



 THE NATIONAL ASSEMBLY MEMBERS LAID	
DATE:	18 NOV 2021
TABLED BY:	L.O.M
CLERK AT THE TABLE:	FINLEY

OFFICE OF THE DATA PROTECTION COMMISSIONER

FIRST ANNUAL REPORT FOR THE 2020/21 FINANCIAL YEAR

September, 2021

Promoting Personal Data Protection by Design

Table of Contents

CONTENTS

1.0	STATEMENT BY THE DATA COMMISSIONER	4
2.0	INTRODUCTION	6
2.1	Background Information	6
2.2	Vision, Mission and Functions of Office of Data Protection Commissioner	7
3.0	FINANCIAL STATEMENT FOR THE YEAR 2020/21	9
3.1	Budget allocation and Utilization	9
4.0	OFFICE OPERATIONAL PLAN	11
5.0	KEY ACHIEVEMENT/ DELIVERABLES	11
5.1	Work Station -Office Space	11
5.2	Human Resource	11
5.3	Financial Resource Mobilization	12
5.4	Stakeholder Engagements and Consultations Forums	12
5.5	Data Protection Regulations, 2021	12
5.6	Policies, Standards Operating Procedures (SOPs)& Manual	13
5.6.1	Map Data Controller/Processors	13
5.6.2	Strategic Plan	13
5.6.3	Data Protection Curriculum	14
5.6.4	Service Charter	14
5.6.5	Complaints Manual	14
5.6.6	Guidance Notes	14
5.6.7	Code of Conduct and Ethics	15
5.6.8	Training Needs Assessment	15
5.6.9	Standards Operating Procedures (SOPs)	16
5.6.10	ICT Policy and Strategy	16
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 Legislation	21
6.2	Data breach Complaints	23
6.3	Registration of Data Controllers and Data Processors	24
7.0	LIST LESSONS LEARNT FROM SECTION 6. ABOVE AND PROPOSE RECOMMENDATIONS	25
8.0	IMPACT OF DATA PROTECTION LAWS	26
9.0	CHALLENGES	27
10.0	CALL FOR ACTION	30
11.0	CONCLUSION	30
12.0	ANNEX:	32

STATEMENT BY THE DATA COMMISSIONER

It is worth noting that the growth of the digital economy and technological advances in Kenya, which largely depend on data, requires a reciprocal legislation on data protection.

Additionally, the changing domestic and global data protection ecosystem, calls for a collaborative effort to respond to public concerns and legislative imperatives in relation to data privacy, use of data and the digital skills agenda.

Likewise, countries need to remain focused on the other aspects of regulatory, accessibility and availability of data for the common good of society.

Being cognizant of this need, 128 out of 195 Countries in the World today have enacted data protection legislations representing 66% countries globally.

To join this emerging global phenomena, the Government of Kenya enacted the Data Protection Act in 2019 which gave effect to Article 31 of the Constitution on the Citizens Right to Privacy.

To actualize this constitutional requirement, the Office of the Data Protection Commissioner was established in November 2020 pursuant to the Data Protection Act, 2019 to regulate the processing of personal data, ensure that the processing of personal data . The Act will also ensure that every data subject is guided by the principles set out in Section 25, 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 and facilitate the realization of a robust Kenyan digital economy.

The Office of the Data Commissioner will mark its first year anniversary on 17th November, 2021 and therefore this First Annual Report is prepared in fulfilment of the legal requirements as envisaged in Section 70 of the Data Protection Act, 2019 which obligates the Data Commissioner to, within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year for on-ward submission to the National Assembly.

Following my appointment on 17th November, 2020, as the pioneer Data Commissioner in Kenya, I began discharging the Mandate and the Functions of the Office of Data Protection Commissioner by first developing an Office Operationalization Plan which focussed on eleven priorities.

These are; Work Station -Office Space, Human Resource Recruitment, Financial Resource Mobilization, Stakeholders Consultations, Development of Data Regulations, Development of Framework for Registration and Certification, Development of Framework for Complaint Handling, Policies Development and Reviews, Development of Standards Operating Procedures (SOPs)& Manuals, Mapping of Data Controller/Processors, Development of Framework for Periodic Audits and Awareness Creation.

