of Advisories issued	9	9	The Target depends on request from Data Controllers and Data Processors
		No. of Data Impact Assessment Reports reviewed	4	4	The Office reviewed and approved Data Protection Impact Assessment from four (4) Data Controllers



#### 6.0 LESSONS LEARNT AND RECOMMENDATIONS

### Investment in Awareness Creation and Training in Data Protection

The Office of Data Protection Commissioner needs to increase awareness creation on the provision of the Data Protection Laws. Similarly Data Controllers and Data Processors need to invest in training on Data Protection including appointment of Data Protection Officers to champion compliance with Data Protection Act and subsequent legislations.

#### High Cost of Non- Compliance

The direct and indirect cost associated with non- compliance is huge and therefore Data Controllers and Data Processors should review their Data Processing Systems, Internal Policies to promote self- regulations.

#### Relationship between Data Breach and Cybercrime

A data breach is a cyber attack in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. This therefore implies that there is need of structured collaboration between the Office of Data Protection Commissioner and he National Cyber Command Centre (NC3) for effective realization of the mandates of the two institutions.

#### Strengthening the Office of Data Protection Commissioner

The Office has witnessed increased High expectations from Kenyans ( Data Subjects) in relation providing data subjects with rights and remedies to protect their personal data from processing that is not in accordance with Act and therefore the Government should fast track fully operationalization of the Office in terms of recruitment of necessary Human Resources, establishment of a robust ICT Infrastructure, finalization of pending data protection laws and increased funding to facilitate enforcement of the provisions of the Data Protection Act, 2019.

#### 7.0 IMPACT OF DATA PROTECTION LAWS

Global

#### 7.1.1 The Evolving Technologies

Technology is advancing at an exponential rate. This has resulted in an increase in the processing of data, occasioned by the increased use of technologies reliant on the Internet of Things (IoT) and the move by institutions to undertake digital transformation. The constant challenge is to ensure that the institutions think ahead and put in place adequate data protection and security safeguards to protect personal data.

Additionally, there is a need for institutions to increase investments in security procedures and systems and incorporate adequate data governance structures to continually identify, protect from or minimise the risks of data breaches.

#### Al.2 Lack of Awareness

Data Protection is still new in Kenya and as such, Data Controllers and Data Processors and the general public need to understand and appreciate their rights and obligations as provided for in the Act. Such an understanding requires knowledge on what data is deemed to be personal data or sensitive personal data, and therefore in need of additional safeguards, transparency on issues relating to where the data is, how it is being used, where it is going, its value and how it is protected.

#### 7.1.3 Financial Resources/ Investmentse

Part of data protection, especially where processes are digital, involves the mapping of an ICT framework and system architecture that provides a Data Centric Security approach to facilitate the establishment of compliance and enforcement frameworks, complaints handling mechanisms and Registration of Data Controllers and Processors frameworks.

The Capital Investment required to establish a robust Data Centric security system and compliance mechanism can be high for both the Regulator and the Data Controller and Data Processor. Further, investment in the Human capital, including capacity building, will equally require some level of investment.

Additionally, organizations need to invest in education and data security safeguards whether ICT based or otherwise, to ensure adequate safety mechanisms to protect from and mitigate from data breaches.

#### 7.1.4 Computer misuse and Cyber Crimes

We live in a world where huge amounts of data are digitized and vulnerable due to the amount of data collected and processed at any one time. Consequently, data breaches as a result of cyber-crimes are expensive as they are likely to cost an organization millions of shillings in revenue loss as well as the and the cost of fines imposed by the regulating authorities.

