



*Approved for tabling.*  
SNA  
27/9/23

PARLIAMENT OF KENYA

THE NATIONAL ASSEMBLY

THIRTEENTH PARLIAMENT- SECOND SESSION - 2023

---


AD HOC COMMITTEE ON THE INQUIRY INTO THE ACTIVITIES OF  
WORLD COIN IN KENYA

---

REPORT ON  
THE INQUIRY INTO THE ACTIVITIES AND OPERATIONS OF WORLD COIN IN  
KENYA

# VOLUME - I

Clerk's Chambers  
Directorate of Departmental Committees  
National Assembly  
Parliament Buildings  
NAIROBI

 THE NATIONAL ASSEMBLY PAPERS LAYD		
DATE:	28 SEP 2023	DAY: Thursday
TABLED BY:	Hon Gabriel Tongoyo, MP Chairperson	SEPTEMBER, 2023
CLERK-AT THE TABLE:	Anne Shubuko	

## TABLE OF CONTENTS

CHAIRPERSON’S FOREWORD .....	iii
ACRONYMS AND ABBREVIATIONS .....	vi
LIST OF ANNEXES.....	viii
CHAPTER ONE .....	ix
1. PREFACE .....	ix
1.1 Establishment of the Committee .....	ix
1.2 Mandate of the Committee.....	ix
1.3 Timeline of the Committee.....	x
1.4 Membership of the Committee.....	x
1.5 Committee Secretariat.....	xi
CHAPTER TWO.....	1
2. BACKGROUND OF THE INQUIRY .....	1
2.1 INTRODUCTION.....	1
2.1.1 Request for Statement by Hon. Gitonga Mukunji, MP .....	1
2.1.2 Response from the Cabinet Secretary for Interior and National Administration and the Cabinet Secretary for Information, Communication and the Digital Economy .....	1
2.1.3 Establishment of <i>Ad hoc</i> Committee of the National Assembly to inquire into the activities and operations of Worldcoin in Kenya .....	4
2.2 LEGAL FRAMEWORK.....	5
2.2.1 The Constitution of Kenya, 2010 .....	5
2.2.2 Data Protection Act, 2019 .....	5
2.2.3 Companies Act, 2015 .....	10
2.2.4 Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010.....	11
2.3 INSTITUTIONAL FRAMEWORK.....	11
2.3.1 The Office of the Data Commissioner.....	11
2.3.2 Communications Authority of Kenya .....	12
2.3.3 Central Bank of Kenya.....	12
2.4 COMPARATIVE ANALYSIS .....	12
2.4.1 United States of America .....	13
2.4.2 Brazil .....	15
2.4.3 South Africa .....	17
2.4.4 United Arab Emirates.....	18

CHAPTER THREE .....	20
3.0 EVIDENCE BY WITNESSES .....	20
3.1 ATTENDANCE BY WITNESSES .....	20
3.2 SUBMISSIONS BY WITNESSES .....	21
3.3 SUBMISSIONS AS PER THE TERMS OF REFERENCE .....	26
3.3.1 Inquire into the Operations and Ultimate Objectives of the Activities of <i>Worldcoin</i> in Kenya .....	26
3.3.2 Inquire into the Legal and Regulatory Compliance of Operations of <i>Worldcoin</i> and its Agents in Kenya .....	35
3.3.3 Inquire Whether Due Diligence was Undertaken by the Relevant Government Agencies Before <i>Worldcoin</i> Started its Operations in Kenya .....	46
3.3.4 Inquire into the Nature, Use and Safety of Data Collected by <i>Worldcoin</i> in Kenya .....	49
3.3.5 Inquire into the Organizational Structure and the Activities of <i>Worldcoin</i> .....	60
3.3.6 Inquire into the Source of Money or Consideration if any Paid to the Members of the Public Who Presented Themselves for Registration and the Potential Beneficiaries .....	62
3.3.7 Inquire Whether Kenyans Were Exposed to any Health Hazards as a Results of the Activities of <i>Worldcoin</i> in the Country .....	65
3.3.8 Inquire into the Legal and Regulatory Gaps that Permitted Operations of <i>Worldcoin</i> in Kenya .....	66
3.3.9 Other Emerging Issues .....	73
CHAPTER FOUR .....	92
4.0 COMMITTEE FINDINGS AND OBSERVATIONS .....	92
4.1 Committee Findings .....	92
4.2 General Observations .....	99
CHAPTER FIVE .....	101
5.0 RECOMMENDATIONS OF THE COMMITTEE .....	101

## CHAIRPERSON'S FOREWORD

This Report contains proceedings, observations and recommendations of the *Ad hoc* Committee established on 15<sup>th</sup> August, 2023 to inquire into the activities of Worldcoin in Kenya.

The inquiry was prompted by a request for a statement from the Hon. Gitonga Mukunji, MP on Wednesday, 2<sup>nd</sup> August 2023, on the floor of the House. The issues raised in the Statement were not satisfactorily responded to by the Cabinet Secretary for the Ministry of Interior and National Administration and the Cabinet Secretary for the Ministry of Information Communication and the Digital Economy, leading to a ruling by the speaker of the National Assembly through the Speaker's Communication No. 055 of 2023, for the formation of an *Ad hoc* committee to inquire into the activities and operations of Worldcoin in Kenya. The speaker further directed the committee to engage concerned parties, but not limited to the relevant Ministries, Departments and Agencies, whose mandates have a bearing on the matter.

In conducting the inquiry, the *Ad hoc* committee set out nine (9) Terms of References including and not limited to; inquire into the operations and ultimate objectives of the activities of Worldcoin in Kenya; inquire into the legal and regulatory compliance of operations of Worldcoin, and its agents in Kenya; inquire whether due diligence was undertaken by the relevant government agencies before Worldcoin started its operations in Kenya; inquire into the nature, use and safety of data collected by Worldcoin in Kenya; inquire into the organizational structure and the activities of Worldcoin; inquire into the source of money or consideration if any paid to the members of the public who presented themselves for registration and the potential beneficiaries; inquire whether Kenyans were exposed to any health hazards as a results of the activities of Worldcoin in the country; inquire into the legal and regulatory gaps that permitted operations of Worldcoin in Kenya; and other emerging issues from the inquiry, which further generated several sub themes under them.

The *Ad hoc* Committee was to consider submissions by witnesses into the inquiry and make necessary observations and recommendations into the matter and submit its report to the House by Thursday, 28<sup>th</sup> September, 2023.

Further, into their inquiry, the *Ad hoc* Committee isolated the issues under consideration into two (2) broad categories of Data Protection and Virtual Assets. In dissecting the issues under consideration, the committee sought to understand the current legal framework which was noted to include the constitution of Kenya 2010, Article 31 (c) & (d) that provides that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed; and the privacy of their communications infringed. The other major statutes included the Data Protection Act, 2019, the Computer Misuse and Cybercrimes Act, 2018, the Kenya Information and Communications, 1998, the Companies Act, 2015 and the Kenya Information and Communications (Importation, Type Approval and

Distribution of Communications Equipment) Regulations, 2010. The major provisions relate to the registration of foreign firms in Kenya and the registration of data controllers and processors.

The committee went further to seek out best practices from other jurisdictions to help it appreciate data protection and virtual Assets. It was noted that the data protection law in the United States is a complex and evolving topic and that there is no single federal law that covers all aspects of data privacy, but rather a patchwork of sector-specific and state-level laws that regulate how personal data can be collected, used, shared and protected. The Committee noted that Worldcoin operated in Kenya despite the lack of regulation on virtual assets, but did not operate in the USA which they claimed lacked regulatory clarity on cryptocurrency leaving an impression that they exploited the weak legal framework in Kenya while respected that of USA despite the fact that both countries did not have regulations on virtual assets.

The Committee also reviewed jurisdictional comparisons of Brazil, South Africa and the United Arab Emirates. Of interest is the South African model which highlighted six principles to guide the approach on regulating CASPs in South Africa, to promote responsible innovation and regulate the conduct of these providers. Further, the United Arab Emirates (UAE) enacted Law No. 4 of 2022 on the Regulation of Virtual Assets (“VAL”). The law also established the Dubai Virtual Assets Regulatory Authority (“VARA”). It covers all virtual assets, including crypto assets and non-fungible tokens (NFTs). The Objectives of the Authority include to promote Dubai as a regional and international hub for Virtual Assets and related services; to boost its competitive edge at the local and international levels; and to develop the digital economy in Dubai.

In conducting the inquiry, the *Ad hoc* Committee also received witness submissions from the National Computer & Cybercrimes Coordination Committee (NC4), the Attorney General, Kenyatta International Convention Centre (KICC), the Communications Authority of Kenya (CA), the Cabinet Secretary, Ministry of Health (MoH), the Directorate of Criminal Investigations (DCI), the Central Bank of Kenya (CBK) and the National Treasury and Economic Planning, the Office of the Data Protection Commissioner (ODPC), the Cabinet Secretary, Ministry of Information, Communication and the Digital Economy, Sense Marketing Limited, the Capital Markets Authority (CMA), the Financial Reporting Centre (FRC), the Cabinet Secretary, Ministry of Interior and National Administration and the National Intelligence Service (NIS). Further, there were three members of the public who at the time were university students who participated in the Worldcoin activities. The Committee also invited Tools for Humanity Corp and Tools for Humanity GmbH (both trading as Worldcoin).

The *Ad hoc* Committee made findings based on each term of reference and drew general observations. The *Ad hoc* Committee observed that the Worldcoin project was founded with the mission of creating a digital identification platform (World ID) that aims to provide each person on earth with a convenient way to verify that they are real human and not a bot and further use

the attendant data to train AI algorithms for future technological advancements. The Committee observed that TFH Corp and TFH GmbH started operating in Kenya, way before making application for registration as data controllers and continued to operate in total disregard to the cessation orders and directives issued by Kenyan Authorities. Their activities therefore, violated the Kenyan laws.

The Committee further observed that Worldcoin's objective of decentralizing global monetary system is a threat to statehood. Unlike the fiat currency, cryptocurrency is a digital, encrypted and decentralized medium of exchange and that there is no central authority that manages and determines the value of the digital currency. Instead, the determination of the value of the virtual currency is through speculative tendencies of the users of the cryptocurrency. Cryptocurrencies pose security concerns due to their potential for anonymity, borderless transactions, difficulty in tracing decentralization, lack of third-party intermediaries, and limited regulation in Kenya.

In addressing the issues under determination from the findings and observation, the committee made the recommendations that will address the gaps in the legal framework and guide on the space of virtual assets in Kenya moving forward.

The Ad Hoc Committee wishes to thank the Office of the Speaker of the National Assembly, and the Office of the Clerk of the National Assembly for the support extended to the Committee in the execution of its mandate and the Secretariat for supporting the Committee. The Committee also extends its profound appreciation to all witnesses and members of the public that appeared before the Committee or submitted Memoranda for their informative and eloquent submissions on the matter.

It is now my pleasant duty and privilege, on behalf of the Ad Hoc Committee pursuant to Standing Order No. 259C(4) of the National Assembly Standing Orders to present this Report to the National Assembly.



**Hon. Gabriel Tongoyo, MP**

**Chairperson, *Ad Hoc* Committee on the Inquiry into the Activities of Worldcoin in Kenya**

## ACRONYMS AND ABBREVIATIONS

AFJOC	African Joint Operations against Cybercrime
AFRIPOL	African Union Police Initiative
AG	Attorney-General
AI	Artificial Intelligence
AWS	Amazon Web Services
BRS	Business Registration Service
CA	Communications Authority of Kenya
CAR	Cyber Activity Report
CBDCs	Central Bank Digital Currencies
CBK	Central Bank of Kenya
CFC	Cyber Fusion Centre
CII	Critical Information Infrastructure
DCI	Directorate of Criminal Investigations
DDoS	Distributed Denial of Service
EAPCCO	East Africa Police Chiefs Co-operation Organization
GBP	Great British Pound
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IGCI	Global Complex for Innovation
INTERPOL	The International Criminal Police Organization
IRA	Insurance Regulatory Authority
ISP	Internet Service Providers
KE-CIRT/CC	Kenya Computer Incident Response Team Co-ordination Centre
KES	Kenyan Shillings
KICA	Kenya Information and Communications Act, 1998.
KICC	Kenyatta International Conventional Centre
KRA	Kenya Revenue Authority
MoICT	Ministry of Information and Communication and Technology
NC4	National Computer and Cybercrimes Coordination Committee
NCB	National Central Bureau
NCSC	National Cyber Security Steering Committee
NFTs	Non-Fungible Tokens
NFTs	Non-Fungible Tokens
NSC	National Security Council
NSCC	National Security Council Committee
ODPC	Office of the Data Protection Commissioner
OTTs	Over-The Top Services
P2P	Peer-to-peer

PS	Principal Secretary
PVOC	Pre-Export Verification of Conformity Standard
RBA	Retirement Benefits Authority
SASSRA	Sacco Societies Regulatory Authority
UAE	United Arab Emirates
UNCTAD	United Nations Conference on Trade and Development
USD	United States Dollar
USDT	United States Department of the Treasury
VAT	Value Added Tax
WLD	Worldcoin Token
WTO	World Trade Organization



## LIST OF ANNEXES

<b>Annex 1</b>	Adoption List
<b>Annex 2</b>	Minutes of the Committee proceedings
<b>Annex 3</b>	Communication from the Chair No. 055 of 2023
<b>Annex 4</b>	Communication from the Chair No. 058 of 2023
<b>Annex 5</b>	Request for Statement by Hon. Gitonga Mukunji, MP
<b>Annex 6</b>	Joint response to the request for statement by Hon. Gitonga Mukunji, MP by the Ministry of Interior and National Administration and the Ministry of Information, Communication and the Digital Economy.
<b>Annex 7</b>	Public Notice calling for submissions from the members of public and notification on the dates and place for public hearings
<b>Annex 8</b>	Letters from the Clerk of the National Assembly to various witnesses.
<b>Annex 9</b>	Written submissions by witnesses. (VOLUME – II)

## CHAPTER ONE

### 1. PREFACE

#### 1.1 Establishment of the Committee

The *Ad hoc* Committee on the Inquiry into the Activities and Operations of Worldcoin in Kenya was established by the National Assembly pursuant to Standing Order 259C on Tuesday, 15<sup>th</sup> August 2023, vide Communication from the Speaker No. 055 of 2023 (*Annex 3*).

#### 1.2 Mandate of the Committee

Through a Communication from the Speaker, the Committee was mandated to among other things, inquire into the activities and operations of Worldcoin in Kenya and engage concerned parties, but not limited to the relevant Ministries, Departments and Agencies, whose mandates have a bearing on the matter.

During the first sitting held on Monday, 21<sup>st</sup> August, 2023, the Committee formulated Terms of Reference of the Inquiry as follows:

- 1) To inquire into the operations and ultimate objectives of the activities of *Worldcoin* in Kenya;
- 2) To inquire into the legal and regulatory compliance of operations of *Worldcoin*, and its agents in Kenya;
- 3) To inquire whether due diligence was undertaken by the relevant government agencies before *Worldcoin* started its operations in Kenya;
- 4) To inquire into the nature, use and safety of data collected by *Worldcoin* in Kenya;
- 5) To inquire into the organizational structure and the activities of **Worldcoin**;
- 6) To inquire into the source of money or consideration if any paid to the members of the public who presented themselves for registration and the potential beneficiaries;
- 7) To inquire whether Kenyans were exposed to any health hazards as a results of the activities of *Worldcoin* in the country;
- 8) To inquire into the legal and regulatory gaps that permitted operations of *Worldcoin* in Kenya; and
- 9) To recommend necessary legislative intervention.

### 1.3 Timeline of the Committee

The *Ad hoc* Committee was required to consider and inquire into the matter and submit its Report to the House by Thursday, 28<sup>th</sup> September, 2023.

### 1.4 Membership of the Committee

In Communication No. 058 of 2023 dated 17<sup>th</sup> August, 2023 (*Annex 4*) the Speaker directed that the Committee shall comprise fifteen (15) Members, five (5) Members each drawn from three Departmental Committees of the National Assembly whose mandate have a bearing on the matter, namely the Departmental Committee on Administration and Internal Security; the Departmental Committee on Communication, Information and Innovation; and the Departmental Committee on Tourism and Wildlife. Nomination of the Members was done through writing to the Speaker by the respective Committees Chairpersons.

The nomination took into consideration the Majority Party and Minority Party in the House. The Majority Party was allocated three (3) slots while the Minority Party was allocated two (2) slots, by each Committee.

The Speaker appointed the Hon. Gabriel Tongoyo, MP, as the Chairperson of the *Ad hoc* Committee from amongst Members of the Departmental Committee on Administration and Internal Security.

In Communication No. 058 of 2023 dated 17<sup>th</sup> August, 2023, the Speaker co-opted three other Members into the Committee.

The Membership of the Committee is as follows:

<b>Hon. Gabriel Tongoyo, MP - Chairperson</b> Departmental Committee on Administration and Internal Security	
<b>Hon. Kareke Mbiuki, CBS, MP - Chairperson</b> Departmental Committee on Tourism and Wildlife	<b>Hon. John Kiarie Waweru, MP - Chairperson</b> Departmental Committee on Communication, Information and Innovation
<b>Hon. Peter Kaluma, MP</b> Departmental Committee on Administration and Internal Security	<b>Hon. Sarah Korere, MP</b> Departmental Committee on Administration and Internal Security

<b>Hon. Mburu Kahangara, MP</b> Departmental Committee on Administration and Internal Security	<b>Hon. Caroline Ng'elechei, MP</b> Departmental Committee on Administration and Internal Security
<b>Hon. Shakeel Ahmed Shabbir, CBS, MP</b> Departmental Committee on Communication, Information and Innovation	<b>Hon. Geoffrey M. Wandeto, MP</b> Departmental Committee on Communication, Information and Innovation
<b>Hon. Gideon Kimaiyo Kipkoech, MP</b> Departmental Committee on Communication, Information and Innovation	<b>Hon. Irene Nyakerario Mayaka, MP</b> Departmental Committee on Communication, Information and Innovation
<b>Hon. Capt. Ruweida Obo, MP</b> Departmental Committee on Tourism and Wildlife	<b>Hon. Geoffrey Ruku, MP</b> Departmental Committee on Tourism and Wildlife
<b>Hon. (Dr.) Edwin Mugo Gichuki, MP</b> Departmental Committee on Tourism and Wildlife	<b>Hon. Innocent Mugabe, MP</b> Departmental Committee on Tourism and Wildlife
<b>Hon. Gitonga Mukunji, MP</b> Co-opted Member	<b>Hon. Umulkher Harun Mohamed, MP</b> Co-opted Member
<b>Hon. Fredrick Ikana, MP</b> Co-opted Member	

### 1.5 Committee Secretariat

<b>Mr. Daniel Mutunga</b> Deputy Director, Departmental Committees
---

<b>Ms. Hellen Kina</b> Clerk Assistant I	<b>Mr. Philip Lekarkar</b> Clerk Assistant I
<b>Mr. Douglas Katho</b> Clerk Assistant I	<b>Dr. Donald Manyala, PhD</b> Principal Research Officer
<b>Ms. Everlyne Claudia Orina</b> Clerk Assistant III	<b>Mr. Boaz Chebiego</b> Research Officer
<b>Ms. Delvin Onyancha</b> Research Officer	<b>Mr. Daniel Ominde</b> Research Officer
<b>Ms. Veron Aluoch</b> Research Officer	<b>Ms. Brenda Michira</b> Research Officer
<b>Mr. Martin Sigei</b> Research Officer	<b>Ms. Winnie Kiziah</b> Media Relations Officer
<b>Ms. Judith Kanyoko</b> Legal Counsel II	<b>Ms. Joyce Kakya Maleve</b> Hansard Officer II
<b>Ms. Rhoda Muchori</b> Hansard Officer II	<b>Mr. Danton Kimutai</b> Audio Officer
<b>Mr. Kelvin Lengasi</b> Audio Officer	<b>Ms. Victoria Wanjiku</b> Intern
<b>Mr. Samuel Nyambei</b> Serjeant-At-Arms	

## CHAPTER TWO

### 2. BACKGROUND OF THE INQUIRY

#### 2.1 INTRODUCTION

##### 2.1.1 Request for Statement by Hon. Gitonga Mukunji, MP

1. On Wednesday, 2<sup>nd</sup> August, 2023, the Hon. Gitonga Mukunji, MP, sought a statement (*Annex 5*) from the Cabinet Secretary for Interior and National Administration and the Cabinet Secretary, Ministry of Information Communication and the Digital Economy through the Leader of Majority Party as follows;
  - a) Given that the Ministry of Interior and the National Administration and Data Commissioner has cast doubt on the safety of Data collection by Worldcoin, could the Ministry provide the steps the government is taking to ensure control of data access, collection and storage especially by foreign entities.
  - b) Who authorized the biometric data collection by Worldcoin and were the correct procedures followed?
  - c) What are the safety guarantees that the government is making to ensure that the data will be exclusively used for the intended purpose and that citizens will suffer no loss?
  - d) Has the government established the ultimate objective of this exercise and for what purpose will the data collected be used?
  - e) Was there prior public participation to inform the public of the risks involved in the exercise?
  - f) What is the source of the money being paid to participants and who stand to benefit from the exercise?

##### 2.1.2 Response from the Cabinet Secretary for Interior and National Administration and the Cabinet Secretary for Information, Communication and the Digital Economy

2. In response to the Statement sought by the Hon. Gitonga Mukunji, M.P, the Cabinet Secretary for the Ministry of Interior and National Administration and the Cabinet Secretary for the Ministry of Information, Communication and the Digital Economy issued a joint preliminary response to the House on Wednesday, 9<sup>th</sup> August, 2023 (*Annex 6*).
3. In their joint statement, they stated that:
  - a) They had received information that an entity calling itself Worldcoin was reported to be harvesting eyeball/iris data from Kenyans in exchange for cryptocurrency tokens worth approximately KES 7,000 on condition that the beneficiaries allowed the scanning of their eyeballs/iris.
  - b) The entity was not registered as a legal entity in Kenya.

- c) Preliminary investigations had revealed that the entity had hired a local company in Kenya called Sense Marketing to do the data capture for them in the country.
- d) the local representatives of Worldcoin, Mr. Emmanuel Otieno who is described to be in charge of operations and Ms. Rael Mwendu who is described as the Country Manager, had been interrogated by the Directorate of Criminal Investigations (DCI).
- e) Among the foreign nationals associated with Worldcoin, are Mr. Piotr Piwowarczyk who was on record of having entered Kenya on several occasions, the last one being in June 2023 having arrived in the country on 11<sup>th</sup> June, 2023 and left on 25<sup>th</sup> June, 2023.
- f) On 2<sup>nd</sup> August 2023, the Government through the Ministry of Interior and National Administration had suspended the activities of Worldcoin in Kenya.
- g) Consequently, criminal investigations had been commenced to establish the authenticity and legality of the aforesaid activities, the safety and protection of the data being harvested and how the harvesters intended to use the data.
- h) It would be critical that the assurances of public safety and integrity of the financial transactions involving such a large number of citizens be satisfactorily provided upfront.
- i) All the activities of Worldcoin and any other entity that may be similarly engaging the people of Kenya stood suspended until the relevant public agencies certify the absence of any risks to the general public whatsoever.
- j) As a precautionary measure, the Immigration authorities had been directed to ensure that no persons whether Kenyan or foreign nationals associated with this entity left Kenya without the clearance of the Director of Criminal Investigations who is in charge of the ongoing investigations.
- k) The investigations would also cover any persons of interest who may be outside the territory of Kenya in accordance with relevant international procedures and protocols on Mutual Legal Assistance (MLA) and the exercise of extra- territorial jurisdiction.
- l) Earlier, the Office of the Data Protection Commissioner learnt that the company had setup booths across the country to scan the iris of interested Kenyans on 19<sup>th</sup> April 2022. This was in anticipation of the launch of their cryptocurrency. The Office of the Data Protection Commissioner commenced its assessment of the organisation in May 2022. In the course of its assessments, the Office initially suspended the operations of Worldcoin in May 2022 for a period of 60 days to ascertain the lawful basis and safeguards adopted by Worldcoin.
- m) Subsequently, the Office of the Data Protection Commissioner conducted a spot check on 24<sup>th</sup> May 2023. The Office, again, raised concerns with the processing activities of the entity and wrote to the entity on 30<sup>th</sup> May 2023 directing the immediate cessation of processing of sensitive personal data, namely: iris and facial data of data subjects. The Office had further directed that Worldcoin safely restricts processing of any data that had already been processed and advise on the safeguards placed on the restricted data.
- n) The Government had registered Worldcoin as a data controller, pursuant to the Data Protection Act, 2019 and the Data Protection Registration of Data Controllers and Data

Processors Regulation, 2021 (Registration Regulations) which requires that entities processing data should be registered with the Office of the Data Commissioner. Such registration was to be done by applying through the ODPC registration portal.

- o) An application for a certificate of registration only signified that an entity had complied with section 18 and 19 of the Act and did not endorse an entity's compliance with the Data Protection Act or its subsidiary regulations, nor was it a valid license for an organisations to operate in Kenya or authorize the operations of an entity. The certificate merely signified that an entity was known to the Office of the Data Protection Commissioner that it processes personal data of persons located in Kenya. Further, it did not amount to certification of the processing activities of an entity or serve as an endorsement of an entity's compliance with other provisions of the Act or any other laws.
- p) A registration certificate had been issued to Worldcoin on 18<sup>th</sup> April 2023 following receipt of the requisite documentation pursuant to the Data Protection Registration Regulations.
- q) The Government had commenced investigations to ensure that Worldcoin complied with the data collection, storage and sharing principles. Immediate mitigation steps had been undertaken and constitution of a multi-agency team comprising of security, financial services and data protection agencies had commenced inquiries and investigations to establish the legality of the activities of Worldcoin, the safety and the protection of data collected with the aim to safeguard personal data and mitigate against any adverse practices.
- r) The government was not aware of any prior public participation exercise by the crypto firm. This was the reason the Government had issued cautionary statements by the Office of the Data Protection Commissioner on 28<sup>th</sup> July 2023 advising the public to be vigilant when engaging with Worldcoin and, in particular, when providing sensitive personal data.
- s) Further, the Communications Authority and the Office of the Data Protection Commissioner had issued a joint statement on 2<sup>nd</sup> August 2023 raising concerns on the operations of Worldcoin as they related to cybersecurity, data protection and consumer protection.
- t) The Government was not aware of the source of funds and that part of the multi-agency team mandate would be to investigate the source of the money that had been issued to the participants and the beneficiaries of this activity.
- u) The Government had expressly directed Worldcoin to cease the collection of personal data and to restrict the further processing of any data that had already been collected from persons located in Kenya. Further, there was need to sensitize Kenyans on the risks of cybersecurity attacks, data breaches and the need for full disclosure before giving consent.
- v) The suspension of the processing of sensitive personal data was not lifted by the ODPC. In particular, the Office raised concerns on whether the consent sought from individuals was voluntary or illusory. In this regard, the Office noted that persons were requested to



give consent and a monetary incentive was provided for the exchange of sensitive personal data.