With support from the Cabinet Secretary, Ministry of ICT, Innovation

and Youth Affairs, Principal Secretary , State Department of ICT and Innovation, The National Treasury, Public Service Commission , Salaries and Remuneration Commission,Parliament through the Communication, Innovation and Technology Committee of the National Assembly and Information Technology Committee of Senate,Communication Authority of Kenya(CA) and Development Partners, Iam delighted to share with you, Key Milestones this Office has achieved in the last one year towards safeguarding personal data through compliance, enforcement, public awareness and institutional capacity development as well as facilitating the realization of a robust Kenyan digital economy.

True, to my undertaking during the launch of 100 Days in Office Report in February,2021, I can confidently state that the Office has realized over 90% of the Commitments contained in the Office Operational Plan as reflected in this Report.

As I conclude, special appreciation goes to the Cabinet Secretary Ministry of ICT, Innovation and Youth Affairs Mr. Joe Mucheru, EGH for his unwavering support in providing policy direction and guidance , all Heads of all institutions in the three Arms of Government, the Private Sector players through KEPSA for their valuable support during the development of Data Protection Regulations and the International Community who have stepped forward to provide financial and technical support .

Special thanks go to the British (UK) Government whose support has facilitated the development of a three (3) year Strategic Plan , the Government of the Federal Republic of Germany who engaged a Consultant to develop the roadmap and Training Needs Assessment and the United Nations Development Programme (UNDP) who have advertised for Consultancy services to develop the Alternative Disputes Resolution Framework.

Last and not least, let me thank all members of the Taskforce on Development of Data Protection Regulations, members of various Multi-Agency Committees who developed the Human Resource Policy Documents, ICT Policy and Strategy and the Committee on Establishment of the Office Registry and deployed staff of ODPC.

The success of the first year would have been in vain, were it not for the Board and Management of the Communications Authority of Kenya who went out of their way to provide a conducive office space for our Office as well as financial and logistical support to ensure that the Office of Data Protection Commissioner was operational.

To Kenyans in general, the Office remains aware of your high expectations with which you demand seamless service delivery in ensuring that the processing of personal data is within the provisions of the Data Protection Laws.



Immaculate Kassait, MBS
DATA COMMISSIONER

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;

- 1) 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.

1.2.4 Functions

The Functions of ODPC is derived from Section 8, of the Data Protection Act, 2019 of 25th November 2019 include:

- 1) To oversee the implementation of and be responsible for the enforcement of the Data Protection Act.
- 2) To establish and maintain a register of data controllers and processors.
- 3) To exercise oversight on data processing operations, either of own motion or at the request of a data subject and verify whether the processing of data is done in accordance with the Data Protection Act.
- 4) To promote self-regulation among data controllers and data processors.
- 5) To conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law.
- 6) To receive and investigate any complaint by any person on

infringements of the rights under this Act.

- 7) To take such measures as may be necessary to bring the provisions of the Data Protection Act to the knowledge of the general public.
- 8) To carry out inspections of public and private entities with a view to evaluating the processing of personal data.
- 9) To promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements.
- 10) To undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals.
- 11) To perform such other functions as may be prescribed by any other law or as necessary for the promotion of the objectives of the Data Protection Act.

2.0 FINANCIAL STATEMENT FOR THE YEAR 2020/21

2.1 Budget allocation and Utilization

During the FY 2020/2021, the Office was allocated Kshs. 25 Million for Recurrent budget by the National Treasury. In addition, the Office also received financial support amounting to Kshs. 20 Million from the Communications Authority of Kenya. The Budget allocation has increased to Kshs. 250 Million and Kshs. 270 Million in the FY 2021/2022 and FY 2022/2023 respectively. The 900% increase in budget allocation is mainly to cater for staff recruitment which is expected to commence during the FY 2021/2022.

The Budget for FY 2020/2021 was utilized 100% to fund the Office Operationalization Plan 11 priorities. The programmes funded during the year under review are;

- 1) **Institutional Capacity Development** which aims to build the capacity of the data protection institution and partnership to enhance data processing operations.
- 2) **Regulatory Services** – which aims at establishing a Policy and Legal framework to safeguard private data.
- 3) **Awareness Creation** – which aims at equipping stakeholders with adequate knowledge on the Provisions of the Data Protection Act, 2019 and any subsidiary legislation on Data Protection.

Please take note that the Financial resource requirement is expected to increase mainly depending on the extent of Office Operationalization measured by percentage implementation of the Organization Structure and Staff Establishment, level of Automation of the Office processes and the percentage completion of Office Space partitioning and acquisition of necessary equipment and furniture.