7.2 Significant Impact of the Office of Data Protection Commissioner

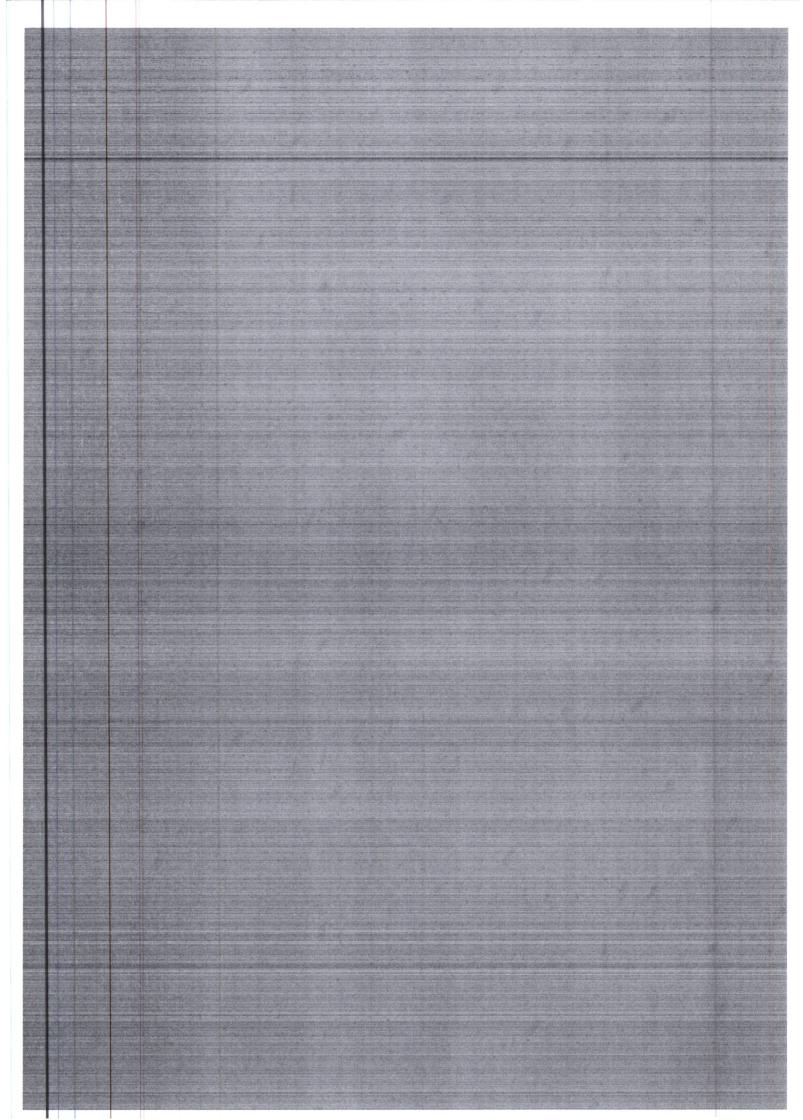
Over the last 11 months, the Office has immensely contributed in the following aspects directly or indirectly touching on lives of Kenyans;

7.2.1 Facilitated implementation of Huduma Namba Program

The establishment and operationalization of the Office of the Data Protection Commissioner was ruled by the High Court in 2020 as one of the conditions the Government should ensure prior to fully roll-out of the Huduma Namba Programme. The issuance of advisory and guidelines on Data Protection Impact Assessment in relation to Huduma Namba has ensured smooth implementation of phase 2.

7.2.2 Actualization of principle of Seeking Consent

Following receipt of 291 Complaints on processing of personal data for election purposes by Political Parties, the Office enforced the Data



## 11.1 PICTORIAL PRESENTATION



CA ag.DG Mercy Wanjau, DC Immaculate Kassait, PS Esther Koimett, Senate and National Assembly committee Members Hon. Kanini Kega, Hon. Gideon Moi, Hon. William Kisang



Taskforce on Data Protection Regulations during a Naivasha retreat



Senate Committee on ICT during a Mombasa Taskforce on Data Regulations Taskforce on working retreat with Ministry of ICT Officials and Organizational Structure Naivasha Retreat the Taskforce on Data Regulations









Data Commissioner Immaculate Kassait Data Commissioner Immaculate Kassait when she met immediate former KFCB CEO Ezekiel when she met EU Delegation in her office. Mutua on forging areas of collaborations

Ministry of ICT PS Jerome Ochieng during a virtual public participation exercise on Data Protection Regulations 2021