### **2.1.3 Establishment of *Ad hoc* Committee of the National Assembly to inquire into the activities and operations of Worldcoin in Kenya**

4. In the Speaker's Communication No 055 of 2023, it was noted that the Cabinet Secretaries could not satisfactorily respond to all the issues raised forthwith, as it became apparent that their explanations raised more Supplementary Questions than provided answers.
5. In this regard, the Cabinet Secretary for Interior and National Administration; and his counterpart for Information, Communication, and the Digital Economy, were asked to retreat and come before the plenary of the House on Wednesday, 16<sup>th</sup> August, 2023, to provide more comprehensive responses on the activities and operations of Worldcoin in the country.
6. In the Communication, the speaker noted that he had received a request from the Cabinet Secretary for Interior and National Administration on the subject matter, seeking his consideration of various approaches for inquiring into the activities and operations of Worldcoin in Kenya. In the request, the Cabinet Secretary suggested the following options –
  - i) That, the relevant Cabinet Secretaries, whose mandates had a bearing on the matter, including the Attorney General, appear separately before the plenary of the House to respond to the matter;
  - ii) That, the relevant Cabinet Secretaries and Heads of Agencies, whose mandates had a bearing on the matter, appear before the relevant Departmental Committees or an *ad hoc* Committee; or
  - iii) That, the relevant Ministries, Departments and Agencies, whose mandates had a bearing on the matter, provide information on the subject matter to the Prime Cabinet Secretary, who would then appear before the plenary of the House.
7. Having carefully considered the three suggested options and to avoid any further equivocation on the matter, the Speaker directed that an *Ad hoc* committee be formed to inquire into the activities of Worldcoin in Kenya.
8. On Tuesday 15<sup>th</sup> August 2023, the Speaker of the National Assembly, informed the House vide Communication No. 055 of 2023 on the establishment of an *Ad hoc* Committee to inquire into the activities and operations of Worldcoin in Kenya.
9. In the Communication, the Speaker directed that an *Ad hoc* Committee of the House comprising fifteen (15) Members, five (5) each drawn from the Departmental Committee on Administration and Internal Security, Departmental Committee on Communication

Information and Innovation and the Departmental Committee on Tourism and Wildlife, to investigate into the activities and operations of Worldcoin. Further, the Speaker in Communication 058 of 2023, coopted three (3) Honourable Members to the Committee.

10. The nomination of Members to the *Ad hoc* Committee was to be in writing to the Speaker, by the respective Chairpersons of the three Committees, taking into consideration the majority party and minority party membership of the House. In this case, the Majority Party was to be allocated three (3) slots while the Minority Party was to be allocated two (2) slots, by each Committee.
11. The mandate of the *Ad hoc* Committee was to inquire into the activities and operations of Worldcoin in Kenya and engage the concerned parties, but not limited to the relevant Ministries, Departments and Agencies whose mandates have a bearing on the matter. The *Ad hoc* Committee was to consider and inquire into the matter and submit its report to the House by Thursday, 28<sup>th</sup> September 2023.

## **2.2 LEGAL FRAMEWORK**

12. The activities of Worldcoin fall under two thematic areas, that is data protection and virtual assets. This section sets out the applicable laws in Kenya.

### **2.2.1 The Constitution of Kenya, 2010**

13. Article 31 (c) & (d) of the Constitution provides that every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed; and the privacy of their communications infringed.

### **2.2.2 Data Protection Act, 2019**

14. In order to implement Article 31(c) and (d) of the Constitution, Parliament enacted the Data Protection Act of 2019. The objectives of the Act include the regulation of personal data processing, adherence to the principles of data processing, safeguarding the privacy of individuals, establishing the necessary legal and institutional framework for personal data protection, and granting data subjects rights and remedies to safeguard their personal data.
15. Section 4(a) of the Data Protection Act provides that the Act applies to the processing of personal data, whether automated or non-automated, entered into a record, and conducted either by or for a data controller or processor. It is important to note that when personal data is processed through non-automated means, it must be part of a filing system, either in its entirety or as a component, to fall within the Act's jurisdiction.

16. Additionally, section 4(b) of the Data Protection Act extends the applicability of the Act to the processing of personal data by a data controller or data processor. The Act envisions data controllers and processors to include those entities that are either physically established or ordinarily resident within Kenya and engage in personal data processing while within the country's borders. It also covers situations where the data controller or processor is not physically based or ordinarily resident in Kenya but is involved in processing personal data of individuals situated in Kenya.

### **Registration of data controllers and processors**

17. The Data Protection Act requires the registration of both data controllers and data processors. For instance, section 18(1) of the Act explicitly states that no individual or entity can function as a data controller or data processor unless they have completed the registration process with the Data Commissioner. Furthermore, under section 18(2) of the Act, the Data Commissioner is tasked with the responsibility of establishing the specific thresholds that necessitate mandatory registration for data controllers and data processors. The threshold is determined by considering factors such as the nature of the industry, the quantity of data being processed, and whether sensitive personal data is involved.
18. Section 19 of the Act sets out specific requirements for the registration application process for those seeking to become data processors or data controllers. These requirements are designed to provide a comprehensive understanding of the intended data processing activities and ensure adherence to data protection standards. For instance, an applicant must provide a detailed description of the personal data the applicant intends to process as a data controller or processor.
19. The application must also articulate the purpose behind processing this personal data, shedding light on the objectives driving these data processing activities. The application must also specify the category or categories of data subjects to whom the personal data relates, ensuring clarity on the individuals whose data is involved. It must also contain the contact details of the data controller or data processor are essential for communication and administrative purposes.
20. An application for registration should also incorporate general description of the potential risks, along with the safeguards, security measures, and mechanisms to protect personal data. Moreover, applicants are required to outline any measures aimed at indemnifying data subjects against potential unlawful use of their data by the data processor or data controller, emphasizing the protection of individual rights.
21. If satisfied that a data controller or data processor has met the requirements for registration, the Data Commissioner shall issue a certificate of registration valid for a period determined

at the time of the application after taking into account the need for the certificate, and the holder may apply for a renewal of the certificate after expiry of the certificate.

22. The Data Commissioner may, on issuance of a notice to show cause, vary terms and conditions of the certificate of registration or cancel the registration where any information given by the applicant is false or misleading; or the holder of the registration certificate, without lawful excuse, fails to comply with any requirement of the Data Protection Act.

#### **Cancellation or variation of the certificate**

23. Section 23 of the Data Protection Act outlines the authority of the Data Commissioner to conduct periodic audits of data controllers and data processors. The primary objective behind these audits is to verify and ensure compliance with the Data Protection Act. In essence, this provision empowers the Data Commissioner to periodically assess and evaluate the data handling practices of these entities to ascertain that they adhere to the stipulated data protection regulations.
24. Section 22 of the Act empowers the Data Commissioner to issue **notice to show cause**, a procedural step that allows the Commissioner to seek explanations and justifications from the parties involved. If, during this process, it is determined that the applicant provided false or misleading information during the registration process, or if the holder of the registration certificate fails to comply with any requirements laid out in the Act without a lawful excuse, the Data Commissioner has the prerogative to either vary the terms and conditions of the certificate of registration or cancel the registration.

#### **Principles of data protection**

25. Section 25 of the Data Protection Act lays down essential principles that every data controller and data processor must uphold in their handling of personal data. These principles serve as a foundational framework for ensuring the protection of the right and privacy of the data subjects. For instance, the Act requires data processing to be conducted in a lawful, fair, and transparent manner in relation to the data subject.
26. Additionally, the collection of personal data should be explicit, specified, and for legitimate purposes, with strict limitations on any further processing that might be incompatible with these initial objectives. Furthermore, the data collected should be adequate, relevant, and limited to what is strictly necessary for the intended purposes.
27. Moreover, when information regarding family or private affairs is required, it should only be collected when a valid explanation is provided, underlining the sensitivity and discretion necessary in such cases. Accuracy in maintaining personal data is crucial, with steps taken to promptly erase or rectify any inaccuracies as needed. The Act further stipulates that data

should not be retained in a form identifying data subjects for longer than necessary for the original purposes of collection.

28. Lastly, transferring personal data outside of Kenya is permissible only when adequate data protection safeguards are in place or with the explicit consent of the data subject.
29. Section 26 of the Data Protection Act guarantees the subjects the right to be informed about how their personal data will be used, ensuring transparency in data processing practices. Data subjects also have the right to access their personal data held by data controllers or processors, promoting transparency and control over their information.
30. Further, data subjects have the right to object to the processing of all or part of their personal data, giving them a say in how their data is utilized. In cases of false or misleading data, data subjects have the right to request corrections to ensure the accuracy of their information. Data subjects can also request for the deletion of false or misleading data concerning them, emphasizing their right to control the integrity of their personal information.

#### **Collection and processing of personal data**

31. Section 28(1) of the Data Protection Act obligates data controllers and data processors to collect personal data directly from the data subject. However, personal data may be collected indirectly where the data is publicly available, the data subject has intentionally made their data public, consent from the data subject is obtained for collection from another source, the data subject is incapacitated (with consent from their guardian), or collecting from another source does not harm the interests of the data subject.
32. Section 32(1) of the Data Protection Act requires a data controllers or processors to ensure that a data subject has given consent for the processing of their personal data for a specific purpose. Further, section 32(2) guarantees the right of data subjects to withdraw their consent at any time, unless otherwise specified in the Act. Importantly, section 32(3) clarifies that the withdrawal of consent does not impact the legality of prior data processing activities based on the initial consent. Finally, section 32(4) highlights that when assessing the freedom of consent, factors such as whether the performance of a contract or service is contingent upon unnecessary data processing consent must be considered, reinforcing the importance of voluntary consent in data processing practices.
33. Section 28(3) emphasizes that personal data must only be collected, stored, or used for lawful, specific, and explicitly defined purposes. Before gathering personal data, section 29 of the Data Protection Act mandates data controllers and processors to inform data subjects about their rights, disclosing the fact that personal data is being collected, specifying the purpose for collection, indicating any third parties to whom the data may be transferred (along with details of protective measures), providing contact information for the data controller or

processor, mentioning whether any other entity may receive the collected data, describing the security measures in place to maintain data integrity and confidentiality, stating if data collection is based on any laws, and outlining the consequences if the data subject fails to provide requested data.

34. Moreover, section 30(1) (a) stipulates that data controllers and processors cannot process personal data without the consent of the data subject. Section 30(1)(b) further specifies conditions under which personal data may be processed without explicit consent. The conditions include performance of a contract involving the data subject, compliance with legal obligations, protection of vital interests, public interest tasks, tasks carried out by public authorities, legitimate interests of the data controller or processor (except when it unjustly harms data subject rights), and purposes related to historical, statistical, journalistic, literary, artistic, or scientific research.

#### **Retention, rectification, erasure and transfer of personal data**

35. Section 39(1) of the Data Protection Act dictates that personal data should only be retained for as long as necessary for its intended purpose, except when retention is mandated by law, needed for lawful purposes, authorized by the data subject, or required for historical, statistical, journalistic, literary, artistic, or research purposes. Further, section 39(2) obligates data controllers and processors to delete, erase, anonymize, or pseudonymize personal data that no longer needs retention as specified when the retention period expires.
36. Further, section 40(1) of the Data Protection Act grants data subjects the right to request data controllers or processors to promptly correct inaccuracies, out-of-date, incomplete, or misleading personal data, or to erase or destroy data that is no longer authorized for retention, irrelevant, excessive, or obtained unlawfully. Section 40(2) emphasizes the responsibility of data controllers or processors to inform third parties with whom they have shared personal data for processing when a data subject requests corrections or erasure of their data.
37. For transfer of personal data outside Kenya, section 48(a) of the Data Protection Act permits the transfer of personal data to another country, provided the data controller or processor can demonstrate to the Data Commissioner that appropriate safeguards ensuring the security and protection of personal data are in place. Section 48(c) outlines specific scenarios where data transfers are permissible, including for contract fulfillment, public interest matters, legal proceedings, protection of vital interests, or the pursuit of legitimate interests by the data controller or processor, as long as they do not infringe upon the rights and freedoms of data subjects.

### **2.2.3 Companies Act, 2015**

38. According to Section 974(1) of the Companies Act, a foreign company is prohibited from conducting business in Kenya unless it is duly registered or has submitted an application for registration, which remains unprocessed within the prescribed time frame. Section 974(2) of the Act expands the definition of carrying on business in Kenya to encompass activities such as offering debentures in Kenya or acting as a guarantor for debentures offered in Kenya. Engaging in business activities without fulfilling the registration requirement constitutes an offense attracting a fine of up to five million shillings.

#### **Procedure for registration of foreign companies**

39. To register as a foreign company, an application must be submitted along with several documents, including a certified copy of the certificate of registration of the foreign company from its home country or an equivalent document; and a certified copy of the company's constitution. The company is also required to submit a list of directors and shareholders with their personal information. If the list includes directors residing in Kenya and serving on a local board, the company shall also submit a memorandum outlining their powers. The Act also requires details of any existing property charges that would require registration under the Companies Act.

40. Upon registration, the Registrar is required to allocate the company a unique identifying number and issue to the company a certificate of compliance. Section 975(5) requires the certificate of compliance to state the name of the company, its unique identifying number, the fact that the company is registered as a foreign company, the date of its registration as a foreign company and the date of its incorporation in its place of origin.

#### **Local representatives of foreign companies**

41. Section 979(1) of the Companies Act stipulates that a foreign company cannot be registered unless it has at least one local representative who meets the prescribed requirements. The local representative of a registered foreign company assumes responsibility for ensuring that all required actions are taken on behalf of the company and can be held personally liable for any penalties imposed on the company due to violations or non-compliance with the Companies Act.

42. Further, section 979(3) of the Companies Act provides that failure by a registered foreign company to adhere to the local representative requirement results in an offense, with both the company and any officer in default subject to potential fines of up to five hundred thousand shillings upon conviction.

## **2.2.4 Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010**

43. Regulation 24 of these Regulations makes it an offence to deal in or use communication equipment without type approval or acceptance, and prescribes a penalty of a fine not exceeding three hundred thousand shillings or to imprisonment for a term not exceeding three years or to both.

## **2.3 INSTITUTIONAL FRAMEWORK**

44. Having noted that the activities of Worldcoin fall under two thematic areas, that is data collection and virtual currency, this section now sets out the relevant institutions in Kenya mandated to oversee the implementation of the applicable laws.

### **2.3.1 The Office of the Data Commissioner**

45. Section 5 of the Data Protection Act, 2019 establishes the Office of the Data Protection Commissioner (ODPC) as the central institution responsible for overseeing and enforcing the Data Protection Act and maintaining a register of data controllers and data processors. Section 8(1) of the Act assigns the ODPC a comprehensive set of functions to ensure the effective implementation and enforcement of Data Protection Act and the attendant regulations.
46. The ODPC has the authority to scrutinize data processing activities, whether initiated independently or upon a data subject's request, to verify their alignment with the Act. It thus plays a role in fostering self-regulation among data controllers and processors.
47. The functions of the ODPC extend to conducting assessments of public and private entities, either on its own motion or upon request, to ascertain compliance with data protection laws. It also serves as a platform for individuals to file complaints regarding infringements of their rights under the Data Protection Act. Furthermore, the ODPC is responsible for public awareness efforts, disseminating information about data protection provisions.
48. As a regulator, the ODPC conducts inspections of both public and private organizations to assess how personal data is being processed. Internationally, the ODPC promotes cooperation in data protection matters and ensures the country's adherence to data protection obligations outlined in international conventions and agreements. Lastly, it conducts research to stay abreast of developments in personal data processing and assesses potential risks or adverse effects on individuals' privacy, thereby upholding the overarching goal of safeguarding personal data in the digital age.
49. Further, section 9 of the Act confers significant authority on the Data Commissioner to execute a range of crucial functions essential for the effective implementation and



enforcement of data protection measures. For instance, the Data Commissioner possesses the autonomy to initiate investigations independently or in response to complaints from data subjects or third parties. In pursuit of these investigations, the Commissioner can seek professional assistance, consultation, or advice from relevant individuals or organizations, whether within or outside the public service.

50. Furthermore, the Data Commissioner has the prerogative to require any entity subject to the Data Protection Act to furnish explanations, information, and assistance, both in person and in writing, to aid in compliance and enforcement efforts. Notably, the Commissioner possesses the authority to impose administrative fines in cases of non-compliance with the Act, thereby promoting adherence to Data Protection Act and regulations.
51. In line with their mandate, the Data Commissioner is entrusted with the flexibility to undertake any necessary activities to fulfill the functions of the Office. Additionally, they can exercise any powers prescribed by other relevant legislation, ensuring a comprehensive approach to data protection and regulatory enforcement. This multifaceted authority underscores the important role of the Data Commissioner in upholding data protection standards and safeguarding individuals' privacy rights.

### **2.3.2 Communications Authority of Kenya**

52. The Kenya Information and Communications Act, 1998 establishes the Communications Authority of Kenya (CA), responsible for licensing and regulating postal, information, and communication services in accordance with the provisions of the Act. Any person intending to operate a telecommunication system must follow the prescribed application process with the Communications Authority of Kenya. A license granted under the Act can authorize the connection of other telecommunication systems and specified telecommunication apparatus to the system covered by the license.

### **2.3.3 Central Bank of Kenya**

53. The Central Bank of Kenya is established under the Central Bank of Kenya Act, 491. Its principal object is to formulate and implement monetary policy directed to achieving and maintaining stability in the general level of prices. This includes regulation of cryptocurrencies through regulations and issuance of advisories.

## **2.4 COMPARATIVE ANALYSIS**

54. This is an analysis of the status of data protection and cryptocurrency in a few jurisdictions around the globe, highlighting their legislative, policy and institutional interventions.

## 2.4.1 United States of America

### *Data Protection*

55. The data protection law in the United States of America is a complex and evolving topic. There is no single federal law that covers all aspects of data privacy, but rather a patchwork of sector-specific and state-level laws that regulate how personal data can be collected, used, shared and protected.
56. It incorporated both general federal legislative and policy frameworks that impact data protection on data protection which among others include:
- a) The Federal Trade Commission Act (FTC Act), which empowers the FTC to enforce consumer protection and data privacy regulations against unfair or deceptive practices by businesses.
  - b) The Health Insurance Portability and Accountability Act (HIPAA), which sets standards for how health care providers and other covered entities can use and disclose personal health information.
  - c) The Gramm-Leach-Bliley Act (GLBA), which requires financial institutions to protect the privacy and security of customer information and to provide notice and choice about how such information is shared.
  - d) The Children's Online Privacy Protection Act (COPPA) prohibits the online collection of personal information from children under 13 without verifiable parental consent and requires online services to post privacy notices and implement reasonable security measures.
57. In addition to these federal laws, several states have enacted their own data privacy laws that offer more protection or rights to their residents. For example, California has the California Consumer Privacy Act (CCPA), which grants consumers the right to access, delete, and opt out of the sale of their personal information by businesses that operate in California or collect data from California residents.
58. Other states, such as New York, Virginia, and Colorado, have also passed or proposed comprehensive data privacy laws that are similar to or inspired by the CCPA.
59. Data protection law in the United States is influenced by the developments in other jurisdictions, especially the European Union, which has a comprehensive data privacy law called the General Data Protection Regulation (GDPR). The GDPR majorly applies to organizations that offer goods or services to individuals in the EU or monitor their behaviour, regardless of where the organization is located.

60. The GDPR grants an individual various rights over their personal data, such as the right to access, rectify, erase, restrict, port, and object to the processing of their data. The GDPR also imposes strict obligations on data controllers and processors, such as conducting data protection impact assessments, appointing data protection officers, and reporting data breaches within 72 hours.

### *Virtual Assets*

61. The regulatory landscape for cryptocurrencies in the United States is currently in a state of evolution, marked by a mix of agency viewpoints, overlapping jurisdictions, and ongoing efforts to coordinate regulatory measures. While the Securities and Exchange Commission (SEC) is often perceived as the most influential regulatory body, other agencies like the Treasury's Financial Crimes Enforcement Network (FinCEN), the Federal Reserve Board, and the Commodity Futures Trading Commission (CFTC) have each offered their distinct interpretations and guidance on cryptocurrency-related matters. To foster cohesion and clarity within this complex regulatory environment, the White House issued an Executive Order, mandating greater collaboration and coordination among these agencies.
62. Diverging views on cryptocurrencies abound among these regulatory bodies. The SEC frequently classifies many cryptocurrencies as securities, emphasizing investor protection and disclosure requirements. In contrast, the CFTC designates Bitcoin as a commodity, stressing the importance of market integrity and oversight. Meanwhile, the Treasury Department categorizes cryptocurrencies as a form of currency, focusing on matters related to money laundering and financial crime prevention. Addressing these discrepancies in definitions, regulatory scope, and jurisdictional boundaries is paramount, and two key entities, the President's Working Group and the Financial Stability Oversight Council, are expected to play crucial roles in shaping a cohesive and comprehensive regulatory framework for the future.
63. From a tax perspective, the Internal Revenue Service (IRS) has defined cryptocurrencies as a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In line with this definition, the IRS has issued tax guidance that requires cryptocurrency investors to report their annual cryptocurrency activities on their tax returns. This underscores the U.S. government's commitment to ensuring compliance and revenue collection in the rapidly growing cryptocurrency sector.
64. Notably, the United States holds a prominent position in the global cryptocurrency ecosystem. It boasts the largest number of crypto investors, houses numerous cryptocurrency exchanges and trading platforms, hosts a substantial presence of cryptocurrency mining operations, and is home to a flourishing ecosystem of cryptocurrency investment funds. This significant

involvement underscores the country's role as a key player in shaping the future of cryptocurrencies, both in terms of regulation and market development.

## **2.4.2 Brazil**

### ***Data Protection***

65. The LGPD, or Lei Geral de Proteção de Dados, is Brazil's General Data Protection Law that regulates the collection, processing, disclosures, and erasure of personal data. The LGPD borrows heavily from the GDPR especially on the definition of personal data and the data subject rights.
66. As does the GDPR, the LGPD provides for extraterritorial jurisdiction. Art. 3 states that the law applies to any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarter is located or the country where the data are located.
67. The legal foundations for data processing vary between the regulations, with the LGPD including research activities and credit score safeguarding. Furthermore, the LGPD doesn't define a specific timeframe for reporting data breaches, and its penalties for violations are comparatively less severe than those under the GDPR.
68. Both the LGPD offer protection for processing of sensitive data and specifically protection against biometric data processing.
69. The LGPD and the Kenyan Data Protection Act both provide for data protection clauses in regard to research activities. The LGPD further protects data privacy in relation to processing for credit score activities unlike the Kenyan Data Protection Act.

### ***Virtual Assets***

70. According to CoinMarketCap, approximately 10 million Brazilians participate in the crypto market. This has led to Brazilian Legislators proposing a series of regulations on cryptos in the past several years as well as creating a regulatory sandbox. They came up with regulatory framework for the virtual currency market in order to reduce the risks of virtual currencies against the financial stability of the economy, reduce the possibility of them financing illegal activities and to protecting the consumer against possible abuses.
71. The virtual asset service provider carries out the exchange between virtual assets and national or foreign currency, exchange between one or more virtual assets, transfer of virtual assets, custody or administration of virtual assets or instruments that enable control over virtual assets and participation in financial services and provision of services related to the offering by an issuer or sale of virtual assets.

72. In order to provide virtual asset services, virtual service providers must comply with certain guidelines such as free initiative and free competition, good governance practices and risk-based approach, information security and protection of personal data, protection and defense of consumers and users, protection of popular savings, soundness and efficiency of operations and prevention of money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction, in alignment with international standards.
73. The government has also declared that bitcoin is an asset and therefore is subject to capital gains taxes and that the existing Anti-Money Laundering (AML) laws extend to virtual currencies in certain contexts. The Special Department of Federal Revenue of Brazil has published a document on cryptocurrency taxes in the country that establishes and regulates the obligation to provide information relating to operations carried out with cryptoactives to the Special Secretariat of the Federal Revenue of Brazil (RFB).
74. Further, Companies must follow standards for communicating financial operations, identifying customers and maintaining records. Institutions authorized to operate by the Central Bank of Brazil may exclusively provide the service of virtual assets, or combine it with other activities, in accordance with the regulations to be issued by a body or entity of the Federal Public Administration indicated in an act of the Executive Branch.
75. The Brazilian government has classified the crime of fraud in the provision of virtual asset services as organizing, managing, offering portfolios or intermediating operations involving virtual assets, with the aim of obtaining an illicit advantage, to the detriment of others, inducing or keeping someone in error, through artifice, ruse, or any other fraudulent means. The penalty is imprisonment for four to eight years and a fine. If the virtual asset service provider operates without authorization, it will be committing a financial crime, with imprisonment for one to four years and a fine.
76. To promote innovation in payment services, demanded by the accelerated digital transformation underway in the global economy, the discussion about the issuance of digital currencies by central banks (Central Bank Digital Currencies - CBDCs) has gained prominence over the last few years in Brazil. The Banco Central do Brasil (BCB) has been promoting discussions, internally and with its international peers, aiming at the possible development of a CBDC that may keep up with the dynamic technological evolution of the Brazilian economy, enhance the efficiency of the retail payment system, foster new business models and other innovations based on technological advances and favor Brazil's participation in regional and global economic scenarios, increasing efficiency in cross-border transactions with consideration that any developments stemming from this environment of innovation will be consistent with the BCB's mission of ensuring the stability of the currency

purchasing power, fostering a sound, efficient and competitive financial system and promoting the economic well-being of society.