Table 1 - Analysis of Approved Budget Vs Actual Expenditure KShs. Millions

Table - 1 Analysis of Approved Budget Vs Actual Expenditure KShs. Millions			
Source of Funding		Approved Allocation KShs. Millions	Actual Expenditure KShs. Millions
National Treasury	Item	2020/21	2020/21
	Personnel Emolument	5	5
	Rent	0	0
	Operations and Maintenance	20	20
	Sub Total	25	25
Communication Authority of Kenya	Development of Human Resource Policy Documents	10.3	10.3
	Development of Data Protection Regulations	9.7	9.7
	Sub Total	20	20
	% of Absorption	100%	

Table 1 below provides an analysis of 2020/21 budget expenditure.

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;

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

4.0 KEY ACHIEVEMENT/ DELIVERABLES

4.1 Work Station -Office Space

During the 2020/21 financial year, the Office of Data Protection Commissioner was hosted by the Communications Authority of Kenya 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, www.odpc.go.ke, 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.

4.2 Human Resource

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;

- 1) Organization Structure and Staff Establishment;
- 2) Career Guidelines;
- 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.

4.4 Data Protection Regulations, 2021

The Office of Data Protection Commissioner in collaboration with the Ministry of ICT, Innovation and Youth Affairs, through a Gazetted Taskforce has developed three sets of draft regulations aimed at operationalising Data Protection Act, 2019. These Draft Regulations are;

1. **Data Protection (General) Regulations, 2021** - These 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, 2019.
2. **Data Protection (Compliance and Enforcement) Regulations, 2021.** -These outline the enforcement provisions, the procedures on exemptions of certain provisions of the Data Protection Act, 2019 as well as the requirements of carrying out the Data Protection Impact Assessment.
3. **Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021** - These set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the duties and obligations of the Data Controllers and data processors

The above regulations have been subjected to stakeholder and public participation as provided for in the Constitution of Kenya, 2010 and further articulated in the Statutory Instruments Act, 2013. A pre-publication engagement with the Delegated Legislation Committee of the National Assembly was also held on 13th August 2021.

4.5 Policy Documents, Standards Operating Procedures (SOPs) & Manual

During the period under review, the Office of Data Protection Commissioner has developed the following policy documents to enhance service delivery;

4.5.1 Strategic Plan

The Office of the Data Protection Commissioner with Support from the UK Government through the Digital Access program has developed a three (3) Strategic Plan. The three main pillars of the plan are;

- a) Institutional Capacity Development which aims at building the capacity of the data protection institutions and partnership to enhance data processing operations.
- b) Regulatory Services – which aim at establishing policy frameworks to safeguard private data.
- c) Awareness Creation – which aims at equipping stakeholders with knowledge and information on the provisions of the Data Protection Act, 2019 and any other subsidiary legislation so as to foster a culture of compliance and self-regulation.

The Draft Strategic Plan will be subjected to Stakeholders' validation prior to finalization.

4.5.2 Data Protection Curriculum

The Office of Data Protection Commissioner has partnered with Kenya School of Government and developed a training Curriculum on Data Protection for both the public and the private Sector. The Draft Curriculum has eight (8) Units to be delivered in 30 hours. The aim of the Curriculum is to improve the competencies of participants in data protection for awareness and compliance with the law.

The draft Data Protection Curriculum is undergoing review and approval by the Kenya School of Government.

4.5.3 Service Charter

The Office of Data Protection Commissioner has developed and launched a Citizen Service Charter to;

- **Enhance Stakeholders' awareness on the services the office provides;**
- **Inform stakeholders, of the standards of services they should expect from the office;**
- **Outline Stakeholders' rights and responsibilities;**
- **Explain the Office rights and responsibilities as a service provider; and**
- **Describe how Stakeholders' can lodge complaints and make suggestions about our service delivery.**

The Draft Service Charter will be finalized once the Data Protection Regulations are approved and gazetted.

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 Complaints ,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



XXXXXXS

Data Commissioner Immaculate Kassait when she met a delegation from Strathmore she hosted the head of delegation Olivier Dubois University in her Office the International Committee of the Red Cross ICRC in her office.