### 2.4.3 South Africa

#### *Data Protection*

77. Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy: - the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information; the State must respect, protect, promote and fulfil the rights in the Bill of Rights.
78. The Protection of Personal Information Act<sup>1</sup> (POPIA) is a comprehensive data protection and privacy law in South Africa. It was enacted in 2013 and fully implemented on July 1, 2021.
79. Section 1 provides for definitions, for example ‘biometrics’ which means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition, “personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— biometric information relating to a person, information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person, among others.
80. Section 5 of the Act provides that, a data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information including the right:
- a) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information;
  - b) to request, where necessary, the correction, destruction or deletion of his, her or its personal information;
  - c) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person; -“Automated means”, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.
  - d) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject.
81. Section 9 provides that Personal information must be processed—lawfully; and in a reasonable manner that does not infringe the privacy of the data subject.

---

<sup>1</sup> [Protection of Personal Information Act \(POPI Act\) - POPIA](#), Retrieved on 28-08-2023

82. The Act recognizes retinal scanning as a part of personal biometric information and provides specific rights of the data subjects.

### ***Cryptocurrency in South Africa***

83. Since the release of the Bitcoin white paper in 2012, the crypto asset ecosystem in South Africa has grown to include more than 10 000 unique crypto assets as at November 2021. The Intergovernmental Fintech Working Group (IFWG) of South Africa reiterates the position globally by Policymakers, regulators and central banks, that crypto assets are not ‘money’ in the legal tender sense of the word, although they perform some of the functions of money.

84. Their challenge was how to achieve regulatory and legal certainty in the most appropriate and responsible manner possible to which they issued a position paper in 2020 that sets out 25 recommendations for a revised South African policy, legal and regulatory position on crypto assets and related activities, and essentially provides a roadmap to putting in place a framework for regulating crypto asset service providers in South Africa.

85. The Intergovernmental Fintech Working Group (IFWG) agreed and proposed six principles to guide the approach on regulating CASPs in South Africa. They include: Principle 1- crypto asset service providers (CASPs) must be regulated, and regulated appropriately; Principle 2- An activities-based perspective must be maintained, and the principle of ‘same activity, same risk, same regulations must continue to apply and inform the regulatory approach; Principle 3 - Proportionate regulations that are commensurate with the risks posed must apply (i.e. a risk-based approach to crypto asset regulation must apply); Principle 4 - A truly collaborative and joint approach to crypto asset regulation must be maintained; Principle 5 - Continue to proactively monitor the dynamic development of the crypto assets market, including maintaining knowledge on emerging international best practices (through standard-setting bodies, etc); and Principle 6: Digital literacy and digital financial literacy levels must be increased amongst consumers and potential consumers of crypto assets. These principles guiding regulation of CASPs aims to promote responsible innovation and regulate the conduct of these providers.

## **2.4.4 United Arab Emirates**

### ***Data Protection***

86. Data Privacy in the UAE is governed by the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data.

87. The law defines data, personal data, and sensitive personal data and makes provision for the processing of personal data both within and outside the UAE. It prohibits the processing of

personal data without the data subject's consent and provides for the obligations of data controllers and processors. It obligates a data controller to take appropriate technical and organizational procedures and measures to implement the standards necessary to protect and secure personal data in order to preserve its confidentiality and privacy. It also requires data controllers to inform the Data Office of any data breach. It further allows the data subject the right for correction of their data and provides a complaints mechanism where a data subject is aggrieved by the manner of processing their data. It also sets out the requirements for the transfer of data outside the UAE.

### *Cryptocurrency*

88. The Emirate of Dubai enacted Law No. 4 of 2022 on the Regulation of Virtual Assets ("VAL"). The law also established the Dubai Virtual Assets Regulatory Authority ("VARA"). It covers all virtual assets, including crypto assets and NFTs. The Objectives of the Authority include to promote Dubai as a regional and international hub for Virtual Assets and related services; to boost its competitive edge at the local and international levels; and to develop the digital economy in Dubai. The Authority is also mandated to increase awareness on investment in the Virtual Asset services and products sector and encourage innovation in the sector. Further, it is the Authority's objective to contribute to attracting investments and encourage companies operating in the field of Virtual Assets to base their business in the Dubai, to develop the regulations required for the protection of investors and dealers in Virtual Assets, and to endeavour to curb illegal practices in coordination with the concerned entities; and to develop the regulations, rules, and standards required for regulating, supervising, and overseeing Virtual Asset Platforms, Virtual Asset Service Providers, and all other matters related to Virtual Assets.
89. The law sets out activities that require a permit from the Authority and prohibits involvement in these activities without a permit. These activities include the provision of Virtual Asset Platform operation and management services, provision of services for the exchange between Virtual Assets and national or foreign currencies, provision of services for the exchange between one or more forms of Virtual Assets, provision of Virtual Asset transfer services;, provision of Virtual Asset safekeeping, management, or control services, provision of services related to Virtual Asset Wallets; and provision of services related to offering, and trading in, Virtual Tokens.
90. The law also provides for a grievance procedure and encourages cooperation of all stakeholders and other government agencies in the execution of the Authority's mandate.



## CHAPTER THREE

### 3.0 EVIDENCE BY WITNESSES

#### 3.1 ATTENDANCE BY WITNESSES

91. The Ad Hoc Committee, pursuant to Article 125 of the Constitution received evidence and information from witnesses on diverse dates from 29<sup>th</sup> August, 2023 to 18<sup>th</sup> September, 2023. This involved the invitation of various witnesses to adduce evidence to the Committee on itemised issues, following a call for submissions from members of the public carried in local dailies dated **24<sup>th</sup> August, 2023** (*Annex 7*). The Committee received sixteen (16) oral submissions and seventeen (17) written Memoranda from the invited witnesses and members of the public.
92. This Chapter of the Report elaborates both oral and written submissions by the witnesses. The Memoranda submitted to the Committee are also annexed at (*Annex 9*) of Volume II of this Report. The table below highlights the list of witnesses engaged and the dates of attendance.

*Table 1: List of Witnesses and Date of Attendance*

No.	Name of Witnesses	Date of Meeting
1.	National Computer & Cybercrimes Coordination Committee (NC4)	29 <sup>th</sup> August, 2023
2.	Attorney General (AG)	30 <sup>th</sup> August, 2023
3.	Kenyatta International Convention Centre (KICC)	31 <sup>st</sup> August, 2023
4.	Communications Authority of Kenya (CA)	
5.	Ministry of Health (MoH)	
6.	Directorate of Criminal Investigations (DCI)	4 <sup>th</sup> September, 2023
7.	Central Bank of Kenya (CBK)	5 <sup>th</sup> September, 2023
8.	Witnesses who Participated in the World Coin Activities: a) Bruce Bogita b) Miruba Marube c) Benard Ochieng	

No.	Name of Witnesses	Date of Meeting
9.	Tools for Humanity Corp (TFH Corp) Tools for Humanity GmbH, Germany (TFH GmbH)	6 <sup>th</sup> September, 2023
10.	Office of the Data Protection Commissioner (ODPC)	7 <sup>th</sup> September, 2023
11.	Ministry of Information, Communication and the Digital Economy	11 <sup>th</sup> September, 2023
12.	Sense Marketing Limited	12 <sup>th</sup> September, 2023
13.	Capital Markets Authority (CMA)	13 <sup>th</sup> September, 2023
14.	Financial Reporting Centre (FRC)	
15.	Ministry of Interior and National Administration	14 <sup>th</sup> September, 2023
16.	National Intelligence Service (NIS)	18 <sup>th</sup> September, 2023

**Table 2: Written Submissions**

No.	Name of Witnesses	Date Received
1.	ISACA Kenya Chapter	7 <sup>th</sup> September, 2023

### 3.2 SUBMISSIONS BY WITNESSES

93. The *Ad hoc* Committee in its inquiry into the activities and operations of Worldcoin in Kenya sought information from witnesses in line with its mandate in accordance with the Speaker's Communication No. 055 of 2023 dated Tuesday, 15<sup>th</sup> August, 2023 (*Annex 3*) and terms of reference as per the National Assembly's Invitation for Public Participation and Submission of Memoranda dated 24<sup>th</sup> August, 2023 (*Annex 7*). The Committee received oral and written evidence falling across the following emerging thematic areas —

**Table 3: Terms of Reference and Thematic Areas**

<b>No.</b>	<b>Terms of Reference (ToR)</b>	<b>Thematic Areas</b>
<b>ToR 1</b>	To inquire into the operations and ultimate objectives of the activities of <i>Worldcoin</i> in Kenya.	<ul style="list-style-type: none"> <li>a) Worldcoin generally;</li> <li>b) Registration/subscription to Worldcoin platform;</li> <li>c) The Orb apparatus;</li> <li>d) Whether TFH Corp and TFH GmbH operated in Kenya as data controller before registration as such;</li> <li>e) The ultimate aim and objectives of the operations and activities of Worldcoin in Kenya; and</li> <li>f) Whether the registration of Kenyans by Worldcoin is still going on despite the pendency of a court order and other administrative directions halting the same.</li> </ul>
<b>ToR 2</b>	To inquire into the legal and regulatory compliance of operations of <i>Worldcoin</i> , and its agents in Kenya.	<ul style="list-style-type: none"> <li>a) Whether Tools for Humanity Corporation and Tools for Humanity GmbH were Required to Register under Part XXXVII of the Companies Act, 2015 before Carrying on their Activities in Kenya;</li> </ul>

No.	Terms of Reference (ToR)	Thematic Areas
		<ul style="list-style-type: none"> <li>b) Whether TFH Corp and TFH GmbH were duly registered as data controller/processor(s) in Kenya;</li> <li>c) The legality of the relationship between TFH Corp and TFH GmbH with their local partners, agents, consultants and marketers; and</li> <li>d) Whether the orbs were legally imported and used by Worldcoin in Kenya.</li> </ul>
<b>ToR 3</b>	To inquire whether due diligence was undertaken by the relevant government agencies before <i>Worldcoin</i> started its operations in Kenya.	<ul style="list-style-type: none"> <li>a) Whether the ODPC conducted due diligence on Worldcoin or its agents before registration as a data controller; and</li> <li>b) Whether KICC conducted due diligence on the nature of activities to be undertaken by Worldcoin within its premises.</li> </ul>
<b>ToR 4</b>	To inquire into the nature, use and safety of data collected by <i>Worldcoin</i> in Kenya.	<ul style="list-style-type: none"> <li>a) The Nature of Data Collected by Worldcoin and its Agents;</li> <li>b) The storage, use and safety of the data collected by Worldcoin and its agents;</li> <li>c) Whether Worldcoin provided full disclosure and informed disclosure before collecting personal data from Kenyans; and</li> <li>d) Worldcoin, cryptocurrencies</li> </ul>

No.	Terms of Reference (ToR)	Thematic Areas
		and other similar players in Kenya.
<b>ToR 5</b>	To inquire into the organizational structure and the activities of <i>Worldcoin</i> .	<ul style="list-style-type: none"> <li>a) The origin of the Worldcoin project; and</li> <li>b) Other jurisdictions where the Worldcoin project has rolled out its operations.</li> </ul>
<b>ToR 6</b>	To inquire into the source of money or consideration if any paid to the members of the public who presented themselves for registration and the potential beneficiaries.	<ul style="list-style-type: none"> <li>a) The Amount of Money invested by Tools for Humanity Corp and Tools for Humanity GmbH in Kenya;</li> <li>b) The Worldcoin Token (WLD);</li> <li>c) Cashing-out the WLD by Worldcoin subscribers in Kenya;</li> <li>d) Whether the WLD and related considerations were used to induce Kenyans to subscribe to the activities of Worldcoin; and</li> <li>e) Whether the relevant government agencies monitored the financial flow related to the activities of Worldcoin in Kenya.</li> </ul>
<b>ToR 7</b>	To inquire whether Kenyans were exposed to any health hazards as a result of the activities of <i>Worldcoin</i> in the country.	The possible health hazards from an exposure to biometric scan
<b>ToR 8</b>	To inquire into the legal and regulatory gaps that permitted operations of <i>Worldcoin</i> in Kenya.	<p>Legal and regulatory gaps identified by:</p> <ul style="list-style-type: none"> <li>a) Communication Authority of Kenya;</li> </ul>

No.	Terms of Reference (ToR)	Thematic Areas
		<ul style="list-style-type: none"> <li>b) Directorate of Criminal Investigations;</li> <li>c) Ministry of Health;</li> <li>d) Attorney General;</li> <li>e) Data Commissioner;</li> <li>f) Ministry of ICT and Digital Economy;</li> <li>g) Central Bank of Kenya;</li> <li>h) Financial Reporting Centre; and</li> <li>i) TFH Corp and TFH GmbH.</li> </ul>
<b>ToR 9</b>	Other emerging issues from the inquiry	<ul style="list-style-type: none"> <li>a) Overlapping regulatory mandate among various authorities governing the cyber space in Kenya;</li> <li>b) Security concerns on blockchain technology and cryptocurrencies in Kenya;</li> <li>c) Legality of cryptocurrency and blockchain technologies in Kenya;</li> <li>d) Whether cryptocurrencies are potential avenues for money-laundering;</li> <li>e) The role of DCI in detection and monitoring of cybersecurity and cybercrimes in Kenya;</li> <li>f) Capacity of the Kenyan authorities to ensure cybersecurity;</li> </ul>

No.	Terms of Reference (ToR)	Thematic Areas
		g) Whether the ODPC has collaborated with other state agencies to effectively discharge its mandates under the Data Protection Act, 2019; h) Measures to indemnify Kenyans from unlawful use of data by Worldcoin or its agents; i) The potential impact of cryptocurrencies on the banking sector in Kenya, and the possible remedial measures; and j) The capacity of the Central Bank of Kenya to regulate cryptocurrencies and other emerging technologies in the financial sector.
<b>ToR 10</b>	To recommend necessary legislative interventions.	Legislative proposal(s)

### 3.3 SUBMISSIONS AS PER THE TERMS OF REFERENCE

94. This section is a collation of submissions by witnesses on their presentation per each term of reference that they were required to submit on, based on the deduced thematic areas as summarised in *Table 2: Terms of Reference and Thematic Areas*.

#### 3.3.1 Inquire into the Operations and Ultimate Objectives of the Activities of *Worldcoin* in Kenya

95. With respect to its first mandate, to inquire into the operations and ultimate objectives of the activities of *Worldcoin* in Kenya, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) Worldcoin generally;
- b) Registration/subscription to Worldcoin platform;

- c) The Orb apparatus;
- d) Whether TFH Corp and TFH GmbH operated in Kenya as a data controller before registration as such;
- e) The ultimate aim and objectives of the operations and activities of Worldcoin in Kenya; and
- f) Whether the registration of Kenyans by Worldcoin is still going on despite the pendency of a court order and other administrative directions halting the same.

***On Worldcoin generally***

96. In a joint submission, Tools for Humanity Corporation (TFH Corp) and Tools for Humanity GmbH, Germany (TFH GmbH) represented by Mr. Alex Blania, Mr. Thomas Scott and Mr. Sam Sadle (hereafter referred to as “the Worldcoin”) indicated that *Worldcoin* consists of a privacy-preserving digital identity network (World ID) built on proof of personhood and a virtual asset token (WLD). They submitted that World ID and WLD are currently available in the first front-end client compatible with the *Worldcoin* protocol (World App).
97. In their submissions TFH Corp and TFH GmbH explained that *Worldcoin* is an open-source protocol, supported by a global community of developers, individuals, economists and technologists committed to expanding participation in, and access to, the global economy. Their mission is to create a globally-inclusive identity and financial network.
98. The Attorney General (AG) on the other hand submitted that according to the information provided on their website, *Worldcoin* consists of a privacy-preserving digital identity network (World ID) built on proof of personhood and, where laws allow, a digital currency (WLD). AG submitted that according to the information available on the Worldcoin website, the organization through its affiliate developer TFH Corp, has created an identification system where a biometric device known as an Orb is able to scan an individual’s eyeball specifically, the iris, in order to seemingly create a unique identification (World ID) for that individual.
99. The AG submitted that Worldcoin is cofounded by US tech entrepreneur Sam Altman (the CEO of OpenAI the company that created ChatGPT- a form of generative AI that offers automated chat services for customer service related queries on websites), and offers free crypto tokens to people who agree to have their eyeballs scanned.
100. The NIS submitted that Worldcoin is a blend of cryptocurrency, blockchain and personal identification, built on Ethereum Blockchain network.

***On the registration/subscription to Worldcoin platform***

101. The National Computer & Cybercrimes Coordination Committee (NC4) submitted that Worldcoin was registered as a data controller and processor in Kenya by the Office of the



Data Protection Commissioner (ODPC) and was issued with the registration certificate Serial No. 01945 dated 18<sup>th</sup> April 2023 for a period of two years. According to NC4, Worldcoin project deployed its physical imaging devices in over thirty (30) stations across Nairobi, and that the scanning process utilized biometrics and resulted in the creation of a “World ID” – a digital passport that served as proof of a unique identity to prevent multiple fraudulent cryptocurrency claims.

102. NC4 submitted that Worldcoin was advertising in several public malls in Nairobi while videos and photos of Kenyans queuing at Worldcoin outlets have been shared on social media platforms (Facebook, Twitter and Instagram), and that one week after the launch, Worldcoin announced that over 350,000 Kenyans had been onboarded.
103. NC4 further submitted that to register/subscribe to the Worldcoin platform, Tools For Humanity required user to register through the Mobile App downloadable from their website ([www.Worldcoin.org](http://www.Worldcoin.org)) using their smartphones and undergo eye retina/iris scans via biometric devices called “Orb”. Similarly, the AG submitted that the Worldcoin website elucidates that for an individual to obtain WLD, the process begins by registering via a mobile application known as World App for the digital tokens and thereafter proceeding to verify one’s identity by having one’s iris scanned and then later claiming the digital coins.
104. According to Worldcoin, if the user wants to use the World ID to prove their humanity and uniqueness, the person will need to visit an Orb to complete the verification process. Worldcoin submitted that once that is complete, the unverified World ID in their World App becomes an Orb-verified World ID. They further submitted that no fees are charged to anyone seeking to sign up for the Orb-verified World ID.
105. The Committee also heard from three (3) witnesses who testified on how Worldcoin and/or its agents recruited them into their platform. Mr. Bruce Bogita, the first witness, informed the Committee that he met with the Worldcoin staff while exiting Quickmart Supermarket, Kilimani where he had gone to shop. He submitted that the said staff called him aside and informed him that they were conducting an iris scan on behalf of Worldcoin after which he would receive a grant worth USD 70.
106. Mr. Miruba Marube, the second witness, informed the Committee that his first contact with Worldcoin was in 2021 at Kenyatta University, where Worldcoin was operating from. He informed the Committee that an agent of Worldcoin approached him and told him that Worldcoin was a new cryptocurrency that uses iris scanning to distinguish Artificial Intelligence (AI) from human beings since AI had created a big impact in the world. He submitted that the agents told him that Worldcoin were looking into separating AI from human beings through an iris scan to enable them determine the transactions/traffic in the internet and take action accordingly.

107. Mr. Benard Ochieng on the other hand, testified that his first encounter with Worldcoin was in March 2023 while doing recruitment at Technical University of Kenya. Mr. Ochieng submitted that he was asked to register in the Worldcoin App and scan his iris so they could be able to differentiate him from AI and was also promised around USD 70 after the iris scan.
108. On whether registration to the platform was consensual, the Worldcoin submitted that the project complied with the requirements of the Data Protection (General) Regulations, and the Guidance Notes on Consent issued by the ODPC, which require consent to be specific, informed, clear, unequivocal and signified through an affirmative action.
109. The Worldcoin submitted that users were asked to agree to TFH’s User Terms and Conditions and privacy notice before they could access World App. The Worldcoin went on to submit that users were/are not, however, required to agree to the Worldcoin Foundation’s Biometric Data Consent Form or to provide any sensitive personal data in order to access or use World App or to have a World ID that is not Orb-verified – no conditionality applies. The Worldcoin submitted that users had a choice to freely provide consent, thus signifying consent to a valid contract.
110. The Directorate of Criminal Investigations (DCI) on the other hand submitted that upon learning about the activities of Worldcoin at KICC, they dispatched investigators who visited KICC where the activities of Worldcoin involving inter alia, the collection of personal data was ongoing. They found over 2,000 people, mostly youth, queuing to be signed up.
111. The DCI submitted that Worldcoin issued 25 WLD upon signing up and verification to incentivize people to subscribe to their platform. It further submitted that the token was converted to USDT on a cryptocurrency exchange then resold for Kenyan Shillings. NC4 explained that each WLD is worth USD 2.1 or KES 299.
112. The Ministry of ICT and the Digital Economy summarized the activities and operation of Worldcoin and its agents in Kenya as follows:

***Table 4: Summary of Worldcoin Activities in Kenya Presented by the Ministry of Information, communication and the Digital Economy***

	DATE	ACTIVITY
1.	31 <sup>st</sup> May 2021	Worldcoin started collecting data in Kenya according to information obtained from Coulson Harney LLP, also known as Bownmans- Advocates representing Worldcoin in Kenya
2.	April 2022	ODPC was approached by BuzzFeed News, USA enquiring the activities of Worldcoin in Kenya. This was when the Worldcoin

	DATE	ACTIVITY
		became known to ODPC
3.	On 19 <sup>th</sup> April 2022	ODPC began assessment of the activities of <i>Worldcoin</i> , giving them 14 days to provide data and details about their operations
4.	6 <sup>th</sup> May 2022	Worldcoin submitted response explaining activities in Kenya, relating to collection of personal data
5.	9 <sup>th</sup> May 2022	ODPC asks <i>Worldcoin</i> to provide a Data Protection Impact Assessment (DPIA) report.
6.	17 <sup>th</sup> June 2022	<i>Worldcoin</i> submits DPIA and DPIA for TFH USA and TFH Germany
7.	23 <sup>rd</sup> June 2022	ODPC NOT satisfied with the DPIA submitted, directs Worldcoin to STOP COLLECTING SENSITIVE DATA from Kenyans for 60 days until ODPC is satisfied with DPIA and legal Basis.  ODPC asks Worldcoin to demonstrate Compliance
8.	14 <sup>th</sup> July 2022	Data Protection Regulations are enacted and become effective
9.	15 <sup>th</sup> July 2022	In response to ODPC's letter of 23 <sup>rd</sup> June 2022, Worldcoin responds to ODPC, seeking to explain compliance and gaps in the DPIA report submitted.
10.	22 <sup>nd</sup> August 2022	TFH Corp and TFH GmbH submit applications to ODPC for registration as data controllers in Kenya
11.	15 <sup>th</sup> September 2022	Registration Certificate issued to TFH GmbH
12.	17 <sup>th</sup> November 2022	TFH Corp provided data collection schedule
13.	18 <sup>th</sup> April 2023	TFH Corp issued with Certificate of Registration Valid for 24 Months
14.	30 <sup>th</sup> May	After conducting spot checks, ODPC writes to <i>Worldcoin</i> to their

	DATE	ACTIVITY
	2023	dissatisfaction on data processing, legal basis for data collection, legitimate interests, and how Worldcoin was seeking to obtain consent  ODPC directed World coin to cease data collection and processing sensitive personal data, provide proof that Worldcoin was obtaining valid, express, informed and specific consent from Kenyans and provide details of processing contracts with data processors and agents including sample signed contracts. All to be supplied within 14 days
15.	16 <sup>th</sup> June 2023	Worldcoin writes explaining how they are compliant, based on the letter of 30 <sup>th</sup> May 2023
16.	28 <sup>th</sup> July 2023	ODPC issues an advisory to the public advising them to be vigilant as they engage with <i>Worldcoin</i> on compliance with Data Protection Act 2019
17.	2 <sup>nd</sup> August 2023	Join Press Statement ODPC and CA expressing continuing concern with Worldcoin since its launch and operations in Kenya. The statement indicated that various countries such as Germany, France, the UK and India had expressed concern over WC OPERATIONS  ODPC directed Worldcoin to cease the collection of all personal data in Kenya
18.	2 <sup>nd</sup> September 2023	ODPC cancelled the registration of Worldcoin as a data controller
19.	5 <sup>th</sup> September 2023	ODPC wrote to the Ministry submitting an investigation report on <i>Worldcoin</i> activities in Kenya and requesting the Ministry to write to the Head of Public Service requesting assistance in stopping all activities of Worldcoin
20.	8 <sup>th</sup> September 2023	At the request of ODPC, the Ministry forwarded the investigation report and requested the Head of Public Service for the Assistance of his office in stopping all the activities of Worldcoin

### ***On the Orb apparatus***

113. NC4 submitted that the Worldcoin Foundation, registered in Cayman, holds the patents to the Orb technology and all user data and issued all Worldcoin tokens through its subsidiary World Assets Limited, registered in the British Virgin Islands.
114. According to NC4, the Worldcoin used the Orb to scan their subscribers' iris to verify their authenticity as true and unique human beings. The company further stated that the iris image was converted into a digital code (hash value) which was then transmitted to their third-party servers hosted by Amazon Web Services (AWS) in the USA.
115. The DCI on the other hand informed the Committee that on 5<sup>th</sup> August, 2023, their investigators visited the premises of Fogo Generators at KC Aurora Complex along Mombasa Road where they recovered 48 Orb apparatus, assorted Worldcoin merchandise, electronic components and pertinent documents.
116. The DCI further noted that the Orbs and other electronic gadgets recovered in the course of investigations were undergoing forensic analysis that would enable the investigators ascertain the exact number of people in Kenya who were signed up and their sensitive personal data collected. Mr. Amin further noted that they had recorded twenty-seven (27) statements from various witnesses and persons of interest.
117. On the number of Orbs, Worldcoin had in the country, and if they were of the same technical specification, the Worldcoin submitted that they had forty-eight (48) of orb machines in Kenya and of the same technical specifications.

### ***On whether the TFH Corp and TFH GmbH operated in Kenya as a data controller before registration as such***

118. The NC4 submitted that the Worldcoin announced the official launch of its financial and digital identity platform in Kenya on 24<sup>th</sup> July, 2023. On their end, the DCI informed the Committee that their attention was drawn to the activities of Worldcoin in Kenya on 31<sup>st</sup> July, 2023, through DCI's Fichua platform and other social and mainstream media – involving the alleged illegal collection of biometric data, specifically the scanning of irises of members of the public in exchange for KES 7,000 worth of WLD by an entity going by the name “Worldcoin” in various parts of the country.
119. Sense Marketing represented by Mr. Kevin Olende, informed the Committee that at the time they began engagements with Worldcoin in October 2022, they had already been in the market for over a year and a half and were conducting activities in malls and campuses, and because of their public operations and the fact that their company was to be added as one of

the many already existing operators, they did not note or sense any cause for alarm and to the best of their knowledge, Worldcoin was legally conducting operations in the country.