Data Commissioner Immaculate Kassait signs Leadership and Integrity Code of Conduct witnessed by Mr. Augustus Munywoki



XXXXXX

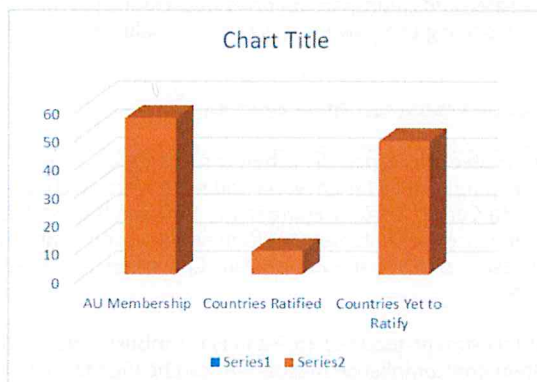


Data Commissioner Immaculate Kassait Data Commissioner Immaculate Kassait during a during swearing in ceremony

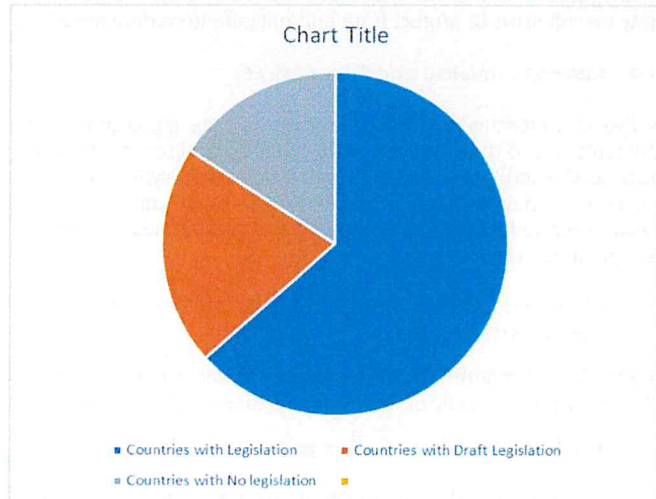


public participation webinar 26th April 2021

Coming back home, in the African Continent, the African Union (AU) member states adopted the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) in 2014. Since its adoption 55 member states have signed the Convention and 8 Members have ratified. Kenya as a member of AU is yet to ratify the Malabo Convention.



However, despite the fact that a number of African Countries have not ratified the Malabo Convention, 52% of Countries have Data Protection Legislation, 13% have no legislation and 17% have draft legislations.



In the Regional front, Kenya is among the Countries which have enacted a progressive Data Protection which seeks to guarantee protection of personal information and privacy as well as facilitated the utilization of personal data for social-economic development and innovation. Other Countries that have legislation on Data Protection include the Republic of Uganda and South Africa. The Republic of Rwanda Data Protection and Privacy Bill is pending approval and Gazettement as a law.

The Development and approval of Data Protection Legislation by var-

ious Countries is a true testimony that Personal Data is becoming a powerful force in the data value exchange and that more citizens or data subjects are demanding protection of their personal information during the collection, storage and analysis of their data.

5.2 Data breach Complaints

A security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual or unauthorized person results to data breach which leads to lodging of complaints by the data subjects.

Globally, during the period under review 3,950 confirmed data breaches were reported. The most significant data breaches are summarized below;

- 1) On January 22, 2020, a customer support database holding over 280 million Microsoft customer records was left unprotected on the web;
- 2) On February 20, 2020, Over 10.6 million hotel guests who have stayed at the MGM Resorts have had their personal information posted on a hacking;
- 3) On April 14, 2020, the credentials of over 500,000 Zoom teleconferencing accounts were found for sale on the dark web;
- 4) On July 20, 2020, An unsecured server exposed the sensitive data belonging to 60,000 customers of the family history search software company, Ancestry.com;
- 5) On August 20, 2020, Researchers at Comparitech uncovered an unsecured database with 235 million Instagram, TikTok, and YouTube user profiles exposed online belonging to the defunct social media data broker, Deep Social;
- 6) On November 5, 2020, a database for Mashable.com containing 1,852,595 records of staff, users, and subscribers data was leaked by hackers;
- 7) On December 10, 2020, an undisclosed number of users of the audio streaming service, Spotify, have had their passwords reset after a software vulnerability exposed account information ;
- 8) On February 18, 2021, the California Department of Motor Vehicles (DMV) alerted drivers they suffered a data breach after billing contractor, Automatic Funds Transfer Services, was hit by a ransomware attack;

In Kenya, the number of reports to the Office of Data Protection Commissioner are complains and data breaches are 352 and 14 respectively. An analysis of the Complains reveals that 291 complains were against political parties, 33 complains were filled against money lending platforms while 28 were due to other forms of personal data processing.