*On the ultimate aim and objectives of the operations and activities of Worldcoin in Kenya*

120. The Committee expressed concern about the real intention of Worldcoin and what they stand to gain by collecting personal data. In response, the Communication Authority of Kenya noted that the intent of Worldcoin was to collect the iris data and create a World ID for the proof of personhood. The Authority explained that the iris is a unique aspect of human being that can be used to distinguish human beings from other artificial beings in the cyberspace.
121. Further, NC4 submitted that Worldcoin intends to use the data to develop a machine learning algorithm that will be able to establish the “Proof of Personhood” protocol. Therefore, TFH (as the developers of the protocol) had to develop an algorithm that could differentiate between real human and fake (i.e., non-human) irises, as well as differentiate one real human’s irises from those of people who have already signed up to the protocol.
122. CA explained that the World ID would be a good platform for creating cryptocurrency that enables everyone to gain income and improve on AI systems as well. Similarly, NC4 submitted that TFH had indicated that they were in the process of creating the world’s largest and most trusted network of cryptocurrency. NC4 also noted that TFH would use the network for promoting the Universal Basic Income (UBI) to support livelihoods of several persons globally.
123. CA further stated that AI relies on the quantity of data gathered for machines, and that the more the data gathered, the better the intelligence gathered for the machines. As such, the Authority submitted that Worldcoin aims to be dominant over the other players in the technological space through the large amount of data collected.
124. Additionally, NC4 noted that in order to make the machine learning algorithm work perfectly and without the risk of discrimination due to an algorithm bias, TFH had concluded that it was necessary to collect and process a diverse and broad amount of sensitive personal data for its training.
125. When asked whether Worldcoin is seeking to decentralize monetary system, Sense Marketing Limited submitted to the Committee that having known the existence of cryptocurrency trade, he understood Worldcoin as one of them joining the market and did not perceive them as trying to decentralize monetary systems.
126. Worldcoin believes that a single, borderless currency can foster economic growth, reduce transaction costs, and promote equality among all participants in the global economy. To

achieve this, Worldcoin has developed a unique protocol that combines a novel World ID system with a Worldcoin token to facilitate secure, transparent, and efficient transactions.

127. When asked about the gain Worldcoin stands to make in collection of personal data, Worldcoin submitted that Worldcoin is not a business entity, and that their main objective is to create a world ID. The Worldcoin went on to state that the World ID would be a good platform for creating cryptocurrency that enables everyone to gain income and improve on AI systems as well. He submitted that the more the data the better the intelligence gathered for the machines. The Worldcoin further submitted that by collecting more data, Worldcoin gains to be dominant over the other players in the technological space.

***On whether the registration of Kenyans by Worldcoin was still going on despite the pendency of a court order and other administrative directions halting the same***

128. The Data Commissioner informed the Committee that the ODPC, pursuant to its powers under section 9(1), 22 and 59 of the Data Protection Act, 2019, as read together with regulation 16 of the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 commenced multiagency investigation to investigate the activities of Worldcoin in Kenya. It is pursuant to the investigations that the ODPC revoked and/or cancelled the registration certificate No. 139-138A-E5D9 and registration certificate No. 325- 9256-645E earlier issued to TFH Corp and TFH GmbH on 5<sup>th</sup> September, 2023.
129. On whether measures taken against the Worldcoin were reactive rather than proactive, particularly in terms of certificate cancellation, the Data Commissioner informed the Committee that on the basis of fair administrative justice, one cannot cancel a certificate without giving the other party a hearing. She submitted that the ODPC notified *Worldcoin* through a letter Ref: ODPC/11/11/8 dated 2<sup>nd</sup> August, 2023 that the office had initiated a formal investigation process in accordance with its powers under Section 9 of the Data Protection Act, 2019.
130. The Data Commissioner submitted that the office initiated investigations after it became clear to the ODPC that *Worldcoin* continued to engage in processing activities involving sensitive personal data in Kenya despite the cessation letter written to them 30<sup>th</sup> May, 2023. The Data Commissioner noted that multi-agency committee reported back to the ODPC on 4<sup>th</sup> September, 2023, hence the certificate cancellation on 5<sup>th</sup> September, 2023 based on the report findings which included failure to seize operations, lack of clarity (inconsistency) of where the data was stored and movement of data to Worldcoin foundation which was not a registered data controller or processor in Kenya.
131. On whether the registration of Kenyans by *Worldcoin* was still going on in the pendency of a court order and other administrative directions halting the same, the Communications Authority of Kenya submitted that no registration was going on in Kenya. In the contrary, the

NIS confirmed to the Committee that online activities were still ongoing on the *Worldcoin* App, noting that it is a worldwide technology that can be operated remotely and will continue.

132. On reasons why the DCI could not stop the ongoing operations at the *Worldcoin* App or the web and whether the physical activities were still ongoing in Kenya, the DCI informed the Committee that they did not have any legal mandate to handle or stop that because individuals themselves were going to those websites and could not police the numerous applications that Kenyans download. They further noted that they were not aware or have information on ongoing registration after stoppage.
133. On whether there were any recommendations made to the CA to bring down the *Worldcoin* App in Kenya, the DCI informed the Committee that the App is held under the Amazon Web Service which is a cloud-based platform and not within Kenyan's jurisdiction and hence has no power to block it.
134. The DCI noted that the Directorate will contact AG and CA to deliberate further on steps that can be taken in order to block *Worldcoin* from operating in Kenya. According to the DCI, the investigations have also established that despite directions from the ODPC vide letter Ref.AI/6217798 dated 30<sup>th</sup> May 2023, served to Ariana Issais of Bowmans Law Firm, acting for and on behalf of Tools for Humanity Corporation, directing for cease of its activities of collecting sensitive personal data, the entity continued with its operations in total disregard to the directives.
135. On the reasons as to why they continued with operations despite the cease order issued by ODPC, Sense Marketing Limited noted that they were not privy to the cease order issued and did not sense any illegality since they had been operating on behalf of *Worldcoin* publicly since October 2022. Sense Marketing admitted of not having a vast knowledge on details of privacy and Data Protection Act 2019.

### **3.3.2 Inquire into the Legal and Regulatory Compliance of Operations of *Worldcoin* and its Agents in Kenya**

136. With respect to its second mandate, to inquire into the legal and regulatory compliance of the operations of *Worldcoin* and its agents in Kenya, submissions received by the Ad Hoc Committee fell within the following thematic areas—
  - a) Whether Tools for Humanity Corporation and Tools for Humanity GmbH were Required to Register under Part XXXVII of the Companies Act, 2015 before Carrying on their Activities in Kenya;
  - b) Whether TFH Corp and TFH GmbH were duly registered as data controller/processor(s) in Kenya;
  - c) The legality of the relationship between TFH Corp and TFH GmbH with their local partners, agents, consultants and marketers; and



- d) Whether the orbs were legally imported and used by Worldcoin in Kenya.

***On whether TFH Corp and TFH GmbH were Required to Register under Part XXXVII of the Companies Act, 2015 before Carrying on their Activities in Kenya***

137. On legal compliance, the AG submitted to the Committee that according to Section 974 of the Companies Act 2015, enjoins foreign companies not to carry on business in Kenya unless they are registered under Part XXXVII of the Companies Act.
138. Further, the AG submitted that for a foreign company to be issued with a compliance certificate, the company must make application in the prescribed form, and provide a certified copy of the certificate of registration from the country of origin, a certified copy of its constitution, a list containing its directors and shareholders and their personal details.
139. The AG concluded that in the absence of a certificate of compliance issued by the Registrar of Companies, a foreign entity cannot validly conduct business in Kenya.
140. The AG submitted that in the case of *Root Capital Incorporated v Tekangu Farmers' Co-operative Society Ltd & Another* [2016] eKLR, the court elucidated the provisions of Part XXXVIII of the Companies Act as follows:

The registration of foreign companies is now captured under Part XXXVII of the Companies Act, 2015; The procedure for registration is prescribed under section 975 (1) of the Act; amongst the documents an applicant for registration must produce is a certified copy of a current certificate of the foreign companies' incorporation or registration in its place of origin, or a document of similar effect. (See section 975. (3)(a). Once the company has been registered the registrar issues to the company with a certificate of compliance (section 975. (4)(b)). Further, under section 975(7), the certificate of compliance is conclusive evidence that the requirements of the Act have been complied with and that the company is duly registered as a foreign company under the Act. It is clear from both the repealed Act and the new Act that for a company to carry out the functions of an incorporated company it must be registered either under the repealed Act or under the new Companies Act, 2015; the need for registration applies to foreign companies as much as it applies to local companies. Irrespective of whether a company was registered under the repealed Act or the Companies Act, 2015 the only conclusive proof that either of the Acts has been complied with and a particular company has been duly registered and thus empowered to perform the functions of a duly registered company is a certificate of registration/compliance.

141. The AG submitted that at the point of registration by the ODPC as a data controller and processor under the Data Protection Act, TFH Corp and TFH GmbH ought to have complied with the laws of Kenya on registration of foreign companies in order to conduct business in

Kenya. The AG submitted that notwithstanding the requirements of Part XXXVIII of the Companies Act, the Business Registration Service (BRS) report indicate that Worldcoin, TFH Corp and TFH GmbH do not appear in the BRS database of registered businesses or companies hence, lack the legal capacity to do business in Kenya.

142. The DCI submitted that investigations have established that TFH Corp is a company registered in the United States with TFH GmbH as its wholly owned subsidiary company registered in Germany both trading as *Worldcoin*. The DCI further submitted that both companies are co-founded by Sam Altman, Chief Executive Officer of Open Artificial Intelligence and Alex Blania.
143. The DCI however, submitted that the two foreign companies are not registered in Kenya as required under the Companies Act, 2015. The DCI further revealed that Tools for Humanity Corporation and Tools for Humanity GmbH have actively facilitated, promoted, marketed and participated in registration and/or sign up of subjects in Kenya and about 34 other countries across the world. The process involves collection of the iris and facial images through scanning using an Orb apparatus.
144. The AG also submitted that TFH Corp and TFH GmbH used personal data to advance commercial interests within the meaning of regulation 14(1) of the Data Protection (General) Regulations 2021. In the circumstances, the AG submitted that the activities of TFH Corp and TFH GmbH were commercial in nature since the cataloguing of iris scans was to further their commercial enterprises and actually induced Kenyans to register on their mobile application World App in exchange for digital tokens for the use of their biometric data.
145. The AG noted TFH Corp and TFH GmbH were required to register and obtain certificate of compliance, prior to their application to the ODPC as data controllers or processors under Part XXXVII of the Companies Act, by the dint of their activities. The AG observed that the Data Protection Act requires an applying company to provide 'establishment documents' which under Kenyan law is a certificate of compliance from the Registrar of Companies.
146. The Cabinet Secretary for ICT and the Digital Economy submitted that the law appeared not to specifically require that foreign applicants must first be registered as a company in Kenya before being registered as a data controller or processor in Kenya. According to the CS, the Data Protection Act is applicable to both locals and non-local persons, as long as they are collecting personal data of persons located in Kenya.
147. The Cabinet Secretary for ICT and the Digital Economy informed the Committee that it is the obligation of a data controller or data processor to fulfil other legal requirements of whatever nature, beyond satisfying the requirements of the Data Protection Act.

148. The Worldcoin submitted that TFH Corp and TFH GmbH did not violate any provisions of the Kenyan data privacy legislation by submitting its application as a foreign entity without local presence in Kenya. They submitted that the registration application portal only requires a foreign company to submit its establishment documents (proof of incorporation) during the application process. The Worldcoin noted that the ODPC thoroughly reviewed and approved both the applications for registration of TFH Corp and TFH GmbH as data controllers in Kenya.
149. The NIS urged the government not to put a lot of bottlenecks for entities trying to put shop in Kenya, and to make sure that Kenya is attractive instead of reacting in a manner that will discourage them from coming. The NIS noted that many of these organizations are looking elsewhere to establish their shops because of the way the world is changing today and the country should look at how to leverage to bring these investors so as to create employment and wealth out of some of these new emerging technologies that are coming up while at the same time safeguard ourselves from any threats that are going to emerge.

***On whether TFH Corp and TFH GmbH were duly registered as data controller/processor(s) in Kenya***

150. CA submitted that the Data Protection Act, 2019 is the framework that governs the processing of personal data and protecting the privacy of individuals in Kenya. The Authority submitted that the Act mandates the Office of the Data Protection Commissioner to licence entities that handle personal data as data processors and data controllers.
151. CA further observed that to ensure the protection of data in the communication sector, section 23(e) of Kenya Information and Communications Act, 1998 (KICA) stipulates that for provision of telecommunication services there is need to ensure that processing of personal data of subscribers is in accordance with the principles set out under the Data Protection Act, 2019.
152. It further submitted that sections 27 (A) and 27 (D) of KICA focus on SIM-card registration where telecommunications operators are required to obtain personal data of their customers prior to provision of services, and to ensure the security and confidentiality of such data.
153. The DCI on the other hand submitted the investigators dispatched from their officer to KICC to inquire into the activities of Worldcoin therein, met the organizers who provided them with a certificate of registration as Data Controller in the name of TFH Corp from the office of the Data Protection Commissioner issued on 18<sup>th</sup> April, 2023 and valid for a period of two years. The DCI submitted that the certificate notwithstanding, the investigators summoned the local organizers who have since recorded their statements in regard to this matter and foreign individuals concerned have also been summoned through INTERPOL.

154. The DCI further noted that their investigations have established that there are data controller certificates issued to two foreign entities namely TFH Corp and TFH GmbH on 15<sup>th</sup> September, 2022 and 18<sup>th</sup> April, 2023 respectively, from the ODPC and the circumstances surrounding the issuance of the certificates by the Data Commissioner to the two entities and whether proper procedures were complied with is a subject of the ongoing investigations.
155. The Worldcoin on the other hand, submitted that on 17 June 2022, TFH submitted its Data Protection Impact Assessment to the ODPC, explicitly referencing provisions of the Data Protection Act. The Worldcoin submitted that the requirement for entities to register with the ODPC was operationalized in July 2022 pursuant to the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, and the registration portal became active in late August 2022.
156. The Worldcoin submitted that TFH Corp and TFH GmbH readily and proactively complied with the registration requirements under the Data Protection Act. The Worldcoin submitted that the application form required TFH to provide descriptions of the personal and sensitive data being processed as well as of the risk and safeguard measures around that processing. The Worldcoin submitted that through the form, each entity also made it very clear that they were not established local entities in Kenya.
157. On the criteria used by the ODPC to register Worldcoin and its agents as data controller in Kenya, the Data Commissioner noted that registration of data controllers and data processors is governed by the Data Protection Act, 2019 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021. The Data Commissioner submitted that pursuant to regulation 5 of the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 Worldcoin submitted to ODPC, the requisite documents for registration as a data controller and were subsequently issued with registration certificates.
158. The registration of TFH Corp and TFH GmbH as data controller was confirmed by AG who submitted that TFH Corp and TFH GmbH presented applications to ODPC for registration as data controllers on 22<sup>nd</sup> August 2022 which were approved and Certificates of registration issued. The Worldcoin on the other hand, submitted that on 22 August, 2022, TFH GmbH submitted its application for registration as a Data Controller to the ODPC. He submitted that TFH Corp followed on 29 August, 2022. The Worldcoin further noted that TFH GmbH was awarded its Certificate of Registration on 15 September, 2022 while TFH Corporation was awarded its Certificate of Registration on 18 April, 2023.
159. Most notably, the Data Commissioner opined that a registration certificate under the Data protection Act, 2019 and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 as a data controller or processor simply signifies that an entity

is known to ODPC and that it processes personal data of persons located in Kenya and does not amount to certification or approval of the processing activities of an entity or serve as an endorsement from the Office of an entity's compliance with other provisions of the Act or any other laws.

160. The AG on the other hand, submitted that for a foreign company to collect and process data in Kenya, the company ought to have furnished its establishment documents to the Data Commissioner. In case at hand, AG submitted that TFH Corp and TFH GmbH were indeed conducting business in Kenya and were required to do so in compliance with the law on registration.
161. The AG submitted that according to information received from the ODPC, two applications for registration as data controllers were made by TFH Corp trading as Worldcoin and TFH GmbH under Section 4 (b) of the Data Protection Act of 2019 as read together with Section 18 and 19 of the same Act which stipulates the requirements for registration as a data controller and/or processor in Kenya.
162. The AG submitted that according to regulation 5(2) (a) of the Data Protection (Registration of Data Controllers and Data Processors) 2021, an application for registration shall be accompanied, inter alia, by a copy of the establishment documents of the entity. Establishment documents under paragraph 2 of the above regulations include—
- a) statute, charter or statutory instrument in which a body is established;
  - b) registration certificate;
  - c) trust deeds in which a trust has been established; and
  - d) other instruments by which a body is established including its governing and administrative structure.
163. The AG went on to submit that the foregoing regulation provides that in order for a foreign company to conduct business in Kenya in effect, collection of biometric data and issuing of digital tokens they need to furnish a copy of the constitutive documents to the Data Commissioner.

***On the legality of the relationship between TFH Corp and TFH GmbH with their local partners, agents, consultants and marketers***

164. On the local representatives, the AG stated that section 979(1) of the Companies Act requires a foreign company to at least have one local representative. On the other hand, section 981 of the Act provides that the local representative shall be held personally liable for any acts of the company in contravention of the Act. However, the AG submitted to the Committee that he was unable to create a nexus between Worldcoin and Sense Marketing as

according to the information availed by the BRS, there are no registration details in relation to Worldcoin.

165. The DCI submitted that their investigators have established that Tools for Humanity Corporation and Tools for Humanity GmbH contracted several individuals and companies to act as Orb operators, agents, consultants and marketers to facilitate and promote *Worldcoin* activities in Kenya. The DCI noted that the TFH's local partners, agents, consultants and marketers include companies and individuals included; Exp Momentum Ltd, Sense Marketing, Bowmans Law firm - Coulson Harney LLP, Fogo Generators, Sava Projects limited, Ariana Issais of Bowmans Law Firm, Rael Mwendu, Wangeci Mwangi and Charles Wanjagi.
166. Mr. Alex Blemia for TFH on the other hand submitted that TFH has formal relationships with Strathmore University, the Blockchain Association of Kenya, American Chamber of Commerce - Kenya, the Africa Blockchain Centre, Safari DAO and others. He went on to submit that TFH also partners with service providers in Kenya for operational, marketing, legal, and other advisory services.
167. The same was confirmed by NC4 that submitted that TFH was allegedly operating in Kenya through its representatives who had been named as Wangeci Mwangi and Rael Mwendu both Kenyan citizens. NC4 further informed the Committee that Platinum De Plus Limited and EXP Kenya, a marketing agency were some of the local firms that have entered into an agreement with TFH through their local representatives for the purposes of coordination of the activities of Worldcoin.
168. Similarly, the documents submitted by TFH Corp and TFH GmbH to the ODPC for registration indicated that the Worldcoin dealt with cooperate partners (Tellem, Bowmans, Station, OBY), Community Partners (Nairobi County, Strathmore University, New Hope Mukuru, Kenya Data Governance and Privacy Society) and Industry partners (Blockchain Association of Kenya, AmCham Kenya, Kenya ICT Action Network).
169. On the responsibility and payment of the Worldcoin representatives, Sense Marketing informed the Committee that they were to help consumers sign up and their payment was on the basis of the total number of people signed up. Sense Marketing submitted that it was in contact with Wangeci Mwangi, who was the Worldcoin representative in Kenya.
170. NC4 submitted that TFH recruited about eleven (11) Orb Operators who were assigned the responsibilities of hiring casual agents who were trained to sensitize potential customers on general cryptocurrency and Worldcoin, and to assist the users to download the World App, then to have their iris image captured through the Orb. Sense Marketing, another local company has been identified as one of the Orb Operators registered by TFH since November 2022.

171. The DCI further submitted that the TFH's local partners, agents, consultants and marketers were reporting to Piotr Piwowarzyk, a Polish national said to be the Africa regional representative for Tools for Humanity. When asked whether he was a subscriber to the Worldcoin ID, Mr. Olende, the MD Sense Marketing Limited informed the Committee that he had been registered in the Worldcoin App as well as gone through an iris scan. He went on to state that one of the requirements of being a Worldcoin agent was to go through the process to understand it.
172. To further probe into the matter, the Committee invited Sense Marketing Limited. In their submission to the Committee, Mr Olende, the Managing Director of Sense Marketing Limited informed the Committee that Sense Marketing Limited is a Kenyan company incorporated under the Companies Act (Cap. 486) (now repealed) with registration number 115791 registered on 6<sup>th</sup> September, 2023 and officially started operation in July 2022. He noted that Sense Marketing is an Experiential marketing agency focusing on below the line marketing, digital marketing, research, creative services, among others.
173. The AG on the other hand, informed the Committee that Sense Marketing is a Private Limited Liability Company incorporated in 2013 under Certificate No. CPR/2013/115791 with 100% of its shareholding registered under one Kevin Odumbe Olende. The AG submitted that the registered office of Sense Marketing Limited is LR. No. 209/37 Lang'ata-Kitengela Road, P.O. Box 15371-00100, Nairobi. Further, the AG submitted that Sense Marketing PLC had a wide object clause which permitted it to transact on a broad range of businesses.
174. The MD informed the Committee that in October 2022, Sense Marketing was made aware of a company called Worldcoin that was operating in the country as a cryptocurrency and was looking for operators to help sign up willing consumers into their platform. He explained to the Committee that he visited few sites where they had operations to see what exactly the company was doing and how they were registering users onto the Worldcoin platform i.e., Lavington mall and Kenyatta university. The MD of Sense Marketing Limited then contacted the Worldcoin representative in the country who was willing to add Sense Marketing Limited as one of their many local operators and was granted a meeting to discuss how the project works and what role they would play. He noted that he was requested to share statutory documents such as company profile, certificate of incorporation and ID copy after which he was sent an Orb Operator Agreement and Due Diligence Questionnaire to sign on 15<sup>th</sup> November, 2022 and received them back on 18<sup>th</sup> November, 2022.
175. The MD submitted that it is through the Agreement that Sense Marketing Limited was contracted as an operator and their task was to recruit a team of agents to be deployed to various malls and events to recruit people onto the Worldcoin platform. He explained that after recruiting the agents, Worldcoin organized and conducted training sessions where they

were taken through the process of registering willing participants and how to operate the Orb. He noted that Worldcoin conducted a series of trainings and sensitizations where they gave strict instructions on how registrations and verifications were to be done, including a caution not to conduct registration and verification of minors.

176. The MD went on to note that once the training was complete, Worldcoin would allocate a venue mainly in malls, where the agents would be stationed. The leases and agreements of the venues were between Worldcoin and the establishments. At each mall/venue, Worldcoin provided a full set up that consisted of a branded display, table with cabinets and the Orbs which were stored in the display cabinets. He also explained that agents were contracted on temporary basis and their payment was commission-based tied to the number of people they signed up on daily basis.
177. The MD submitted that the agents were tasked with speaking to people about Worldcoin and those interested were assisted/requested to download the Worldcoin App from the Apple Store or Google Play Store in order to register for the service after accepting all the terms and conditions. Once downloaded, they were to use the Orb to verify proof of humanity. The MD noted that Worldcoin provided the Orbs and was in control of the program running the Orbs which as per the information provided were to be used to verify a person is a human. They were informed that the orb did not store any data and all scans would be deleted once the verification was done.
178. The DCI on the other hand explained that, as to the scope of engagement between TFH Corp and TFH GmbH and their local partners, agents, consultants and marketers constituted any criminal act, is subject of the ongoing investigations. The DCI further noted that a travel restriction has been placed against all persons involved pending outcome of the investigations.
179. When asked about the specific role of each of the Worldcoin partners, agents, consultants or marketers, and why some suspects who may appear to have flaunted some of the regulations within the law have not been charged, the DCI informed the Committee that Exp Momentum Ltd contract was specifically to identify the venue of operations, Sense Marketing was a liaison contact persons or gave advice when interacting with various entities in terms of their operations, Bowmans Law Firm gave advice on legal matters and was a representative of Tools For Humanity GmbH and Tools For Humanity Corporation, Fogo Generators were contracted through Sava Project Limited in terms of logistics since they had a warehouse along Mombasa Road and therefore provided storage for the equipment and other commodities, Ariana Issais, Rael Mwendu, Wangeci Mwangi and Charles Wanjagi were consultants of individuals marketing the activities of Worldcoin through the two companies within the various recruitment areas and Charles Wanjagi was also an orb operator and was the one handling most transactions.



180. The DCI further noted that all the named persons had been summoned and recorded statement and are still persons of considerations. He stated that investigation process must follow several laws and the investigators must gather information based on facts and not rumors to give a strong backing before determining infringement of any of these laws and charging of individuals.
181. But according to AG, section 979 (1) of the Companies Act requires a foreign company to have at least one local representative. The AG went on to submit that according to section 981 of the Companies Act, a local representative of a registered foreign company is answerable for the doing of all acts, matters or all things that the company is required by or under the Act and is personally liable to a penalty imposed on the company for contravention of, or failure to comply with the provisions of the Act.
182. When asked on how TFH paid its Kenyan partners and orb operators, and whether the partners and orb operators were registered by the Data Commissioner, the Worldcoin submitted that the partners and orb operators were paid in fiat currency or stable coin and not in Worldcoin. The Worldcoin submitted that the Partners were not registered at the Data Protection Commission, as they do not touch personal data but just operate the device collecting the image data with consent of the person which is sent to the Worldcoin servers.

***On whether the orbs were legally imported and used by Worldcoin in Kenya***

183. The Committee sought to know whether the Communications Authority of Kenya was involved in the approval of the equipment used to mine personal data from Kenyans. The Authority observed that they had no records and applications made to bring the said equipment into the country. The Authority submitted that it only learnt about the activities of Worldcoin in Kenya through media.
184. The DCI on the other hand, explained that the Orb as a machine was/is manufactured in Germany and from Germany the company exporting to Kenya was/is Tools for Humanity GmbH. The DCI noted that noted that the clearing agent was called Bridgeways Limited and the goods were transmitted via DHL to Jomo Kenyatta International Airport and declared as biometrics scanners. They were stored at a store along Mombasa Road where the DCI officers picked them. He further noted that they had made inquiries and had engagements still going with KRA to unveil more on them.
185. When asked whether the orb is a telecommunication device, the DCI informed the Committee that the device has a sim card for transmitting information, a hard drive, and a wireless capability thereby confirming that the device is a telecommunication device. CA on the other hand, noted that they had one orb machine in their forensic laboratory brought by DCI officers for further investigation, and that they had no knowledge of the whereabouts of the other orb machines.