The numbers of complaints and data breaches is expected to increase drastically as more Kenyans become aware of their rights and available mechanisms in place to safeguard their personal information.

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 the 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.

7.1.2 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

		% of Complaints received and investigated	100	100	Investigations on the 14 received data breach complains are ongoing
		No. of Institutions / Data Controllers trained	2	2	The Office trained senior officers from Teachers Service Commissioner and Huduma Namba Secretariat
		No. of Awareness Workshops	10	16	The Office held sixteen virtual workshops to create awareness on Data Protection Act, 2019 and Draft Data Protection Regulations
Institutional Capacity and International Cooperation	Office Operationalization	Functional website	100%	100%	Developed an Interactive Website which is functional;
		Approved Organization Structure and Staff Establishment	100%	100%	Developed five (5) Human Resource Policy Documents including the Organization and Staff Establishment which was approved by Public Service Commission;
		System Audit Framework	1	1	Developed System Audit Framework for monitoring compliance by Data Controllers and Data Processors;
		Service Charter	50%	50%	Draft Service Charter in Place
	Cooperation	No. of Cooperation	2	2	The Office applied and Joint two International Associations on Data Protection; - Commonwealth Common Thread Network - African Network of Data Protection Authorities

5.0 STATISTICAL INFORMATION ON DATA PROTECTION

5.1 Data Protection Legislation

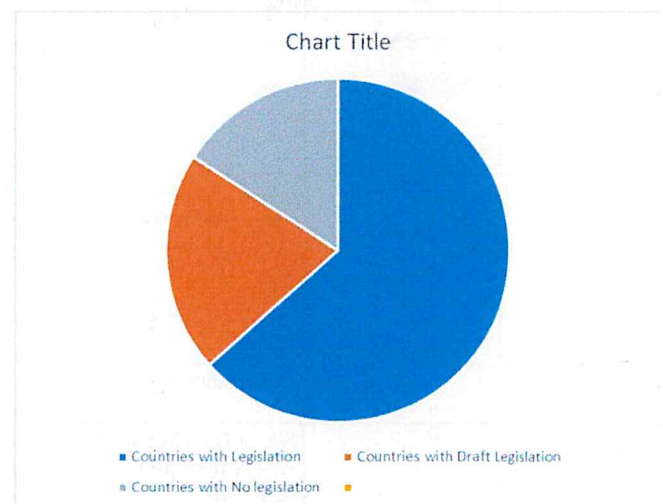
The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive as the primary law regulating how companies protect EU citizens' personal data. The GDPR ushered in a new era of data privacy regulation and governance in Europe and indeed across the world in 2018.

GDPR gave individuals new rights over their data especially on accountability on Entities (Data Controllers and Data Processors) collecting, storing, analysing and managing personally identifiable information.

Globally, 128 out of 194 countries had put in place legislation to secure the protection of data and privacy according to UNCTAD 2020 Report as shown below;

- 66% of Countries have Data Protection Legislation ;10% have draft Legislation; 19% have no legislation and 5% have no data.

- 66% of Countries have Data Protection Legislation ;10% have draft Legislation; 19% have no legislation and 5% have no data.**



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	Achievements 2020/21	Remarks
Compliance and Enforcement	Personal Data Protection Services	Sets of Data Protection Regulations	3	3	3 Sets of Draft Data Protection Regulations developed awaiting review by National Assembly. • Data Protection (General) Regulations, 2021; These regulations set out the procedures for enforcement of the rights of the data subjects as well as elaborating on the duties and obligations of the data controllers and data processors. • Data Protection (Compliance and Enforcement) Regulations, 2021 These regulations outline the compliance and enforcement provisions. • Data Protection (Registration of Data Controllers and Data Processors) Regulations, 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	• The Office has developed the following Data Protection Policy documents; a. Guidelines on Data Protection Impact Assessment, b. Guidelines on Seeking Consent from c. Data Subjects and Manual on Complaints
		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

Protection Act leading to deregistration of complainants from register of political parties and inclusion of an opt out mechanism by political parties when processing personal data.