186. On the number of Orbs they got as a company and whether they conducted due diligence on the orbs, Sense Marketing submitted that the orbs were allocated according to the number of venues available. Sense Marketing went on to note that they would be allocated at most two orbs at a time per venue/mall. Sense Marketing further noted that they relied on the training conducted that indicated the orbs to be biometric scanners used to verify humanity and would delete the information collected afterwards. Sense Marketing admitted of not knowing whether the orbs were telecommunication devices/captured data and that they did not go through type approval.
187. Further the ODPC submitted that in places where *Worldcoin* sought to sign up users, *Worldcoin* alleged that it partnered with like-minded local entrepreneurs called “Orb Operators.” According to *Worldcoin*, these Orb Operators are independent contractors who would have gone through a written application and interview process, and also have been screened and verified to be in compliance with applicable know-your-customer (KYC) requirements.
188. When asked whether CA should take responsibility for not conducting type approval on the orbs at the port of entry into the country, the DCI noted that they made a request to confirm from CA in regard to what type of approval the Orb was. According to the report from the CA shared with the DCI, the devices were not declared Orbs, but as biometric scanners, and technically, perhaps from a telecommunication point of view, it was not a telecommunication equipment. Nonetheless, CA report had a disclaimer that they perhaps require some more information from the manufacturer. The DCI noted that they had a written report from CA on their findings and would present it to the Committee.
189. Further the *Worldcoin* submitted that in early 2022, TFH reviewed the list of equipment published by the Communications Authority of Kenya (CAK) as examples requiring type approval. The *Worldcoin* went on to submit that given the categories listed thereunder, and the nature and function of the Orb device, it was concluded that the Orb was not likely to fall within the list. The *Worldcoin* further submitted that the Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010 (“Type Approval Regulations”) do not appear to be crafted with the intent that equipment such as the Orb be considered communication or terminal equipment that would require type approval/acceptance.
190. The DCI further informed the Committee that a portioning blame on any government entity or agency will be subject to the outcome of their ongoing investigations. As a recommendation, the DCI submitted that the Communication Authority (CA) should have technical personnel at the entry and exit points in the country to provide technical expertise and ensure that all telecommunication devices that come into the country are declared and meet all the requirements as stipulated in law.

191. Furthermore, under the Guidelines on the Use of Internet of Things (IoT) Devices, where the IoT and Machine to Machine devices require the use of Mobile Station International Subscriber Directory Number (MSISDN), the KICA (Numbering) Regulations would apply to the devices. The Orb devices do not require the use of MSISDN and therefore do not need to be assigned numbering in accordance with the KICA (Numbering) Regulations, 2010. In this regard, the Guidelines would not apply to the Orb devices.

192. In sum, the Worldcoin submitted that the company did not engage in any wrongdoing and that a mutually beneficial settlement or decision can be reached for all stakeholders involved. The Worldcoin submitted that TFH prays that the suspension barring its operations in Kenya, be lifted, with the necessary legal and regulatory oversight.

### **3.3.3 Inquire Whether Due Diligence was Undertaken by the Relevant Government Agencies Before *Worldcoin* Started its Operations in Kenya**

193. With respect to its third mandate, to inquire whether due diligence was undertaken by the relevant government agencies before *Worldcoin* started its operations in Kenya, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) Whether the ODPC conducted due diligence on Worldcoin or its agents before registration as a data controller; and
- b) Whether KICC conducted due diligence on the nature of activities to be undertaken by Worldcoin within its premises.

#### ***On whether the ODPC conducted due diligence on Worldcoin or its agents before registration as a data controller***

194. The Data Commissioner informed the Committee that TFH Corp and TFH GmbH electronically submitted their respective applications for registration as data controllers on 22<sup>nd</sup> August, 2022, upon coming into force of the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

195. She went on to submit that both TFH Corp and TFH GmbH submitted duly filled in Form DPR1 under the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 having the particulars of the data controller, the purpose for which personal data is processed and a description of categories of personal data being collected.

196. The Data Commissioner further submitted that TFH Corp and TFH GmbH submitted establishment documents duly certified/notarized by a lawyer and upon prompting by the reviewer through the online systems, the two organizations were requested to submit proof of their annual turnover.

197. The Data Controller submitted that on 2<sup>nd</sup> September, 2022, Coulson and Harney LLP Advocates (trading as Bowmans) informed the ODPC via email that TFH GmbH, was Venture Capital-backed and was at the pre-revenue stage therefore, no revenue was being generated and consequently a system generated Certificate of Registration Serial No. 00379 dated 15<sup>th</sup> September, 2022 was issued valid for a period of 24 months.
198. The Data Commissioner went on to state that, upon submission of an income statement for the year ended 31<sup>st</sup> December, 2021 for TFH Corp, certified on 7<sup>th</sup> March, 2023 by Thomas Scott, a system generated Certificate of Registration Serial No. 01945 dated 18<sup>th</sup> April, 2023 was issued to TFH Corp - valid for a period of 24 months. The certificate for registration as a data controller were issued after TFH Corp submitted all the statutory requirements for registration under the Data Protection Act and attendant regulations.
199. The Data Commissioner further noted that section 4 of the Data Protection Act, 2019 applies not only to data controllers and data processors established or ordinarily resident in Kenya but also to those not resident in Kenya but processing personal data of data subjects located in Kenya. Therefore, the Act's provisions explicitly state that data controllers and data processors do not have to be resident or established in Kenya for them to make an application for registration under the Act and the Regulations.
200. The Data Commissioner informed the Committee that an application for a certificate of registration as a data controller and/or data processor only signifies that the entity has complied with sections 18 and 19 of the Data Protection Act, 2019 and does not endorse an entity's compliance with the Data Protection Act in its entirety or its subsidiary regulations, nor is it a valid license for an organization to operate in Kenya or authorize the operations of an entity. The Commissioner further submitted that the Certificate simply signifies that an entity is known to the ODPC and that it processes personal data of persons located in Kenya. She further submitted that the Certificate does not amount to certification or approval of the processing activities of an entity or serve as an endorsement compliance with other provisions of the Act or any other laws.
201. The Data Protection Commissioner noted that Section 8(e) of the Data Protection Act mandates ODPC 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 the Act or any other relevant law. She submitted that the ODPC in exercise of this power, conducted a spot check in various malls and at the ID4 Africa Conference held at the College of Insurance in May 2023 and established that the processing activities as relates to; provision of iris and facial data for the performance of a contract, legitimate interest, legal basis and consent did not meet the requirements of the Data Protection Act.

202. The Commissioner submitted that in view of the foregoing, the ODPC on 30<sup>th</sup> May, 2023 issued a cease notice restricting further collection and processing of sensitive personal data by Worldcoin. Further on 2<sup>nd</sup> August, 2023 communication was sent to Worldcoin where the ODPC reaffirmed that the cessation of processing was not lifted and a further directive was made to stop processing of all personal data immediately.
203. On its part, when asked about the due diligence undertaken on the TFH Corp, TFH GmbH or their agents before registration as data controllers or processors, the CS for ICT and Digital Economy submitted that there was no indication that any due diligence was undertaken on Worldcoin or any of its agents prior to the decision to register it as Data Controller in Kenya.

***On whether KICC conducted due diligence on the nature of activities to be undertaken by Worldcoin within its premises***

204. On the activities and operation of Worldcoin at KICC, the Ag. CEO Ms. Patricia Ondeng informed the Committee that on 28<sup>th</sup> July, 2023, the facility received a client named Ms. Evarline Adongo of Exp Momentum, who visited their marketing office and expressed interest in using KICC's grounds for a product activation that was intended to run for four days with effect from 29<sup>th</sup> July, 2023 to 1<sup>st</sup> August, 2023 and that Exp Momentum would utilize their own branded tents while engaging the public.
205. The correspondences submitted to the Committee involved Ms. Adongo of Exp Momentum and KICC Corporation after she visited the Centre and further discussions regarding event details, rates, payment and booking extensions were conducted through email and a physical meeting at the facility.
206. The Ag. CEO informed the Committee that the approval criteria to hold a meeting or gathering at KICC generally involves discussions about event dates, availability of space, rates and payments. She further submitted that the center requires 100% payment from private clients while Government Clients provide LSO/LPOs as a confirmation and that upon receiving payment a client is confirmed.
207. Ms. Patricia further informed the Committee that the client (Exp Momentum) was invoiced KShs. 448,920 (Four hundred and forty-eight thousand nine hundred and twenty Kenya shillings only) for using KICC grounds for the product activation and they made a payment of KShs. 441,180 (Four hundred and forty-one thousand one hundred and eighty Kenya shillings only) which included a 2% withholding tax. She thus submitted that the activities of Worldcoin within its premises were duly approved.
208. When queried on how it took the facility less than 24 hours to approve booking for the Worldcoin while it took the same facility two weeks to approve meeting of the Parliamentary

Co-operative Society (PACOSO), Mr. Geoffrey Thande, Director of Business Development Services at KICC stated that it took less than 24 hours to approve the Worldcoin event because it was an outdoor activity and that KICC grounds were available for use at the time of the request. He further informed the Committee that the approval time for different activities varies depending on the type and complexity of the event

209. Ms. Patricia, the Ag. Director KICC, also informed the Committee that the event was booked to run for four days from 29<sup>th</sup> July, 2023 to 1<sup>st</sup> August, 2023, and that request to prolong the event by an additional thirteen days was declined by the facility due to concerns that arose upon realization that the event had attracted large crowds that led to long queues affecting the flow of traffic along the City Hall Way.
210. On crowd management and emergency service plan on the Worldcoin or any of its agent's activities, the ag. CEO informed the Committee that the center has always put in place crowd management and emergency services for all its big events whereby an outsourced security in addition to their own security personnel and a standby ambulance are availed in addition to having a police station within the facility. She noted that the facility also deploys additional security personnel depending on client's needs.
211. On approval or concurrence sought from any other Government authorities and security agencies regarding the activities of Worldcoin at KICC, the ag. CEO stated that a meeting took place between KICC and the Director of Criminal Investigation (DCI) officers in relations to the booked event by Exp Momentum since it had attracted large crowds at the facility and they gave all the relevant information requested by the DCI team.
212. In conclusion, she noted that Exp Momentum was a valued client at the center with whom they have collaborated with on numerous events bookings in the past like the FIFA World Cup trophy tour on 27<sup>th</sup> May, 2022 and the Qatar winners flag off on 17<sup>th</sup> November, 2022 which earned the facility a revenue of over two million Kenya shillings.

### **3.3.4 Inquire into the Nature, Use and Safety of Data Collected by *Worldcoin* in Kenya**

213. With respect to its fourth mandate, to inquire into the nature, use and safety of data collected by *Worldcoin* in Kenya, submissions received by the *Ad hoc* Committee fell within the following thematic areas—
- a) The nature of data collected by Worldcoin and its agents;
  - b) The storage, use and safety of the data collected by Worldcoin and its agents;
  - c) Whether Worldcoin provided full disclosure and informed disclosure before collecting personal data from Kenyans; and
  - d) Worldcoin, cryptocurrencies and other similar players in Kenya.

### ***On the Nature of Data Collected by Worldcoin and its Agents***

214. According to the CA, Worldcoin is an identification project that uses a combination of Artificial Intelligence (AI), cryptocurrencies and blockchain technologies. According to the Authority, Worldcoin is based on emerging technology whose future bears uncertainty both in terms society and regulation. It reckoned that Worldcoin collects sensitive personal data, whose storage and access remains unclear.

215. The Ministry of Health on the other hand submitted that the Worldcoin collected biometric identifiers, which are unique and measurable characteristics of individuals, which are valuable tools in healthcare for patient identification, access control, and data security. The Ministry categorized biometric identifiers into: -

**a) Physiological Biometrics:**

216. The Ministry defined physiological biometrics as stable physical characteristics of a person, that are not influenced by stress like face or fingerprint, palm, or iris. It noted in general, that the body ages, but the palm vein lines will not change pattern.

217. The Ministry further sub-classified physiological biometrics into morphological biometrics and biological biometrics. It defined morphological biometrics as attributes that relate to a person's physical size and shape and encompass various methods, such as:

- i) fingerprint recognition, widely used for secure access to electronic health records and hospital identification;
- ii) facial recognition, which identifies individuals by analyzing facial features using cameras and software algorithms;
- iii) iris recognition, which utilizes the unique patterns in the iris of the eye for identification, and its known for its high accuracy though costly to implement;
- iv) retinal scans, which scans the distinctive pattern of blood vessels in the retina, and is used in highly secure environments due to its accuracy;
- v) palm vein recognition, which scans the unique vein patterns in the palm of the hand.

**b) Biological Biometrics**

218. The Ministry submitted that the most common example of biological biometrics are the DNA biometrics. It observed that DNA biometrics are the most accurate biometric identifiers but limited by high costs, ethical concerns, and longer processing times.

**c) Behavioral Biometrics**

219. The Ministry noted that behavioural biometrics involve measuring unique identifying and measurable patterns in human activities, including:

- i) voice recognition, which identifies individuals based on the unique characteristics of their speech;
- ii) keystroke dynamics, which is less common in healthcare but useful for secure access control, identifying individuals by their unique typing rhythm;
- iii) signature recognition, although less secure compared to other biometrics, it can be employed for identity verification in digital documents or systems.

**d) Multimodal Biometrics**

220. The Ministry observed that multimodal biometrics involves combining two or more biometric identifiers to enhance security. For instance, healthcare settings may use a combination of fingerprint recognition and facial recognition for more robust access control to sensitive medical records.

221. In addition to physiological, biological, behavioural and multimodal biometrics, the Ministry of Health submitted that there are other advanced biometric identifiers that are being explored, including:

- e) Gait Analysis, which identifies individuals based on their unique walking patterns, although not common, some research is being conducted in this area.
- f) Heartbeat Recognition, which the Ministry defined as unique heartbeat patterns can serve as an identifier, but this technology is still largely experimental.
- g) Odour Recognition, which has the theoretical potential of using the unique body odour for identification.
- h) Ear Shape, which has the potential to use the distinctive features in the shape of the ear for identification.

222. The Ministry of Health went on to warn that each of the foregoing biometric identifiers has its own advantages and disadvantages in terms of accuracy, cost, ease of use, and acceptability. It further noted that healthcare organizations need to carefully consider those factors, along with ethical and privacy concerns, when implementing biometric identification systems to ensure the best fit for their specific needs and priorities.

223. When asked if they have been able to extract data from the confiscated orbs, the DCI informed the Committee that the orbs were submitted for forensic analysis but they were



unable to extract any data from the gadgets since the drive in the orb is encrypted and could not crack the code. The DCI noted that they have written to the investigators to request the manufacturers to give encryption keys to see if they could recover any data from the hard drives.

224. NC4 further submitted that in addition to the scans, Worldcoin also collected other personal data including, emails, phone numbers, national IDs, photographs and videos of individuals.
225. Both the CS for ICT and Digital Economy and the Data Commissioner submitted that from the documents submitted to the ODPC and the investigation report from the multiagency team, Worldcoin stated its intention to collect both physically and in-app the following data from data subjects: irises, facial images, name, email address, phone number, date of birth, country of residence, IP address and device information.

***On the storage, use and safety of the data collected by Worldcoin and its agents***

226. On storage, the Data Commissioner submitted that according to the Data Protection Impact Assessment submitted to the ODPC, Worldcoin stated that all personal data is stored in Amazon Web Services (AWS) cloud services which is a cloud service with server locations in secure regions and dispersed to ensure data resilience, with best-in-class systems in place to protect customers' data.
227. The Data Commissioner submitted that in the documents submitted to ODPC, Worldcoin stated its intention to collect both physically and in-app, the following data from data subjects: irises, facial images, name, email address, phone number, date of birth, country of residence, IP address and device information for the purpose of signing up to the products and services, that is:
- a) The World ID, which is a technology to prove a person is real and unique while protecting privacy. It is a proof of personhood protocol that allows users to prove they are human without revealing their identity World App and World Token.
  - b) Worldcoin token (WLD), which is a utility token distributed globally and freely to people.
  - c) World App, which is a mobile application platform that enables payment, purchases and transfers using world coin, digital assets and traditional currencies and allows access to World ID. Allows individuals to validate their uniqueness as well as offering a self-custodial wallet. It is the avenue to send and receive supported crypto tokens.
228. The Data Commissioner noted that the purpose of the information collected as indicated in registration application form was intended for proving humanness, proving uniqueness, issuing World ID, verifying World ID and user account, distributing grant of pre-claimed

Worldcoin token (WLD), machine learning, know 'your customer, on-boarding users, fraud-detection and carrying out the operations and enabling use of the Application.'

229. On the use of the data collected by Worldcoin, from the Privacy Notice provided by TFH Corp, the Data Commissioner submitted that the data collected was to be used for the purposes of providing services to customers, conducting research to develop and improve product, training the algorithm to better recognize unique users, analyzing use of services to provide better support, using wallet address to send Worldcoin tokens (WLD) or other cryptocurrencies Worldcoin support, complying with applicable laws (such as using your IP address to block individuals whose country does not allow them to access the Services), handling requests, complaints and inquiries, resolving disputes, troubleshooting issues, and enforcing agreements with their customers, including this Privacy Statement and the Worldcoin User Agreement, and contacting you regarding updates to the Services.
230. According to NC4, with the capabilities of cryptocurrency with user verification based on iris, Worldcoin and its proxies may have access to and control of huge sensitive personal data. It noted that the capabilities are being further investigated for possible impacts on the socio-economic status of Kenyans as well as the national security.
231. NC4 further submitted that one of the key features of Worldcoin's entry into Kenya is the launch of a peer-to-peer (P2P) exchange that allows individuals to quickly and easily access digital currencies and US dollars directly with one another, without the need for a centralized third party to facilitate the transactions. That it was estimated that 4 million Kenyans were active crypto currency users in the country.
232. On the use and safety of the data collected from Kenyans, Sense Marketing Ltd informed the Committee that the company was not collecting any personal data or information from Kenyans and to the best of their knowledge, the orb was a device used to verify proof of humanity.
233. On the safety of the data collected by Worldcoin in Kenya, the Ministry of Health submitted that data breaches involving biometric data can lead to severe implications like identity theft, causing stress and other mental health issues.
234. Further, the Data Commissioner submitted to the Committee that the Data Protection Impact Assessment provided by Worldcoin enumerated following possible risks: unauthorized access to sensitive biometric data and potential misuse of data by third-party consultants. The Data Commissioner submitted that Worldcoin indicated that they had implemented the following safeguards to counter the risks:
- a) utilization of AWS cloud services with robust technical and organizational measures;
  - b) encryption and partitioning of data both in transit and at rest;

- c) strict access controls that limit data access to essential personnel;
- d) employing data minimization and anonymization techniques;
- e) logical Access control; traceability (logging);
- f) archiving and minimizing the amount of data;
- g) operating security and protection of servers;
- h) cybersecurity and cloud services; managing hardware,
- i) backups and maintenance;
- j) network security as technical and organizational measures to mitigate risks and ensure compliance with data protection principles; and
- k) implementation of internal security measures including a written Internal Information Security Policy, Incident Response Plan Code of Conduct, Internal Biometric Data Processing Policy, Internal Information Security Policy, Business Continuity Plan, Operator Code of Conduct, Incident Response Plan, and Business Continuity Plan;

235. On the use of the data collected by TFH Corp and TFH GmbH in Kenya, the CS for ICT and Digital Economy noted that the data collected by Worldcoin was used for; provision of services to the Worldcoin customers; conducting research to develop and improve Worldcoin products; training Worldcoin algorithm to better recognize unique users; analyzing customer wallet address to send then WLD tokens and other cryptocurrencies that the Worldcoin supports; complying with applicable laws; handling requests, complaints and inquiries; and resolving disputes, troubleshooting issues and enforcing agreements.

236. On the storage of data collected from Kenyans, the Cabinet Secretary for Information, Communication and the Digital Economy submitted that according to the information provided by Worldcoin in its Data Protection Impact Assessment (DPIA) with the exception of data stored locally on the Orb itself, all data was stored using Amazon Web Services (AWS) cloud services. The Cabinet Secretary noted that in the DPIA, Worldcoin indicated that iris and facial images as well as inferred data are processed until the machine learning-training of algorithms is completed. The Cabinet Secretary submitted that Worldcoin estimated that the machine-learning training of algorithms should have been accomplished by the end of 2022. The Cabinet Secretary submitted that immediately afterwards, all biometric data would be erased. Accordingly, once Worldcoin progresses to Phase 2, the intention was that all data would have been deleted unless the user had consented to this data being retained for Orb improvement purposes.

237. Moreover, in the assessment of the Cabinet Secretary, the connection between cryptocurrency and biometrics, including iris scan and facial recognition is the need for identification and authentication of actors in cryptocurrency trading platforms for digital transactions, the same way banks have to authenticate whoever presents themselves for a transaction before the transaction can take place.

238. On the safety measures, the Cabinet Secretary submitted that section 31 (1) of the Data Protection Act, 2019 stipulates that where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes, a data controller or a data processor shall, prior to the processing, carry out a Data Protection Impact Assessment (DPIA).
239. The Cabinet Secretary submitted that the DPIA outlines all security related risks and the corresponding mitigation measures. Ordinarily when dealing with sensitive personal data, unauthorized access to the data, misuse of the data, identity theft and impersonation and fraud are some of the risk factors anticipated.
240. The Cabinet Secretary gave a chronology of events as follows.

***Table 5: Chronology of Communication between ODPC and Worldcoin representatives Coulson and Harney LLP (Bowmans) as presented by the Ministry of Information, Communication and the Digital Economy***

1.	On 23 <sup>rd</sup> June 2022	The ODPC directed <i>Worldcoin</i> to stop processing sensitive personal data of Kenyans
2.	On 30 <sup>th</sup> May 2023	The ODPC directed <i>Worldcoin</i> to cease processing personal data until it demonstrates compliance with Data Protection Act 2019
3.	On 28 <sup>th</sup> July 2023	ODPC issued an advisory to the Public asking Kenyans to exercise caution in providing personal data to <i>Worldcoin</i>
4.	2 <sup>nd</sup> August 2023	ODPC and the Communications Authority issued a joint press statement advising Kenyans to be cautious while dealing with <i>Worldcoin</i> and further directing <i>Worldcoin</i> to cease collecting data
5.	10 <sup>th</sup> August 2023	ODPC obtained conservatory orders from the High Court of Kenya directing <i>Worldcoin</i> , its employees and agents to stop collecting data
6.	2 <sup>nd</sup> August 2023	The ODPC cancelled the Registration Certificates of <i>Worldcoin</i> , bringing to an end all its operations in Kenya, the Ministry wrote to the Head of Service seeking assistance of his office in enforcement

**Table 6: Chronology of Communication between ODPC and Worldcoin representatives Coulson and Harney LLP (Bowmans) as presented by the Office of the Data Protection Commissioner (ODPC)**

NO.	DATE	ACTIVITY
1.	April 2022	Attention of ODPC was drawn that Worldcoin has been collecting sensitive personal data from persons resident in Kenya and transferring the same out of Kenya.
2.	19 <sup>th</sup> April 2022	ODPC wrote to the Chief Executive Officer of WorldCoin requesting for information into the collection of sensitive personal data, particularly the legal basis for collection, transfer of the personal data, proof of consent for the transfer amongst other information. The entity was to provide the information within 14 days.
3.	21 <sup>st</sup> April 2022	ODPC received a response from the firm of Coulson Harney LLP (Bowmans) Indicating that they represented Tools For Humanity-Corporation trading as Worldcoin, requesting for the extension of the 14 days period referred to above.
4.	25 <sup>th</sup> April, 2022	The ODPC granted the request for extension of the 14-day period and indicated the date of submission as 6th May, 2022.
5.	6 <sup>th</sup> May 2022	Worldcoin provided a response to the ODPC request for information giving a background of their operations, Technical Approach, Operational Approach, Project Status and Plan amongst other information.
6.	25 <sup>th</sup> May 2022	Global representatives of Worldcoin accompanied by their legal representatives attended a meeting at the ODPC wherein they were requested to submit a Data Protection Impact Assessment (DPIA).
7.	17 <sup>th</sup> June 2022	Coulson Harney LLP submitted a DPIA for both Tools for For Humanity Corporation-USA and Tools for Humanity GmbH Germany.
8.	23 <sup>rd</sup> June 2022	ODPC communicated to Couslon Harney LLP (Bowmans) seeking preliminary clarification on the DPIA's submitted specifically on the lawful basis for processing personal data, and

NO.	DATE	ACTIVITY
		instructed that the processing of personal data of persons located in Kenya be restricted for a period of 60 days or until the Office was satisfied with its DP1A and a clarification on the legal basis was provided.
9.	15 <sup>th</sup> July 2022	ODPC received a letter from Coulson Harney LLP (Bowmans) noting Tools For Humanity Corporation USA indicated that it wholly owns Tools for Humanity GmbH Germany as its subsidiary and responded to the issues raised in ODPC Correspondence.
10.	22 <sup>nd</sup> August 2022	ODPC received through its online system an application from TFH GmbH Germany and TFH-USA to be registered as Data Controllers pursuant to Sections 18 and 19 of the Act and the Regulations.
11.	24 <sup>th</sup> August 2022	DCPC generated invoice to Tools For Humanity GmbH - Germany and Tools For Humanity-USA.
12.	2 <sup>nd</sup> September, 2022	ODPC received an email from Coulson and Harney LLP communicating that Tools for Humanity GmbH, was a venture capital-backed and was at the pre-revenue stage therefore no revenue was being generated.
13.	5 <sup>th</sup> September, 2022	<p>ODPC wrote to Couslon Harney LLP advising Worldcoin to;</p> <ul style="list-style-type: none"> <li>a) Prepare and maintain a clear data processing schedule and record of processing activities that details and provides a clear trail of the lawful purposes relied upon for each processing activity during the lifecycle of the personal data; and</li> <li>b) Provide details on how it intends to comply with the provisions of the Act and address the maters raised in the letter, which primarily centered on the proper identification of the lawful bases relied upon.</li> </ul>
14.	15 <sup>th</sup> September 2022	A system generated Certificate of Registration Serial was issued to Tools For Humanity GmbH-Germany valid for a period of 24

NO.	DATE	ACTIVITY
		months.
15.	10 <sup>th</sup> November 2022	Worldcoin responded and attached data processing schedule for Kenya and reattached the DPLA.
16.	18 <sup>th</sup> April 2023	TFH Corp issued with Certificate of Registration Valid for 24 Months.
17.	30 <sup>th</sup> May, 2023	ODPC noted that the processing undertaken by Worldcoin requiring the provision of iris data and facial data did not meet the requirements of the Act and issued a directive to Worldcoin to cease the processing of sensitive personal data and safeguard the data that had already been processed.
18.	13 <sup>th</sup> June, 2023	ODPC held a virtual meeting with Worldcoin representatives, where ODPC enumerated its concerns on the lawful basis of collecting the sensitive personal data.
19.	16 <sup>th</sup> June, 2023	Worldcoin responded to the ODPC letter of 30 <sup>th</sup> May, 2023 providing clarity on the issues raised.
20.	28 <sup>th</sup> July, 2023	ODPC issued a cautionary statement to the public.
21.	1 <sup>st</sup> August, 2023	Worldcoin reported that their agents had been arrested for offences under the Act and the Computer Misuse and Cybercrimes Act.
22.	10 <sup>th</sup> August, 2023	ODPC obtained Conservatory Orders in Nairobi Office of the Data Protection Commissioner vs. Tools For Humanity Corporation (WORLD COIN) and Tools For Humanity GMBH (WORLD COIN) AND 1 OTHER for all personal data including sensitive personal data collected from Kenyans and Kenyan residents.

241. The Worldcoin on the other hand submitted that neither TFH nor the Worldcoin Foundation has ever sold users' personal or biometric data. He noted that all the personal and biometric data collected in Kenya is securely stored on servers either in the United States, the European Union (Italy, Germany, or Poland), or South Africa. He went on to note that

person's free and informed consent is always secured before the processing of their personal data.

***On whether Worldcoin provided full disclosure and informed disclosure before collecting personal data from Kenyans***

242. The Communications Authority of Kenya submitted that the Kenya Information and Communications (Consumer Protection) Regulations, 2010 obligate any service provider of such technology, as the *Worldcoin*, to provide full disclosure to consumers on any such services being offered. In line with the Regulations, the Authority noted that *Worldcoin* did provide full disclosure to those who showed up to register.
243. On the nature of data collected from the members of the public, Sense Marketing Ltd alluded to the Committee that the agents under the company were not collecting or recording any data from the participant. Sense Marketing submitted that the mandate of the agents was limited to talking to people about *Worldcoin* and the cryptocurrency. Sense Marketing noted that they only took willing participants through the process of downloading the App, accepting terms and conditions and latter conduct an iris scan to prove humanity. There was no additional information required to distinguish the irises. Sense Marketing Ltd went on to submit that it did not consider themselves as Data Controller or processor but as orb operators.
244. On whether it was also collecting data from minors, Sense Marketing submitted that the training they undertook was specific that no minors were to be registered but admitted that there could be possibilities that minors were registered since they did not have a proper mechanism of identifying one. Sense Marketing submitted that it relied on judgment through appearance.
245. On the masses witnessed at KICC, Sense Marketing Ltd submitted that all the Orb operators were required to be at the venue during the KICC product activation. He informed the Committee that the Orb operators were eleven (11) in total but did not know any information about them or the number of Orbs each had. As Sense Marketing, they operated two orbs. Sense Marketing noted that in his view, the mass of people experienced at KICC would have been as a result of the inducement in terms of tokens and would not have been the same if there were no tokens being offered.
246. The Worldcoin on the other hand submitted that throughout our Orb-verification operations in Kenya, TFH has made privacy policy available both on the World App and on the Worldcoin website. The Worldcoin further submitted that TFH had complied with the obligation to register with the ODPC as applicable and has a data protection officer in place currently.



247. In similar regard, Sense Marketing Ltd submitted that during the engagement with participants in the various venues, the participants were informed of what *Worldcoin* was about and willing participants were directed on how they could download the Worldcoin App and register for the service after accepting the terms and conditions then proceed for iris scan to verify proof of humanity.

On consent, ISACA Kenya Chapter noted concerns regarding the WLD token issued by the Worldcoin. ISACA noted that the issuance of WLD token was an indication of lack of freely given and informed consent. ISACA went on to submit that the Data Protection Act, 2019 requires data controllers and data processors to obtain clear and informed consent from individuals before collecting and processing their personal data.

***On Worldcoin, cryptocurrencies and other similar players in Kenya***

248. The Communications Authority of Kenya submitted that cryptocurrencies are digital currencies that have an ascribed value that may fluctuate depending on the supply and demand. Cryptocurrency being a new and emerging technology, majority of consumers have no sufficient knowledge on its use.

249. The Committee further sought to know whether there are other players such as *Worldcoin* that were operating in Kenya. In response, Communications Authority of Kenya stated that there were other players in data mining such as Google, Meta and Twitter but were not as advanced as Worldcoin. It also submitted that in cryptocurrency, Bitcoin is an active player as well in cryptocurrency space that is owned by no individual.

**3.3.5 Inquire into the Organizational Structure and the Activities of *Worldcoin***

250. With respect to its fifth mandate, to inquire into the organizational structure and the activities of *Worldcoin* in Kenya, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) The origin of the Worldcoin project; and
- b) Other jurisdictions where the Worldcoin project has rolled out its operations.

***On the origin of the Worldcoin project***

251. TFH Corp and TFH GmbH submitted in their joint submission that Tools for Humanity (TFH), the original contributing team for the Worldcoin project headquartered in San Francisco, was founded in 2019 by Alex Blania, Sam Altman, and Max Novendstern with the mission of creating a global identity and financial network owned by everyone.

252. NC4 submitted that the *Worldcoin* project was initiated by Tools for Humanity GmbH a global software and hardware development company based in Berlin, Germany and Tools for Humanity Inc. based in the USA.

253. According to the Worldcoin, TFH Corp conducted the initial research, technical development of hardware and software, and field testing of the Worldcoin protocol. In addition to having developed and helped launch the project, TFH continues to provide its client of the Worldcoin protocol, World App. It has, since July 2023, also been contracted by the Worldcoin Foundation to support Orb-verification efforts globally.
254. Further, the Worldcoin submitted that the Worldcoin Foundation is the sole member and sole director of World Assets Limited, a business company incorporated in the British Virgin Islands. He submitted that World Assets Limited is the entity responsible for issuing the 75% of all the WLDs that have been allocated to the Worldcoin community.
255. The Worldcoin submitted that in each country they operate they partner with independent local third parties, called Operator Partners. Operator Partner relationships can take different forms, such as temporary event staffing, fixed locations at existing storefronts, or “Orb Operators” whose teams go out into their community—typically near high-traffic areas like shopping centres and university campuses—to help people securely sign up for World ID.
256. The Worldcoin went on to submit that all the Operator Partners underwent extensive training, including Data Compliance training. He observed that the training is designed to be easily understood by everyone. The Worldcoin went on to note that in addition to initial training, there is training to ensure that Orb Operators are utilizing the most up-to-date information in the field.

*On other jurisdictions where the Worldcoin project has rolled out its operations*

257. NC4 submitted that the project operated in (34) other countries including Uganda, Sudan, Germany, Argentina, Brazil, Chile, France, Hong Kong, India, Japan, Korea, Mexico, Portugal, Singapore, Spain and United Kingdom. It was however, noted that Worldcoin did not operate in the US and China due to the strict regulatory environment.
258. The Worldcoin submitted that Worldcoin seeks to create a global community of users, operators and developers and has invested in similar types of engagement and partnerships in other countries, including Germany, Portugal, Spain, Chile, and Argentina.
259. The Worldcoin further submitted that the World App and the associated self-custodial wallets are currently available in 168 countries around the world. World ID verifications are currently routinely available in 17 countries across five continents, including: Africa (Kenya - suspended; Uganda), Asia (Hong Kong; India; Japan; Singapore; South Korea), Europe (France, Germany, Portugal, Spain, and the United Kingdom), North America (Mexico; United States), and South America (Argentina; Brazil; Chile).

260. They further submitted that verifications may also be available, from time to time, in other countries at events like conferences. In that regard, the Worldcoin submitted that WLD is available on many virtual asset exchanges around the world, with the notable exception of the United States. He noted that WLD is not intended to be available in the United States due to the lack of clarity in that country's definition and treatment of digital asset tokens.

### **3.3.6 Inquire into the Source of Money or Consideration if any Paid to the Members of the Public Who Presented Themselves for Registration and the Potential Beneficiaries**

261. With respect to its sixth mandate, to inquire into the source of money or consideration if any, paid to the members of the public who presented themselves for registration and the potential beneficiaries, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) The Amount of Money invested by Tools for Humanity Corp and Tools for Humanity GmbH in Kenya;
- b) The Worldcoin Token (WLD);
- c) Cashing-out the WLD by Worldcoin subscribers in Kenya;
- d) Whether the WLD and related considerations were used to induce Kenyans to subscribe to the activities of Worldcoin; and
- e) Whether the relevant government agencies monitored the financial flow related to the activities of Worldcoin in Kenya.

#### ***On the Amount of Money invested by Tools for Humanity Corp and Tools for Humanity GmbH in Kenya***

262. According to TFH Corp and TFH GmbH in their joint submission, the two companies have invested over KES 700 million in Kenya with budget plans projected to increase.

263. The Committee inquired about the source of money paid to Kenyans, if Worldcoin was registered as a bank and whether money laundering laws were adhered to as well as who bears the liability in case of any complaints as the company is not registered locally. In response, the Worldcoin stated that TFH had raised over USD 200 million worldwide for the purpose of building orbs and developing blockchain technology. Worldcoin submitted that the Money is also used to develop intellectual property as the company is also valued at the tune of about USD 2.4 billion.

264. The Worldcoin submitted that there is no direct source of revenue and that TFH Corp is fully funded by venture capital to develop technology and there were no money laundering activities that are conducted by Worldcoin. The Worldcoin went on to state that liability is dependent on the specific allegation against, citing Meta and Uber that are active in Kenya without any local representative. It would depend on the allegations against them to determine liability.

### ***On the Worldcoin Token (WLD)***

265. The Worldcoin submitted that on 24 July 2023, WLD moved from “beta” to “live,” meaning the digital asset became liquid, available on exchanges, and transactable on the blockchain. The Worldcoin submitted that a full educational whitepaper with WLD tokenomics issued and published on the Worldcoin website at [whitepaper.worldcoin.org](http://whitepaper.worldcoin.org).
266. The Worldcoin submitted that for subscribers to receive an Orb-verified World ID and claim their share of WLD, consumers must download the World App, a freely downloadable application available in the Apple and Android app stores. He went on to submit that the World App provides a consumer with two self-custodial digital wallets, one to hold various virtual assets, and another containing an unverified World ID.
267. The Worldcoin further submitted that upon token launch, 10 billion WLD tokens were “minted” (launched on the blockchain). The Worldcoin went on to submit that currently, roughly 1.28% percent of the tokens are in circulation. Additional tokens are added to the circulating supply over time, primarily as Orb-verified individuals claim their free WLD token grants. The Worldcoin sent on to submit that in addition to claiming WLD grants offered to Orb-verified World ID holders, anyone can purchase WLD on several online exchanges.
268. The Worldcoin went on to submit that currently, all holders of Orb-verified World IDs can claim three (3) WLD tokens every two weeks for free. (In late July 2023, people were able to claim 25 WLD tokens in a “Genesis grant” celebrating Worldcoin’s launch.) He submitted that the WLDs are issued by World Assets Limited. They went on to note that the free WLDs appear in the World App, and that the recipient of the free WLD may then, through third-party exchanges, opt to exchange the WLD for any other virtual or fiat asset at their discretion.
269. On the process of converting the WLD into currency, Sense Marketing Limited submitted that the tokens would be put in a crypto wallet then one would go to the blockchain market to look for willing buyers who would purchase the tokens according to the agreed exchange rate and the seller would receive the money through Mpesa. He noted that the tokens would vary between 1 to 25 WLD weekly.

### ***On cashing-out the WLD by Worldcoin subscribers in Kenya***

270. The Worldcoin submitted that there was no direct monetary compensation or consideration paid to Kenyans in exchange for completing the Orb verification process. The Worldcoin submitted that the World Assets Limited was not giving people approximately KES 7,000 when they signed up, as reported in some media, rather, it was giving them an amount of WLD tokens.

271. On how and whether KES 7,000 promised to Kenyans was paid, the DCI informed the Committee that after learning about the alleged illegal collection of biometric data specifically the scanning of irises and that people were just queuing and getting money just for the photos to be taken, they came in as DCI and mopped up the organizers. The DCI noted that in their effort to get in touch with the people who received the money was not easy since the participants were not willing to give information but they managed to get three who informed them that they were being asked to download the *Worldcoin* App, and that in the App there was a platform similar to PayPal called "*Wise*" which is capable of converting USD and GBP into KES. The WLD were being converted to USD and then to KES on the platform then sent to individuals on Mpesa at a peer-to-peer level of engagement.
272. The Worldcoin on the other hand, submitted that in Kenya, in response to local demand, a software function in the World App that offers independent Operator Partners the ability to exchange Kenyan Shillings for USDC (a digital "stablecoin" whose value is pegged to the U.S. dollar, offered by the company Circle) in a so-called "peer-to-peer" (P2P) marketplace was created.
273. According to the Worldcoin, the P2P platform provides an easy way for Kenyans to find independent agents who can swap virtual assets for fiat currency by matching agents with their clients (similar to what mobile money agents do, but entirely digitally). The Worldcoin went on to note that the P2P platform is fully available to verified users and in a limited form to non-verified users. The Worldcoin submitted that the P2P transactions are independently undertaken by users and are not controlled or directed by TFH or the Worldcoin Foundation.

***On whether the WLD and related considerations were used to induce Kenyans to subscribe to the activities of Worldcoin***

274. On whether the members of the public were unduly influenced to subscribe to the *Worldcoin* platform, the Worldcoin submitted that there was no undue inducement or any other form of constraint or coercion to participate in *Worldcoin*. The Worldcoin submitted that the people in Kenya and around the world freely chose to participate in the *Worldcoin* activities, and did so in large numbers.

***On whether the relevant government agencies monitored the financial flow related to the activities of Worldcoin in Kenya***

275. When asked whether the CBK can trace and track the financial flow related to the activities of Worldcoin in Kenya, CBK submitted that it could not monitor specific transactions, especially within mobile payment platforms like M-Pesa, given the large volume of transactions involved. CBK went on to emphasize that the fast-evolving nature of cryptocurrencies is being addressed by a task force, which aims to provide more information

on virtual assets and service providers by the end of the month, potentially leading to policy and regulatory frameworks.

276. Further, when asked if it could trace the conversion of WLD into KES via M-Pesa, CBK indicated the challenges of monitoring such transactions due to the massive volume of transactions in M-Pesa and suggested that it may not be possible to detect smaller amounts like the reported KES 2.5 billion. CBK emphasized the complexities of monitoring cryptocurrency-related transactions, particularly within the context of a mobile payment platform like M-Pesa, and emphasized the ongoing efforts to address regulatory and policy concerns related to cryptocurrencies in Kenya.

### **3.3.7 Inquire Whether Kenyans Were Exposed to any Health Hazards as a Results of the Activities of *Worldcoin* in the Country**

277. With respect to its seventh mandate, to inquire whether Kenyans were exposed to any health hazards as a result of the activities of *Worldcoin* in the country, submissions received by the Ad Hoc Committee fell within the following one thematic area—

a) The possible health hazards from an exposure to biometric scan.

#### ***On the possible health hazards from an exposure to biometric scan***

278. The Ministry of Health submitted that whereas biometric identifiers offer various benefits, including increased security and ease of access, exposure to biometric scans generally carries low health risks, but there are some important considerations:

#### **a) Physiological Biometrics:**

279. For fingerprint recognition, the Ministry submitted that there is risk of cross-contamination from shared scanners, potentially spreading germs including bacteria and viruses, hence increasing the risk of infection.

280. The Ministry further submitted that the use of infrared light may cause eye irritation with prolonged exposure in facial recognition. Similar to facial recognition, the Ministry submitted that the infrared light used in palm vein recognition could lead to skin irritation with excessive exposure. Relatedly, the Ministry submitted that while iris and retinal scans are generally safe, prolonged or repeated exposure to the light sources used may cause discomfort or harm.

281. Additionally, the Ministry submitted that DNA biometrics, involves chemical exposure during DNA extraction and analysis, which can be harmful if mishandled, though patients are typically not directly exposed.

#### **b) Behavioral Biometrics:**

282. In this category, the Ministry submitted generally that voice recognition is of low-risk, but noise emitted during verification could lead to auditory strain or discomfort. It also noted that keystroke dynamics and signature recognition are of little to no direct health risk, but improper use of keyboard or writing tool may contribute to musculoskeletal issues over time.

**c) Multimodal and Advanced Methods:**

283. The Ministry submitted that gait analysis, heartbeat recognition, odour recognition, and ear shape are typically non-intrusive with little to no direct health risks to individuals.

284. In general, the Ministry submitted that concerns over data privacy, accessibility and misuse may cause psychological stress or anxiety. It also noted that individuals may experience discomfort or minor injuries during biometric data capture, particularly with modalities using infrared rays (e.g., eye strain during an iris scan). The Ministry also noted that some devices may use materials that can trigger allergic reactions in sensitive individuals (e.g., latex in fingerprinting devices).

285. Worldcoin on the other hand, submitted that the Orb device was certified to be compliant with Kenyan requirements under the Pre-Export Verification of Conformity Standard (PVOC) from the Kenyan Bureau of Standards. The Worldcoin further submitted that he Orb had been certified by TÜV Rhineland (Germany's most reputable certification service provider) as compliant with IEC 62471 "Photobiological Safety of Lamps and Lamp Systems", the globally accepted standard for lamps, lamp systems, and other non-lamp sources of optical radiation that emit light in the spectral region of 200 to 3000 nm. Worldcoin thus concluded that here are no health or safety hazards associated with scanning one's iris at an Orb device.

286. When the Committee inquired on the health effects of scanning the iris on the orb machine, Worldcoin stated that there was no complaint that was reported to them concerning the health effects by the people scanned by the orb. Worldcoin further intimated to the Committee that he had equally had his iris scanned severally during the development of the orb and had not felt any health complications.

**3.3.8 Inquire into the Legal and Regulatory Gaps that Permitted Operations of *Worldcoin* in Kenya**

287. With respect to its eighth mandate, to inquire into the legal and regulatory gaps that permitted the operation of *Worldcoin* in Kenya, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) Communication Authority of Kenya;
- b) Directorate of Criminal Investigations;
- c) Ministry of Health;

- d) Attorney General;
- e) Data Commissioner;
- f) Ministry of ICT and Digital Economy;
- g) Central Bank of Kenya;
- h) Financial Reporting Centre; and
- i) TFH Corp and TFH GmbH.

### ***Communication Authority of Kenya***

288. The Communications Authority of Kenya submitted that the scope of the current laws regarding ICT consumer protection does not adequately cover issues regarding digital currencies and assets. It opined that there is need to develop an appropriate overarching legal framework for the regulation of new and emerging technologies, including digital platform services, social media services and over-the-top services.
289. The Communications Authority of Kenya noted that as the government pursues 100% digitalization of its public services, there is a heightened risk of being a target of the ever-evolving cyber threats.
290. The Authority of Kenya submitted that there is a constraint when it comes to balancing strict regulation, facilitation of innovation and creation of an enabling environment that will contribute to the envisaged digital economy. The Authority noted the global challenge of managing the rapidly evolving new and emerging technologies, such as Artificial Intelligence (AI), Blockchain, Virtual, Augmented and Extended realities, means that there is need for a more progressive and responsive regulatory framework.
291. CA further noted that there is no framework to regulate Digital Service platforms especially Over-the Top Services (OTTs). However, the Authority noted that it is developing a Regulatory Sandbox to nurture innovation as well as inform regulatory decisions and facilitate socioeconomic development. It further submitted that the Authority in consultation with the Ministry of Information, Communications and the Digital Economy is undertaking regulatory reforms with a view to expand the scope of regulatory mandate to address the emerging identified challenges. The Authority further noted that it is currently working with other agencies under the NC4 to develop regulations that will operationalize the Computer Misuse and Cybercrimes Act (CMCA), 2018.

### ***Directorate of Criminal Investigations***

292. The DCI on the other hand noted the need to strengthen and encourage use of Sandbox by other financial regulatory agencies such the one currently under Capital Markets Authority to test and inform regulations and guidelines for online investment applications in Kenya. In addition, the DCI noted the need to review the Computer Misuse and Cybercrimes Act 2018



to fully deal with the current realities in the cyberspace such as Artificial Intelligence (AI) as well as need to incorporate Communications Authority technical personnel to be stationed at all border entry points to provide technical expertise on all technological equipment's imported into the country.

293. The DCI informed the Committee that the Data Protection Act and the regulations thereunder do not sufficiently address key issues like the documents to be presented to the Data Commissioner to ascertain eligibility for issuance of a certificate as a Data controller and/or processor as a juristic person. The DCI submitted that the framework lacks regulatory framework for provision of documents to be presented to the Data Commissioner to ascertain eligibility for issuance of relevant certificate(s) to foreign entities.
294. The DCI further noted that the framework is not sufficient to enable the Commissioner to ensure that data subjects are properly taken through purpose for data collection, handling, transfer, entities, involved, possible risks and safeguards before accepting to give out their data. DCI further submitted that the framework has inadequate consumer protection of the data subjects and lacks procedures for thorough vetting of local and foreign data controllers and/or processors.

#### *Ministry of Health*

295. The Ministry of Health submitted that the collection of biodata from citizens has implications for privacy, security, and human rights. The Ministry underscored the need for robust, and forward-looking legislative interventions to govern the collection of biodata from Kenyans.
296. The Ministry submitted that it is currently driving digital transformation within the health sector to accelerate the achievement of universal health coverage. To ensure data security and uphold good data governance principles throughout the data lifecycle, the Ministry is developing various legislations and policies, including:
- a) **Digital Health Bill**, covering the classification of health data that includes medical equipment data, builds on the Data Protection Act to establish a framework for responsible handling, protection, and privacy of sensitive personal health data. It also creates a legal framework for a comprehensive integrated health information system and a Digital Health Agency to manage it. Additionally, it enables health data portability and the establishment of a client registry for unique identification.
  - b) **Health Data Governance Framework**, to set standards for governing health data throughout its lifecycle, including data collection.
  - c) **Telemedicine Guidelines**, to provide guidance on managing the telemedicine ecosystem in the country, including obtaining consent from clients/patients through telemedicine platforms.

- d) **National Unique Patient Identifier Framework**, to facilitate unique identification of clients across the healthcare system, although it is not based on biometric identifiers.

*Attorney General*

297. The AG submitted that there is a lack of a comprehensive Legal Framework to regulate emerging markets in cryptocurrency. The AG went on to state that the lack of legal framework to regulate emerging markets in cryptocurrencies has exposed the country to inherent risks, speculative trading, high price volatility, possibility of criminal activities, tax evasions, financing terrorism and money laundering, data theft and financial fraud.
298. As such, AG recommended the formation of a comprehensive oversight framework on crypto assets activities and players in Kenya. The AG *further recommended the development of regulations to establish a registration system for image rights and encompassing a dynamic definition of image personality rights which may include rights in characteristics, mannerisms or traits unique to that personality.*
299. AG also submitted that there is no consensus on the way to account for tax with respect to *Worldcoin* and in particular how to recognize any attendant income or losses, the appreciation of fair value and how to account for it in financial statements.
300. The AG further submitted to the Committee that *Worldcoin* situation has raised privacy concerns regarding the processing, storage and sharing of personal data where entities violate the data protection rules by sharing sensitive data or use open-source software that are easily compromised.
301. The AG went on to inform the Committee that the promoters of *Worldcoin* mislead consumers by using deceptive marketing strategies to induce people to exchange their personal data with tokens thus contravening their consumer rights.

*Data Commissioner*

302. The Data Commissioner informed the Committee that the Office faces challenges such as gaps in the legal framework on personal data protection, inadequate human capacity and voluntary provision of personal information in regulating the processing of personal information. She noted that for these to be addressed, the Office recommends for a review of the Data Protection Act, 2019 and Regulations as well as enhancement of the staff capacity and regional presence.
303. On whether the ODPC lacked enforcement capacity, the Data Commissioner submitted to the Committee that they have proposed in terms of legislative reform to be given data police for enforcement since their enforcement unit only deals with investigation and not arrests which as an office they conducted. The data Commissioner noted that the remedies available

at their disposal is enforcement notice, penalty notice and compensation to the data subject which they have demonstrated. The office has given *Worldcoin* an enforcement notice as well as timeline, failure to adhere to the enforcement notice will then lead to the penalty.

304. On whether the ODPC is a member of NC4, the Data Commissioner further submitted that the ODPC is neither a member nor co-opted member of NC4. The Commissioner went on to state that there is already a proposal to have them sit at the NC4.

***Ministry of ICT and Digital Economy***

305. The Ministry recommended that:

- a) There is need for policy and regulatory review to address emerging technologies such as AI and blockchain technologies. While at it, there is need to strike a balance to ensure responsible development and application of technology, while being careful not to stifle its development.
- b) There is need to strengthen provisions on due diligence before, during and after registration of data processors and controllers. Periodic assessment, and periodic reporting mechanisms should be put in place for data controllers and data processors. This will determine their eligibility for renewal of registration certificate.
- c) There is need for policy and institutional reforms to ensure surveillance and response where necessary is satisfactory since the Worldcoin started collecting data in 2021 only for the Data Protection Commissioner to know a year later.
- d) The Data Protection Act needs to provide for a Board, or similar authority to which the Data Commissioner reports or accounts in its daily operations.
- e) There is need for amendments along the models of Communications Authority of Kenya (CA) created under the Kenya Information and Communication Act, 1998 or the Media Council of Kenya. There is need for accountability through a Board and Council.

***Central Bank of Kenya***

306. The CBK submitted that converting crypto assets to legal tender requires the development of comprehensive regulatory frameworks, robust risk management practices, effective AML and KYC measures, and the establishment of secure systems to minimize potential risks to financial stability and address the challenges mentioned above.

307. Further, according to CBK, regulation of crypto assets requires widespread public discussion. CBK therefore, submitted that it is imperative to consult the wider public before making any decisions on the next steps of coming up with policies.