7.2.3 Regulation of Digital Lenders in Kenya

The emergence of fintech has led to an increase in the availability of sensitive personal data in digital formats, which makes it more susceptible to security breaches. To ensure compliance with the Data Protection Act, 2019, the Office submitted recommendations to the Central Bank of Kenya (Amendment) Bill 2020. The recommendations on ensuring protection of personal data were adopted in the amended CBK Act, 2021.

7.2.4 Compliance by Data Controllers and Data Processors

Majority of Data Controllers and Data Processors in both the public sector and the private sector have resulted to data minimization to ensure compliance with the provisions of Data Protection Act.

Many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. If the DPA is not complied with, organisations will face the heaviest fines yet – up to 2% of previous year turnover. A renewed emphasis on organisational accountability will demand proactive robust privacy governance. This will require organisations to review how they write privacy policies to make these easier to understand, and enforce compliance.

In addition, DPA requirements will mean changes to the ways in which technologies are designed and managed. Documented Data Protection Impact Assessments will be required to deploy major new systems and technologies that are likely to result in high risk to the rights and freedoms of data subjects. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced data security approaches and incident response procedures. The concept of Privacy now becomes enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. And organisations will be expected to look more into data masking, pseudonymisation and encryption.

Lastly, Individuals and teams tasked with data and information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with (new) data subject rights – rights to have data deleted and to have it ported to other organisations. This will also have an impact on Third Party vendors that an organization works with.

The enforcement of the Data Protection Act, 2019 will be actu-

alized by the approval and gazettelement of Data Protection Regulations 2021.

8.0 CHALLENGES

The Office faced numerous operational challenges ranging from lack of adequate staff, management of high public expectations to limited funding during the year under review.

9.0 CALL FOR ACTION

The Office of Data Protection Commissioner calls upon the following Actors to prioritize their respective responsibilities for effective implementation of Data Protection Act, 2019.

- a) National Assembly
The National Assembly through the Delegated Legislation Committee to prioritize the review, approval and gazettelement of the draft Data Protection Regulations to be submitted by the Ministry of ICT, Innovation and Youth Affairs.
- b) Institutions both in the public and private sector
 - 1) Appreciation of the provisions of the Data Protection Act, 2019 and enhance mechanisms to promote compliance and self-regulation;
 - 2) Adoption of best practices that take into account principles of processing data and the rights of data subjects and safeguards as stipulated in the DPA, 2019;
 - 3) Undertake Data Protection Impact Assessment as provided for under DPA, 2019;
 - 4) Document and report any data breach and mitigation taken and;
 - 5) Pro-actively seek guidance from the Office Data Protection Commissioner
- c) Members of the Public
 - 1 Know their rights as data Subjects

10.0 CONCLUSION

It is not in question that our world is rapidly changing. With the dawn of the fourth industrial revolution, and even since the outbreak of the Covid-19 Pandemic, technological and social advances have led to an increase in the use of digital applications which in return has generated an unprecedented and exponential amount of digital data that needs to be safeguarded. In addition, the ICT ecosystem is ever deepening inter-connectivity, and as such regulation equally has to evolve, hence there is need for;

- 1) Regulatory co-operation across sectors and other jurisdictions to ensure that the positive dimensions of the ICT ecosystem are enjoyed while also creating an enabling environment that contributes to innovation and investment.
- 2) Balance between maximizing the benefits of the ICT ecosystem and securing optimal policy and regulatory objectives designed to address potential and actually negative consequences of the dynamic ICT landscape such as the infringement of data subject rights.

11.1 PICTORIAL PRESENTATION



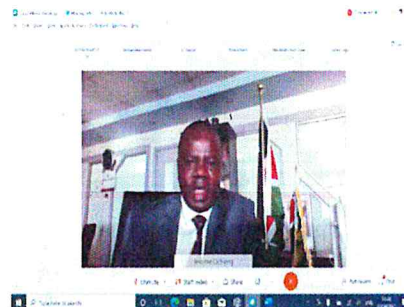
CA ag.DG Mercy Wanjau, DC Immaculate Kassait, PS Esther Koimett, Senate and National Assembly committee Members Hon. Kanini Kega, Hon. Gideon Moi, Hon. William Kisang



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



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



Data Commissioner Immaculate Kassait when she met immediate former KFCB CEO Ezekiel Mutua on forging areas of collaborations