308. CBK further submitted that the Financial Reporting Centre (FRC) has constituted a working group which is currently undertaking a risk assessment on VAs and VASPs. Government agencies and private players such as commercial banks are involved in this exercise. CBK proposes that we await the risk assessment report on the issue.

### *Financial Reporting Centre*

309. According to the Financial reporting Centre (FRC), regulation of emerging technologies will always be faced with challenges as regulators try to catch up with the developments in the blockchain sector. FRC submitted that blockchain evolves on a daily basis thus making it difficult for regulators to keep up.

310. In that regard, FRC highlighted the following challenges and concerns in regulating the blockchain sector:

### *Money laundering and terrorism financing*

311. FRC submitted that due to the anonymous nature of transactions on VASPs, the number of users attracted to these platforms to launder money or carry out financially suspicious activities is alarming. FRC went on to note that VAs and VASPs are decentralized meaning most of the activities are unregulated and are not monitored.

312. As such, FRC noted that most users are attracted to the Vas and VASPs because the platforms are unregulated. However, FRC submitted that the lack of regulation and or mechanisms to implement the regulations in place, pose a challenge towards to the efforts to combat money laundering and Terrorism Financing.

### *Consumer protection*

313. FRC further submitted that the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe (MONEYVAL) published a report in June 2023 that highlighted fraud and child sexual exploitation as predicate offences identified by VASPs.

314. FRC went on to note that the report identified a vacuum in the regulations when it came to content moderation and consumer education by VASPs. Most of the regulations around VAs and VASPs focus more on licensing, registration and taxation. VASP platforms are capable of sharing entertainment content some of them may be harmful to the users.

315. The FRC observed that certain platforms have been utilized for fraudulent purposes. It further noted that creators of virtual assets take advantage of their high volatility to introduce virtual assets that may not generate any future profits for users or asset holders. It is essential to establish rigorous regulations and laws to safeguard against such occurrences in the future.

### Taxation concerns

316. FRC observed that the most difficult aspect of taxing virtual assets is that they are pseudonymous. FRC noted that the public addresses used are incredibly difficult to link with an individual or firm, making tax evasion easier.
317. FRC further submitted that there is need for classification of VAs for purposes of taxation. FRC noted for instance, that if the asset is sold as a commodity, value added tax (VAT) may be charged on it and thus the end user bears the cost. Most virtual assets gain value when they have been employed in a specific context rather than a free market value. What this means is that the normal rules of the market (that is demand and supply) may not necessarily affect the value of a virtual asset. This makes it difficult to come up with rules on fair trading.

### ***TFH Corp and TFH GmbH***

318. According to Worldcoin, there are currently no specific financial regulations that are applicable to virtual asset swaps in Kenya. Worldcoin noted that as a result, there are no licence, mandatory incorporation/registration and/or permits requirements that would apply to the provision of the WLD, the World App, or World ID on a cross-border basis to customers located in Kenya.
319. Worldcoin submitted that five institutions including the CBK, CMA, Insurance Regulatory Authority (IRA), Retirement Benefits Authority (RBA) and the Sacco Societies Regulatory Authority (SASSRA) formed a working group in December 2022 to investigate future regulations concerning the use of virtual assets in Kenya.
320. TFH Chief Legal Officer attended a meeting with the CMA in May 2022, introducing the project to CMA staff, and ultimately it was concluded that the Worldcoin project would not be an appropriate candidate to qualify under the requirements of the CMA's Regulatory Sandbox.
321. Indeed, in a "Cautionary Statement on Worldcoin" issued by the CMA on 2<sup>nd</sup> August 2023, the CMA stated, in pertinent part, as follows: 'The CMA has assessed the available public information concerning Worldcoin and hereby notifies the public that Worldcoin is not regulated in Kenya. Further, that Worldcoin-related products including crypto-tokens or their derivatives are not investment products within the scope of the Capital Markets Act and hence not under the regulatory purview of the CMA'.
322. In addition to the aforementioned cross-agency technical working group, the proposed Capital Markets (Amendment) Bill, 2023 proposed to widen the 'securities' definition to capture cryptocurrencies and possibly crypto assets; however, the Capital Markets (Amendment) Bill, 2023 is yet to be introduced to the Kenyan Parliament for First Reading

and the progression of the Capital Markets (Amendment) Bill, 2023 through the legislative process for now remains unclear.

323. The CBK National Payments Strategy 2022 – 2025 makes mention of crypto assets and currencies, and the various developments recorded in the crypto industry; however, the said strategy also highlights the various associated risks, such as high volatility. The strategy also indicates that the CBK will continue to provide a supportive regulatory framework, with a focus on issues such as stability and security of the financial and payment systems, and, in particular, cyber-resilience.

324. In the discussion Paper on Central Bank Digital Currency (CBDC), published in May 2023 the CBK highlighted the interest by central banks worldwide on the importance of developing a Central Bank Digital Currency. Ultimately, the CBK noted that a rollout of a Kenyan CBDC should not be “a race to the first”. The CBK also noted that it is not keen to implement a Kenyan CBDC in the short- to medium-term, but rather its focus should be to strengthen Kenya’s existing payment infrastructure.

### **3.3.9 Other Emerging Issues**

325. With respect to its ninth mandate, to inquire into other emerging issues, submissions received by the Ad Hoc Committee fell within the following thematic areas—

- a) Overlapping regulatory mandate among various authorities governing the cyber space in Kenya;
- b) Security concerns on blockchain technology and cryptocurrencies in Kenya;
- c) Legality of cryptocurrency and blockchain technologies in Kenya;
- d) Whether cryptocurrencies are potential avenues for money-laundering;
- e) The role of DCI in detection and monitoring of cybersecurity and cybercrimes in Kenya;
- f) Capacity of the Kenyan authorities to ensure cybersecurity;
- g) Whether the ODPC has collaborated with other state agencies to effectively discharge its mandates under the Data Protection Act, 2019;
- h) Measures to indemnify Kenyans from unlawful use of data by Worldcoin or its agents;
- i) The potential impact of cryptocurrencies on the banking sector in Kenya, and the possible remedial measures; and
- j) The capacity of the Central Bank of Kenya to regulate cryptocurrencies and other emerging technologies in the financial sector.

#### ***On the overlapping regulatory mandate among various authorities governing the cyber space in Kenya***

326. The Communications Authority of Kenya highlighted overlapping regulatory mandates among the various Authorities governing the digital space among the legal and regulatory

bottlenecks that occasion the unchecked activities of *Worldcoin* in Kenya. It noted that the overlapping regulatory mandates calls for more collaborative regulatory approaches to the governance and regulation of the digital space in Kenya.

327. CA submitted that it has made efforts to enter into partnerships with various agencies to enhance its regulatory effectiveness. For instance, the Authority submitted that it has a Memorandum of Understanding (MOU) with the Central Bank of Kenya (CBK) whose purpose is to enhance co-regulation of digital financial services.
328. CA further submitted that ICT is an enabler of development across all sectors. The CA noted that towards the realization of the envisaged digital transformation, collaboration and a multi-agency approach will enhance adoption of technology. However, to keep in pace with technological dynamism, we must prioritize adoption of robust and up-to date policy, legal and regulatory frameworks without stealing innovation.
329. The DCI on the other hand, informed the Committee that there is an urgent need to review the Data Protection Act to appreciate the overlapping roles of other regulatory Government agencies and investigative agencies in investigation and enforcement of Data Protection Act including but limited to, the Communications Authority, the Registrar of companies, Central Bank of Kenya, Capital Markets Authority, Consumer Protection Agency, KRA and National Police Service among others with stricter punishment for data mishandling and/or contravention of the Act. The review should also include the specific eligibility criteria for approval of an application as Data Controller and/or Processor as well as provision for back-ground check especially for entities intending to collect sensitive personal data.
330. On whether the DCI and the ODPC were members of the NC4, the DCI responded that the Directorate is an alternate member of the NC4 and they meet monthly to look at issues that affect cybercrime in the country. The DCI noted that they were currently developing the regulations that will operationalize the Computer Misuse and Cybercrimes Act, 2018 and the regulations were at the public participation stage. The DCI however, noted that the ODPC is not a member or an alternate member of NC4.
331. On why the DCI was bringing on board the Nuclear Power and Energy Agency into their investigations, the DCI informed the Committee that the investigators wanted to get a professional opinion in order to address issues specific to absorption rate, and whether the radiation was within the acceptable standards to enable them capture the same in their report and findings.

***On the legality and security concerns on blockchain technology and cryptocurrencies in Kenya***

332. The CBK defined blockchain as a distributed database or ledger shared among computers on a common network. CBK went on to state that each computer/node participates in the validation of transactions and the maintenance of the blockchain ledger. CBK noted that nodes are responsible for storing a copy of the blockchain ledger, verifying the authenticity of transactions, and adding new blocks to the chain. The blockchain maintains a secure and decentralized record of transactions, ensuring that data remains immutable (cannot be altered) upon entry.
333. The DCI on the other hand defined blockchain as an open, distributed ledger that records transactions safely and permanently. According to the DCI, blockchain slashes the cost of transactions and eliminate intermediaries like lawyers and bankers, and thus lowering the cost of doing business. The DCI noted that with the increase in more internet technologies, the adoption of blockchain will require broad coordination and will take time to be adopted. The DCI further noted that blockchain is the medium through which crypto-currency is transacted.
334. The CS for ICT and Digital Economy on the other hand, described blockchain technology as an advanced database mechanism that allows transparent information sharing within a business network. The CS submitted that blockchain database stores data in blocks that are linked together in a chain. The CS ICT and Digital Economy observed that in blockchain, the data is chronologically consistent because you cannot delete or modify the chain without consensus from the network and as a result, one can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. Further, the CS opined that the system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of transactions.
335. CBK submitted that the elements of transparency, security and finality provide many applications for blockchain technology, with the best-known application in cryptocurrency/asset. CBK also defined cryptocurrencies as privately issued digital assets that depend primarily on cryptography and blockchain/distributed ledger technology (DLT). CBK noted that the most widely used cryptocurrency, Bitcoin, was established in 2009 following the publication of a seminal paper on peer-to-peer transactions by "Satoshi Nakamoto" in 2008. According to CBK, Bitcoin remains the biggest and most known crypto asset and was created as an answer to the deficit in trust in the financial industry following the 2008 Global Financial Crisis.
336. Similarly, the AG submitted that cryptocurrency is a currency founded on blockchain technology and based on a study by the World Trade Organization (WTO), cryptocurrency could be described as a decentralized, distributed record or "ledger" of transactions in which



the transactions are stored in a permanent and near inalterable way using cryptographic techniques.

337. The DCI on the other hand, informed the Committee that unlike the fiat currency, cryptocurrency is a digital, encrypted and decentralized medium of exchange and that there is no central authority that manages and determines the value of the digital currency. Instead, the determination of the value of the virtual currency is through speculative tendencies of the users of the cryptocurrency.
338. CBK further itemized the IMF categorization of cryptocurrencies as follows:
- a) **Unbacked crypto assets;** are transferable and primarily designed to be used as a medium of exchange. They are often decentralized. However, there are examples of unbacked crypto assets that are centrally issued and controlled. Most unbacked crypto assets are currently used for speculation and not for payment purposes. Prominent examples include Bitcoin and Ether.
  - b) **Utility tokens;** provide the token holder with access to an existing or prospective product or service. These are usually limited to a single network (that is, the issuer) or a closed network linked to the issuer. For example, a tokenized store card or certain gaming tokens might be considered types of utility tokens.
  - c) **Security tokens;** are tokens that provide the holder with rights like that of a traditional security, for example, the right to a share in the profits of the issuer.
  - d) **Stablecoins;** aims to have a stable price value. This objective is normally pursued by the crypto asset being linked to a single asset or a basket of assets, for example, fiat funds, commodities such as gold, or other crypto assets. Stablecoins can also seek stabilization using a mechanism other than being linked to an asset, for example, through an algorithm. These "algorithmic" stablecoins are mainly used in decentralized finance (DeFi). Prominent examples include Tether, Binance USD, and USD Coin.
339. On the relationship between blockchain and cryptocurrency, the NIS submitted that blockchain and cryptocurrency technologies are closely linked, with cryptocurrency being a prominent application of Blockchain technology. The NIS submitted that Blockchain is a decentralized and tamper-resistant digital ledger, while cryptocurrencies use cryptography for security.
340. The DCI submitted that blockchain is the technology behind *Bitcoin*, the first virtual digital currency that has gained international application in financial settlements. In addition, the DCI noted that uncertainty regarding taxation, security risks, transaction irreversibility, scalability issues, lack of merchant adoption and trust of digital currencies being purely speculative are some of the elements of cryptocurrency that poses great security and economic concerns.

341. On the use of cryptocurrency in Kenya, the NIS submitted that cryptocurrency adoption is notable, with the country ranking first globally for peer-to-peer trading volume. The NIS submitted that various cryptocurrency exchanges operate in Kenya, with Bitcoin being the most used cryptocurrency, and others like Ethereum and Ripple gaining popularity.
342. However, the CBK cautioned that cryptocurrencies are neither issued by any central bank nor a public authority and are therefore not considered legal tender. It noted that only banknotes and coins issued by the CBK are considered as currency, while noting that, since crypto assets are not backed by a public authority, they are considered high-risk and speculative.
343. Similarly, the DCI informed the Committee that cryptocurrency is not a legal tender and is unregulated by the CBK, however, it is not criminalized by the Kenyan Laws. The DCI noted that the lack of regulation coupled with the absence of express provision of the law criminalizing cryptocurrencies in Kenya have allowed for the transfer and trade in cryptocurrency without any regulatory checks therefore thriving and encouraging anonymity in financial transactions across borders on various online platforms as well as creating easy access to finances by criminal groups including terrorists and also a fertile avenue for money laundering and tax evasion.
344. According to the CBK, the growth of the crypto industry is driven by the speed of transactions, low transactions, and costs, decentralization of finance, and anonymity. Additionally, CBK opined that crypto assets have attracted users because it offers more control as opposed to fiat currency. Further, CBK submitted that the promise of high returns due to the high volatility and erratic growth in the value of crypto assets has attracted a swathe of crypto investors, spanning both individuals and institutions. Moreover, CBK noted that the lack of taxation mechanisms has made crypto attractive to users.
345. The DCI submitted that the laws of Kenyan are silent on cryptocurrency which is a popular financial tool for organized crime thus encouraging transfer of unregulated digital currency outside the existing legal framework which has occasioned the rise in crypto-jacking as an emerging crime trend with no laws to address it. The DCI further submitted that the delicate and volatile nature of transactional data makes traceability of such financial transactions difficult and thus derogates the efforts made by the investigative agencies.
346. CBK submitted that compared to physically issued banknotes and coins, and electronic mobile money which is backed one-for-one with the fiat currency, holders of crypto assets do not benefit from the same level of consumer protection accorded by legal tender issued by CBK. CBK opined that crypto assets experience extreme volatility and the risk of collapse, with no recourse for affected investors.

347. Further, the CBK submitted that due to the extreme volatility of the crypto market and the recent collapse of stablecoins and crypto exchanges, there has been a slowdown in the uptake of crypto assets. To illustrate, CBK noted the global crypto industry faced a reduction in the value of crypto assets and market capitalization by more than half in 2022. For instance, CBK submitted that Bitcoin was trading at below USD 16,000 on 20<sup>th</sup> November, 2022, down from USD58,000 exactly a year earlier. CBK opined that the volatility has led to investor caution and reduced interest in crypto assets. More importantly, CBK noted that the volatility has highlighted key liquidity issues faced by crypto asset firms and other fintechs, exacerbated by poor governance frameworks.
348. Further, the AG observed that despite the warning by the CBK on the use of cryptocurrencies due to their volatility, no law put in place to regulate the use of cryptocurrency. The AG further stated that from the FRC report made on 16<sup>th</sup> August 2023, there has been a rapid growth of the digital asset ecosystem and its potential to drive financial innovation and efficiency, but if not urgently regulated, money laundering and other crimes are expected to rise.
349. On the criminal acts associated with cryptocurrencies, the Financial Reporting Centre (FRC) on the other hand submitted that cryptocurrencies can be used for money laundering and terrorism financing just like the fiat currencies can be used for illicit activities. FRC enumerated the crime risks associated with virtual assets:
- a) **Pseudonymity** - Proceeds of crime can be paid in crypto due to their nature that allow users to create wallets and conduct transactions without revealing their true identities.
  - b) **Global accessibility** - allowing them to be accessed from anywhere in the world making it possible for money launderers to move funds across borders.
  - c) **Availability of mixers and tumblers** - who make it difficult to trace the source of funds.
  - d) **Ease of interface** - with electronic payment solutions i.e. PayPal, Mpesa, electronic cards, makes it easy to move proceeds of crime across electronic wallets and borders.
350. NIS on the other hand, submitted that the current state of cybersecurity in Kenya is characterized by dynamic and unpredictable challenges due to the increased adoption of cyber technologies. The NIS noted that the Kenya's cybersecurity readiness is considered reactive, with limited structures for protection and response. It cited the key vulnerabilities to include overdependence on foreign tech, weaknesses in critical infrastructure systems, inadequate cybersecurity investment, inadequate regulatory frameworks, and insufficient cybersecurity awareness. NIS further submitted that Kenya also faces challenges such as limited threat visibility, rising cybercrimes, lack of information sharing, and the use of digital platforms by criminal groups.
351. The NIS highlighted cyber sabotage (disruption of critical infrastructure), cyber espionage (theft of data), cyber terrorism (using technology for violent acts), and cyber

subversion (propaganda and misinformation) among the predominant manifestations of cybercrimes in Kenya. Further, the NIS noted that the numerous incidents in 2023 illustrate these threats, including ransomware attacks on government and private entities, data breaches, and phishing attacks.

352. The NIS submitted that one of the most prevalent cyber threats is phishing attacks, where hackers impersonate reputable entities or trading platforms to trick users into revealing sensitive information. The NIS further submitted that malware poses another substantial risk, with crypto-mining malware exploiting the computational power of infected machines and wallet-stealing malware compromising digital assets. The NIS submitted that fraudulent trading platforms have emerged, resulting in substantial financial losses for unsuspecting users.
353. On the concerns about the security of cryptocurrency accounts, the NIS submitted that users access their digital assets through private keys, and if the keys are not securely stored, they can be vulnerable to theft. Moreover, the NIS submitted that the lack of regulatory oversight in the cryptocurrency space leaves investors without adequate protection and legal recourse in the event of fraudulent activities.
354. On third-party application of cryptocurrency, the NIS submitted that the same is useful for monitoring cryptocurrency prices and managing portfolios, but can pose risks, especially when they require sharing sensitive information with developers. The NIS also noted that money laundering and terrorism financing have made cryptocurrency vulnerable, as the anonymity of cryptocurrencies has been exploited for illicit financial activities.
355. On the identity theft through SIM card fraud, where stolen identities are used to fraudulently register SIM cards and engage in cryptocurrency transactions. To mitigate these risks, individual crypto traders should carefully read and understand the terms and conditions of trading platforms, double-check the legitimacy of websites, enable two-factor authentication (2FA) or multifactor authentication (MFA), exercise caution when using third-party applications, and avoid using trading platforms as long-term storage for digital assets.
356. The NIS also enumerated the economic implications of cryptocurrencies, including financial inclusion, remittances, investment opportunities, potential impacts on monetary policy, and taxation challenges. It also noted the regulatory implications of cryptocurrencies to encompass consumer protection, anti-money laundering (AML) and know-your customer (KYC) procedures, market integrity, investor safety, financial enter stability, international competition, and legal recognition.
357. The NIS noted that blockchain has several advantages in Kenya, including combating corruption, reducing national debt through digital asset frameworks, improving democracy

and elections, promoting financial inclusion, enhancing agriculture and food security, streamlining land titling, and facilitating affordable housing.

358. The NIS however, noted that cryptocurrencies also pose security concerns due to their potential for anonymity, borderless transactions, difficulty in tracing decentralization, lack of third-party intermediaries, and limited regulation. In acknowledging the opportunities and risks presented by cryptocurrencies, the NIS submitted that it has established an internal Working Group dedicated to investigating cryptocurrency-related activities and emerging trends. The Working Group engaged in consultations with various regulatory bodies and institutions, including the Central Bank of Kenya, Capital Markets Authority, Kenya Revenue Authority.
359. The NIS submitted that while cryptocurrencies offer economic benefits and innovative applications, they also raise complex regulatory and security challenges that require careful consideration and balanced approaches to ensure responsible and safe use in Kenya. NIS also submitted that blockchain intelligence tools can help government regulators detect and mitigate illicit financial activities, and public awareness campaigns are needed to educate the populace about cryptocurrency risks and mitigation strategies. The NIS went on to noted that to mitigate the threats, it has taken measures such as cybersecurity sensitization programs, system security audits, cyber operations, and issuing advisories to relevant government agencies
360. Further, the NIS underscored the need to develop a comprehensive national cybersecurity risk management framework, acceding to international conventions, developing regulations for emerging technologies, strengthening legal frameworks, enhancing governance and coordination, investing in cybersecurity capacities, improving threat monitoring and enhancing international cyber cooperation.
361. The NIS noted the need to integrate cyberspace as the fifth dimension of warfare in the National Security Strategy (NSS) due to its cross-cutting and cross-border dimensions and influence on the socio-economic status of the nation.
362. The NIS urged policymakers to formulate and enforce regulations governing virtual assets and providers to combat fraud, money laundering, and terrorism financing. It further submitted that international cooperation among regulatory authorities is essential for effective monitoring of cryptocurrency service providers and maintaining regulatory efficacy.
363. On its part, the NIS submitted that it has employed an elaborate and robust protocols and strategies to monitor cryptocurrency activities for financial crimes and terrorism. The NIS submitted that the Worldcoin and other cryptocurrency platforms have been under close monitoring by the Service for signs of money laundering and terrorism financing. It further

submitted that the strategies employed have been effective, although they may need to be complemented by enhanced law and policy.

364. On money laundering and terror financing, the NIS informed the Committee that it began monitoring Worldcoin when it started hiring its sales team and they monitored them alongside other cryptocurrencies but Worldcoin did not meet their threshold on national security reconciliation revolving around potential links to financial crimes, money laundering and terror activities and looked at it as a normal emerging cryptocurrency. The NIS submitted that analysis had not established any indications of money laundering or terror financing by Worldcoin.
365. On how to secure crypto from being used as a tool for money laundering and funding of terrorism, the NIS submitted that Kenya needs clear legislation outlining what is money laundering and what is not as well as giving us the capabilities to be able to fuel the space and also regulate it. The NIS noted that regulating cryptocurrency can only be done through legislation as well as adequate allocation of resources in terms of funding to allow government entities charged with the responsibility to be able to undertake their mandate since the tools that are required and must be invested upon are not very cheap.
366. The NIS noted that it has recognised the growing influence of cryptocurrencies, and has included cryptocurrency-related activities in their intelligence and counterintelligence efforts. The NIS noted that an initial focus was on a local cryptocurrency project called NURUCOIN, which was involved in fraudulent activities amounting to KES 27 billion, and that the matter was referred to the Directorate of Criminal Investigations (DCI) for further action.

***On whether cryptocurrencies are potential avenues for money-laundering***

367. The Financial Reporting Centre (FRC) submitted that the rapid evolution of financial technologies and the increasing prominence of virtual assets have brought forth new challenges and opportunities for the financial sector. FRC noted that as virtual asset adoption grows, it becomes imperative to establish a regulatory framework that promotes transparency, security, and compliance.
368. FRC described virtual assets as a form of digital or virtual currency that utilizes cryptography for security. It went on to note that the assets exist purely in digital form and are typically decentralized, meaning they are not controlled by any central authority like a government or financial institution.
369. Statistically, FRC submitted that the number of virtual asset owners have increased, particularly in the last two years. AFRC noted that a wealth report carried out by *Knight Frank* in 2022 stated that 6% of Kenya's dollar millionaires own Non-Fungible Tokens (NFTs). Additionally, a report by *United Nations Conference on Trade and Development*

(UNCTAD) states that 8.5 percent of the Kenyan population or 4.25 million people own cryptocurrencies.

370. Based on open-source research, Kenya had a growing ecosystem of virtual assets with a growing interest in cryptocurrencies being used for various purposes like investment, cross border payments and online transactions. The Chainalysis report 2022 Geography of Cryptocurrency Report places Kenya in position 19 on crypto adoption and position 5 with peer-to-peer exchange.
371. However, upon evaluation of the Kenyan regulatory landscape, there is an apparent gap in definitive regulatory and Institutional framework that covers the Virtual Asset and Virtual Asset Service Providers sector. Most of the activities carried out by the service providers tend to be regulated by the already present financial institutions. These institutions have neither classified nor issued guidelines on the various Virtual Assets and Virtual Asset service providers in the country.
372. FRC submitted that the Kenya's Anti-Money Laundering and Terrorism Financing Mutual Evaluation Report 2022 rated the country non-compliant with FATF Recommendation 15 on the general and comprehensive requirements of regulation and risk assessment of VAs and VASPs. The main reason for the rating was a lack of legal and enforceable regulation and policies to regulate the VA sector. The Mutual Evaluation recommended that Kenya should take a policy decision as to whether to prohibit or allow VASPs in Kenya. Where a position is taken to allow VASPs, licensing/ registration requirements should be implemented, and a risk assessment relative to ML/TF risks with regards to their operations should be conducted. Additionally, a framework for supervision of VASPs for AML/CFT should be set up.
373. Further, on September 1<sup>st</sup>, the Finance Act 2023 introduced a 3% tax to apply to all digital assets transactions, crypto currencies included came into force. The introduction of tax on blockchain transactions is step in the right direction toward recognizing virtual assets and blockchain transactions in law. However, taxation of the sector may face some challenges as there are no laid down laws, regulations, procedures or defined institutions currently that regulate or supervise virtual assets and virtual asset service providers.
374. While noting that cryptocurrencies are unregulated and not criminalized in Kenya, CBK submitted to the Committee that it is currently monitoring global trends in cryptocurrency regulation and anti-money laundering measures. However, CBK submitted that it is actively working towards establishing a clear policy position on cryptocurrencies and virtual assets

*On the role of DCI in detection and monitoring of cybersecurity and cybercrimes in Kenya*

375. The DCI informed the Committee that section 35(b), (d) and (i) of the National Police Service Act No.11A of 2011 mandates the Directorate of Criminal Investigations with the responsibility of detecting and investigating cybercrimes. The Act also charges the DCI with the responsibility of coordinating the country's INTERPOL Affairs. In addition, Section 47 of the Computer Misuse and Cybercrimes Act, 2018 sets out the powers and investigation procedures of offences under the Act and grants the powers to the National Police Service among other relevant Government agencies.
376. The DCI, further noted that the DCI has a dedicated Cyber Forensic Laboratory that facilitates investigators in collection, forensic analysis, preservation and presentation of digital and electronic evidence in courts. The DCI went on to note that the Digital Forensic Lab has a section that conducts internet patrols whose main task is to identify any scam targeting Kenyans and/or any information about Kenyans published in the dark-web/dark-net and they prepare reports which are shared with cybercrime investigators for action. The DCI further noted that the Crime Research & Intelligence Bureau and the Investigations Bureau within the DCI play a critical role in detection, investigation, preservation and documentation of evidence as well as identification and apprehension of suspects.
377. DCI informed the Committee that his directorate is an alternate member of National Computer and Cybercrimes Co-ordination Committee (NC4) and also has officers seconded at KE-CIRT/Coordination Centre and other institutions. DCI noted that it also works hand in hand with other government regulatory agencies, telecommunication service providers and other foreign law enforcement agencies. They also collaborate on cybercrime issues at the sub-regional by participating in East Africa Police Chiefs Co-operation Organization (EAPCCO) annual meeting through various committees and sub-committees, cybercrime sub-committee being one of the key committees.
378. In addition, they are also in the regional and international level by participating in the INTERPOL cyber surge project which is an initiative by INTERPOL for the African region that involves law enforcement officers from member countries. The African Union Police Initiative (AFRIPOL) and INTERPOL's African Joint Operations against Cybercrime (AFJOC) in collaboration with INTERPOL's Cyber Fusion Centre (CFC) and INTERPOL's private partners performed an extensive analysis on malicious and vulnerable infrastructure within member country jurisdiction and generated a Cyber Activity Report (CAR). Mr. Amin submitted that the CAR was disseminated to Kenya as one of the member countries via Kenya's INTERPOL National Central Bureau (NCB). The operation is currently ongoing with expectations to advise all vulnerable Internet Service Providers (ISP) and inform all Critical Information Infrastructure (CII) on their targeted assets.



379. The DCI informed the Committee that it is a member of the African Heads of Cybercrime Units initiative where all heads of units meet annually under the auspices of INTERPOL with the aim linking the unit heads to enable collaboration and co-operation. The initiative has helped in sharing of intelligence, vulnerabilities, challenges and best practices. The DCI further noted that the DCI is also a member of INTERPOL Global Complex for Innovation (IGCI) that brings together experts from a wide range of backgrounds through INTERPOL Innovation Centre which develops contemporary and creative solutions to challenges in policing. IGCI facilitates thought leadership and connects law enforcement, academia and private sector partners to exchange knowledge and explore new technologies and emerging cyber threats.
380. The DCI further informed the Committee that their investigators have engaged various Government regulatory agencies such as Central Bank of Kenya, Communications Authority, Office of the Data Protection Commission, Registrar of Companies, Capital Markets Authority, Kenya Bureau of Standards, Nuclear Power and Energy Agency, Consumer Protection Agency and INTERPOL to give an input in the investigations and investigations were at an advanced stage and shall share their recommendations with the ODPP upon conclusion.
381. In conclusion, the DCI echoed to the Committee that the Investigations into the Worldcoin operations and activities were at an advanced stage and that the investigators were exploring all legislations that could have been violated including but not limited to; Penal Code, Computer Misuse and Cybercrimes Act 2018, Data Protection Act 2019, Kenya Information & Communication Act, Proceeds of Crime and Anti-Money Laundering Act, 2009, Prevention of Terrorism Act 2009 and The Companies Act 2015.
382. The DCI also noted the urgent need for additional budgetary allocation to enable the DCI improve the capacity of the cybercrime unit through regular trainings and provision of equipment justifying that the ICT world is dynamic and ever-changing thus the need to deal with threats while appreciating innovation. The DCI further noted that owing to the emerging new technologies like Artificial Intelligence, malwares, ransomwares and botnets, the DCI recommend that more funding be channeled to the Directorate to enable development and enhancement of modern simulation laboratories, malware laboratories and penetration testing tools among others. In addition, the Directorate requires to purchase International Mobile Subscriber Identifier (IMSI) catchers which will enable it to fully handle its mandate of detection, prevention and investigations of crime.

*On the capacity of the Kenyan authorities to ensure cybersecurity*

383. On the qualifications of the officers currently managing Kenya's cybersecurity, the DCI informed the Committee that they have a DCI cyber -comprehensive unit comprising of graduate officers in ICT are well trained both locally and internationally as well as exposed

to best international practices currently managing cyber lab and that they shall continue to recruit best brains in the market so that they are up to speed with happenings in the contemporary world.

384. The DCI added that despite the constant attacks from both local and foreign entities, they are well placed and well-grounded in addition to having a well-trained team to help in performing their duties to the best of their capacities. The DCI noted that that it has an Incident Response Team Unit that responds to all incidences that happen within the country and also collaborate with other government agencies like the Central Bank of Kenya, Communication Authority of Kenya and Information and Communication Technology Authority. The DCI further noted that it has seconded four officers at the Kenya Computer Incident Response Team coordination Centre (KE-CIRT/CC) who participate in all operations.

385. On collaboration with other jurisdictions, the NIS informed the Committee that when it comes to critical installations and assets, the NIS is very careful about collaboration and cannot open up their critical infrastructure to each and every person. The NIS noted that even though they have close allies, they still have Kenyans interests at heart that they have to safeguard. The NIS further submitted that they do collaborate with other countries, but with limitations. The NIS noted that they have a very robust research and innovation department as well as the requisite human resource and they are trying to create their own solutions, software and hardware so as to become less dependent on foreign equipment and software. The NIS further noted that most of their software are in-house and only collaborate with other countries in case of something that they cannot get and when they get it, they try to do reverse engineering and ensure that they are able to do and create their own so that they are completely safeguarded against cyber espionage and sabotage.

***On whether the ODPC has collaborated with other state agencies to effectively discharge its mandates under the Data Protection Act, 2019***

386. The Data Commissioner submitted to the Committee that the ODPC in collaboration with other agencies from CA, CBK, Ministry of ICT and Digital Economy, NC4 and a Data Protection professional commenced investigations to ascertain the activities of *Worldcoin* in Kenya. From the investigations, the ODPC established that:

- a) TFH Corp and TFH GmbH were registered as data controllers by the ODPC;
- b) TFH, Worldcoin Foundation and World Assets Limited are not required to register as foreign companies before authorization to operate as data controllers/processors in Kenya, and thus were not registered as foreign companies under the Companies Act, 2015;

- c) TFH & *Worldcoin* were, through their products – World App, World ID and Worldcoin Protocol collecting personal and sensitive personal data. The location of the data remains unclear but includes – Italy, South Africa, Germany, Poland and United States.
- d) From a preliminary review of the documentation, the security of the data cannot be impeached. However, there is need for the Government to conduct an independent security audit.
- e) TFH indicated that the precise number of verified Kenyan users is 508,569.
- f) The purposes of collection of the personal data varied and included provision of World ID, provision of Worldcoin, development, training and testing machine learning models.
- g) From the evidence available, the consent obtained from Kenyans was insufficient and did not comply with Section 32 of the Data Protection Act, 2019.

387. The Data Commissioner further submitted that the multiagency team made the following recommendation:

- a) The current suspension on operations of TFH in Kenya to continue for a period of 12 months until the data controller satisfies to have met specified conditions including – a security audit, provide the Government access to the data, registration with BRS, establishment of a local representative, simplify their consent, carry out a DPIA and provide clarity on data storage.
- b) Cancellation of the Data Controller Certificates for TFH Corp and TFH GmbH for - failure to comply with the ODPC directive of 30<sup>th</sup> May, 2023 to cease and desist processing of sensitive personal data, failure to conduct a DPIA on the new processing operations and inconsistencies on where the Kenyan data is stored.
- c) Worldcoin applies to a registered Kenyan Regulatory Sandbox Program (preferably Capital Markets Authority sandbox) which allows for the project's products, solutions and services to be tested before roll out to the Kenyan market.
- d) World App to be pulled down from all App Stores within the Kenyan Region until recommendations number 1 to 3 are fully and satisfactorily met.
- e) Legal reforms on:
  - (i) data localization requirement for large scale collection of sensitive personal data;
  - (ii) ODPC be allowed discretion in issuance of administrative fines;

(iii) companies conducting commercial activities of significant impact to national security and economy to have a physical office in Kenya.

- f) AG, CMA & CBK spearhead regulation of digital assets and cryptocurrency (define the same as 'securities' under CMA Act.
- g) KRA to monitor the identified companies for payment of income tax on income derived from cryptocurrency in accordance with the Finance Act, 2023.

***On the measures to indemnify Kenyans from unlawful use of data by Worldcoin or its agents***

388. The Data Commissioner submitted to the Committee that the Data Protection Act is a self-healing statute which provides for safeguards to Kenyans against unlawful use of their data by a data controller or data processor. She further submitted that in order to protect data subjects, the Act has empowered the ODPC to:

- a) cancel a data controller's certificate as provided in section 22 of the Data Protection Act;
- b) issue enforcement notices as provided in section 58 of the Data Protection Act, issue penalty notices as provided in Section 62 of the Act;
- c) issue administrative fines as provided in section 63 of the Data Protection Act; and
- d) direct the compensation to the data subject as provided for in section 65 of the Data Protection Act.

389. The Data Commissioner went on to state that the foregoing provisions are sufficient indemnification provisions to ensure that data subjects can be indemnified in cases where unlawful use has occurred. In the interim, the Data Commissioner submitted that it had taken a raft of measures including the revocation/cancellation of the registration certificate No. 139-138A-E5D9 and registration certificate No. 325- 9256-645E earlier issued to TFH Corp and TFH GmbH respectively on 5th September 2023. The Commissioner further noted that pursuant to section 58 of the Act, the ODPC had issued Enforcement Notice to *Worldcoin*.

390. The Data Commissioner further stated that if investigation conducted establishes that there has been violation of data subject, the data subject has the right to have personal data erased and forgotten as provided under section 40 of the Data Protection Act. The Data Commissioner further observed that in the recommendations of the multi-agency, an audit should be conducted in the case of *Worldcoin* to confirm that information has actually been deleted if they are found guilty of violating data subject rights. The Commissioner further submitted that the Act provides for compensation of data subject in case the individual files for breach.

391. The assertions by the Data Commissioner were affirmed by the Worldcoin which submitted that a user can revoke her consent and have her image data and World App

account data deleted at any time directly in World App, through the online request portal at [worldcoin.org/requestportal](http://worldcoin.org/requestportal) or via email.

392. The AG also submitted that at this point of time, it is unclear to the Office of the Attorney General, the intention behind the cataloguing of Iris scans, whether the biometric data collected will be utilized for the intended purpose, if Kenyans who participated were afforded an opportunity to opt out of the storage of their biometric data and indeed if informed consent was garnered from the citizens who participated in the endeavor.
393. The Committee sought to know if there are other independent audits done on the algorithms of *Worldcoin*, the Worldcoin submitted that there have been independent audits run by other firms to cross examine Worldcoin and the information was provided to the ODPC. The Worldcoin submitted that the information was stated in their website to ensure transparency.

***On the potential impact of cryptocurrencies on the banking sector in Kenya, and the possible remedial measures***

394. FRC submitted that CBK issued a public cautionary statement and circular to financial institutions on trading in cryptocurrency thus limiting access to banking services for cryptocurrency-related businesses leading to an increase of peer-to-peer trading.
395. FRC noted that Kenya has included crypto currencies, NFTs and transactions carried out on the blockchain in the definition of digital assets. According to FRC, that implies that transactions carried out on the blockchain are now required to pay 3% tax of the total transaction. FRC noted however, that the Kenya Revenue Authority (KRA) is yet to communicate on guidelines or the procedure for tax remittance.
396. FRC reported that in January 2023, the Financial Sector Regulators Forum, a joint body of all financial sector regulators in Kenya resolved to work together to work on recommendations for the establishment of an oversight framework to regulate blockchain activities in Kenya. FRC submitted that the Forum came up with the Capital Markets (Amendment) Bill 2023 to amend Section 2 of the Capital Markets Authority Act to include definitions on blockchain, crypto currencies and crypto miners.
397. FRC submitted that the Capital Markets (Amendment) Bill, 2023 proposed an amendment to the definition of securities under the Act by including digital currencies. FRC submitted that the Bill defines digital currencies as digital representations of value that lack the legal status of currency or money and are not issued or guaranteed by a central bank or public authority. According to FRC, the Bill also proposes to have a baseline of 10,000 customers and an operation period of two years for VA to be allowed to enter the Kenyan market by CMA.

398. Moreover, FRC submitted that the proposal provides that for a person to be granted a license to trade in digital currency they must first register with CMA, keep a record of all transactions and pay tax on any gains made on transactions carried out on the trading platform.
399. FRC further submitted that in June 2023, it set up a multi-agency working group to conduct a risk assessment with the aim of identifying, understanding, and assessing the overall ML/TF risks related to VA and VASPs in the country. In that regard, FRC noted that the assessment is at data collection stage with FRC having circulated the relevant questionnaires to the public, reporting entities, law enforcement agencies and other appropriate entities.
400. In April 2023, the National Treasury and Economic planning established a Committee to develop an oversight framework for crypto assets activities and players in Kenya with a view to addressing policy and regulatory gaps identified in Kenya's Mutual Evaluation Report.
401. When asked about the potential impact of cryptocurrencies on the banking sector in Kenya, and the remedial measures being considered to address the challenges CBK recognized that cryptocurrencies and blockchain technology have the potential to disrupt traditional banking services. CBK noted that the disruption of traditional banking services by cryptocurrencies and the blockchain technology is a global trend, and CBK is closely monitoring developments in the space to understand their implications for the financial sector in Kenya.
402. CBK submitted that whereas there are potential benefits to adopting blockchain technology and digital assets, such as increased efficiency and reduced costs, there are also risks and challenges that need to be addressed. CBK went on to enumerate the following areas for consideration:
- a) Cryptocurrencies and blockchain technology can drive competition and innovation in the financial sector, thus, banks need to adapt and explore ways to incorporate blockchain technology into their operations to remain competitive.
  - b) To mitigate risks and ensure stability, it is essential to establish clear and comprehensive regulations for the use of cryptocurrencies and digital assets. This will provide a level playing field for both traditional banks and emerging fintech companies.
  - c) Collaboration between traditional banks and fintech companies is beneficial. Banks should explore partnerships and collaborations with fintech firms to leverage the technology while maintaining regulatory compliance.

- d) Banks should assess the potential risks associated with cryptocurrencies and develop risk management strategies. This includes addressing issues related to money laundering, fraud, and customer protection.
- e) Central bank digital currency (CBDC). Some central banks around the world are exploring the development of CBDCs, which are digital versions of a country's fiat currency. The Central Bank of Kenya is also studying the possibility of issuing a digital currency, which could coexist with physical cash and provide a secure and efficient payment system.

403. Further, CBK submitted that whereas cryptocurrencies and blockchain technology pose challenges to traditional banking, they also offer opportunities for innovation and efficiency. CBK noted that it is committed to fostering a competitive and secure financial sector that can adapt to the changes while maintaining stability and protecting consumers. CBK submitted that it will continue to assess and respond to developments in the rapidly evolving landscape

***On the capacity of the Central Bank of Kenya to regulate cryptocurrencies and other emerging technologies in the financial sector***

404. When asked about the capacity of CBK to manage emerging technologies like blockchain and artificial intelligence within its current mandate and what the committee could do to safeguard Kenya's financial system, the Governor CBK submitted that they have been proactive in staying updated with new technologies, including Central Bank Digital Currency (CBDC) research and payment system innovations. CBK assured the Committee of its commitment to financial stability and staying updated with technology.

405. When asked to explain the approach of CBK to regulating cryptocurrencies and the considerations taken in developing the approach, CBK submitted as follows:

- a) CBK has actively explored the concept of central bank digital currencies (CBDCs). They conducted research, engaged in public participation, and received comments from various sources globally, considering both the advantages and disadvantages.
- b) CBK believes that Kenya is currently in a reasonably good position regarding financial inclusion and digital payments. M-Pesa, for example, has significantly improved financial inclusion over the past decade.
- c) CBK does not consider the introduction of a central bank digital currency to be a top priority at this stage. Instead, the focus is on identifying challenges in the existing payment system and improving it to further enhance financial inclusion.

- d) CBK is closely monitoring developments in the cryptocurrency and digital payment space, acknowledging the adoption of Bitcoin as a legal currency in some countries such as Namibia and the Central African Republic.
- e) CBK is not ignoring these developments but is exercising caution to maximize opportunities while minimizing risks associated with rapidly evolving technologies. They recognize the potential risks related to issues like money laundering and terrorism financing.



## CHAPTER FOUR

### 4.0 COMMITTEE FINDINGS AND OBSERVATIONS

#### 4.1 Committee Findings

406. Arising from the first term of reference, on the operations and the ultimate objectives of the activities of Worldcoin in Kenya, the Committee made the following findings.

#### **THAT:**

- 1) Worldcoin is a cryptocurrency platform that aims to provide universal access to the global digital economy by authenticating individuals using iris scans. It is an ecosystem comprising three components; privacy-preserving digital identity network (World ID) built on proof of personhood, Worldcoin Token (WLD) and Application wallet (World App). To participate, a user is required to register through mobile app downloadable from the website [www.worldcoin.org](http://www.worldcoin.org) using a smart device and undergo iris scan via biometric device called Orb.
- 2) The Worldcoin is a global project initiated by Tools for Humanity GmbH, a global software and hardware development company based in Berlin, Germany and Tools for Humanity Inc. based in the USA. The project operates in thirty-four (34) other countries. It does not however, operate in the US and China due to lack of clear regulatory framework.
- 3) TFH Corp and TFH GmbH are the two companies registered as data controllers in Kenya on 15<sup>th</sup> September, 2022 and 18<sup>th</sup> April, 2023 respectively, but data was moved to Worldcoin Foundation which was not a registered data controller or processor in Kenya.
- 4) To verify the authenticity of the user as a true and unique human being, the user's iris is scanned using the Orb, a device provided by TFH. The iris image is converted into a digital code which is then transmitted to the TFH third party servers hosted by Amazon Web Services in South Africa.
- 5) The Orb is a telecommunication device with a capability to transmit real time iris images converted into digital code to their third-party servers hosted outside the country and not a biometric scanner as claimed to have been declared at the point of entry in Kenya. Despite being a telecommunication device, the orbs did not undergo type approval by the CA as required by the *Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010*.
- 6) In Kenya, Worldcoin deployed orbs in over thirty (30) locations in Nairobi including malls and learning institutions and started collecting data in public places in May 2021,

before registering as data controllers contrary to section 19(7) of the Data Protection Act, 2019. This fact only became known to ODPC in April 2022, and to the MoICDE and other Government agencies towards the end of July 2023. This is after the registration went live at KICC on 24<sup>th</sup> July 2023 and when the matter became of grave public concern after long queues of people seeking to register were experienced.

- 7) Worldcoin enticed Kenyans to subscribe to the platform by issuing 25 Worldcoin Tokens on verification. The tokens were to be converted to USDT, a virtual US dollar on a cryptocurrency exchange then converted to Kenyan currency. Each Worldcoin token was worth USD 2.1 or KES 299 which translated to a total of USD 54 or approximately KES 7,700 at the time.
  - 8) In order to sign up for World ID and receive free share of Worldcoin token, a person verifies their unique personhood using an Orb. The orb contains a variety of camera sensors and machine learning models that analyze facial and iris features. Once that determination is made, the orb takes a set of pictures of the person's irises and uses several machine learning models and other computer vision techniques to create an iris code, which is a numerical representation of the most important features of an individual iris pattern.
  - 9) Worldcoin continued to engage in data collection involving sensitive personal data in Kenya in total disregard of cessation directive issued by the ODPC on 30<sup>th</sup> May, 2023. The registration of Kenyans by Worldcoin online App is still going on despite the pendency of a court order and other administrative directions halting the same in entirety.
  - 10) Worldcoin did not disclose the cease order issued by the ODPC to their orb operators as disclosed by Sense Marketing hence, they continued with their operations without sensing any illegality.
  - 11) The promoters of *Worldcoin* misled consumers by using deceptive marketing strategies to induce people to exchange their personal data with tokens thus contravening their consumer rights in contravention of section 12 of the Consumer Protection Act, 2012.
  - 12) There is a possibility that minors were registered and scanned by the Worldcoin, since they did not have proper mechanisms for verifying the age of the data subjects.
  - 13) It is hard/impossible to establish the exact number of orbs in the country. The various witnesses stated with uncertainty that there were forty-eight (48) orbs in the country.
407. Arising from the second term of reference, on the legal and regulatory compliance of operations of Worldcoin and its agents in Kenya, the Committee made the following findings.

**THAT:**

- 1) The Committee found Tools for Humanity Corp and Tools for Humanity GmbH, Germany (Worldcoin) being culpable of violating Kenyan laws, including sections 19 and 48 of the Data Protection Act, 2019, section 12 of the Consumer Protection Act, 2012, the Computer Misuse and Cybercrimes Act, 2018 and Regulation 24 of the Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010. Their activities constituted acts of espionage and a threat to statehood.
- 2) Worldcoin, Tools for Humanity Corp (USA) and Tools for Humanity GmbH (Germany) do not appear in the Business Registration Services database of registered businesses or companies in Kenya and hence lack the legal mandate to transact any business in Kenya according to Part XXXVII of the Companies Act, 2015.
- 3) Despite collecting data on behalf of Worldcoin, Sense Marketing Ltd and other local partners were not registered as data processors and/or controllers as required by section 18 of the Data Protection Act.
- 4) Having noted the Orb is a telecommunication device with a capability to transmit real time iris images converted into digital code to their third-party servers hosted outside the country, the orbs did not undergo type approval by the CA contrary to the *Kenya Information and Communications (Importation, Type Approval and Distribution of Communications Equipment) Regulations, 2010*.

408. Arising from the third term of reference, on whether due diligence was undertaken by the relevant government agencies before Worldcoin started its operations in Kenya, the Committee made the following findings.

**THAT:**

- 1) The Cabinet Secretary for Information, Communication and the Digital Economy misled the country on the status of Worldcoin in Kenya. The Committee took note of the television interview with NTV on 2<sup>nd</sup> August, where the Cabinet Secretary stated that:
 

“As far as the Data Act 2019 is concerned, they (Worldcoin) are acting within the law. The ODPC got wind of this, wrote to the entity and they have had several meetings. We are going to approach this issue from a multifaceted approach, [...]”
- 2) The Committee noted that the foregoing statement was inconsistent with the submission dated 11<sup>th</sup> September, 2023 by the Cabinet Secretary for Information, Communication and the Digital Economy to the Committee. In the said submission, the Cabinet Secretary noted that while the Worldcoin started collecting data in public places in 31<sup>st</sup> May, 2021

and applied for registration as data controllers in Kenya on 22<sup>nd</sup> August, 2022, one year after commencing their activities in Kenya, contrary to section 18 of the Data Protection Act, 2019.

- 3) When tasked to respond to the contradictory statements, the Cabinet Secretary denied the said statements at the Plenary and during the proceedings of the Ad hoc Committee, claiming no knowledge of the statements alluded to, whereas it is in the public domain that the Cabinet Secretary made the said statements in an interview with a national television.
  - 4) The Committee noted that all concerned government entities only became aware of the Worldcoin activities way after they had commenced their operations in Kenya, following public uproar.
  - 5) Worldcoin declared the orbs as biometric scanners only but not as telecommunication devices as well. The Committee therefore, was unable to establish whether the Commissioner of Customs has mechanisms in place to physically inspect electronic gadgets imported into the country, and whether there are mechanisms to collaborate with other related government agencies like the Communications Authority of Kenya.
  - 6) KICC did not conduct due diligence on the nature of activity planned to be held at their facility including which product was being activated, but went ahead and offered authorization based on the fact that they had collaborated with the client (Exp Momentum) on numerous occasions in terms of bringing business to the facility.
  - 7) The ODPC received a Data Protection Impact Assessment (DPIA) from TFH Corp and TFH GmbH, prior to registering the two companies as data controllers, pursuant to the Data Protection Act, 2019 and the *Data (Protection Registration of Data Controllers and Data Processors) Regulation, 2021*.
409. Arising from the fourth term of reference, on the nature, use and safety of data collected by Worldcoin in Kenya, the Committee made the following findings.

**THAT:**

- 1) Despite the claim by Worldcoin that data collected was safely stored in Amazon Web Services based in South Africa, it was not clear whether the data stored could be retracted and deleted should need arise.
- 2) The transfer of personal data outside Kenya did not comply with the provisions of section 48 of the Data Protection Act.

- 3) It is unclear whether there are any security measures taken by *Worldcoin* to ensure the safety of data collected and whether there would be a possibility for forensic analysis on the same.

410. Arising from the fifth term of reference, on the organizational structure and the activities of Worldcoin, the Committee made the following findings.

**THAT:**

- 1) The Worldcoin project was co-founded in 2019 by Mr. Alex Blania and Mr. Sam Altman, a US tech entrepreneur and the CEO of OpenAI, the company that created ChatGPT. Piotr Piwowarczyk is the Regional Representative; Wangechi Mwangi, the East African Manager; and Rael Mwendu, the Marketing Specialist. Worldcoin partnered with other local representatives including Sense Marketing, Exp Momentum, Platinum D Plus and Hezron Gikonga.
- 2) Tools for Humanity Corp was founded in 2019 in Delaware, United States and headquartered in San Francisco, California, United States. Tools for Humanity GmbH, a limited liability company headquartered in Erlangen, Germany, is a subsidiary wholly-owned by Tools for Humanity Corporation.
- 3) The Worldcoin Foundation was founded in October 2022 to support and grow the community of Worldcoin protocol users and developers until the community becomes self-sufficient. The Foundation is an exempted limited guarantee foundation company incorporated in the Cayman Islands, and is independent of TFH.
- 4) The Worldcoin Foundation is not registered in Kenya as data processor or controller but is handling Kenyan data.
- 5) Worldcoin Foundation submitted that their aim is to realise more inclusive, fair, and just institutions of governance and of the global digital economy. The Committee found that whereas Worldcoin claim that their main intentions are proof of personhood and establishment of World ID, their real intention is inclined on decentralization of the global monetary system.
- 6) The Worldcoin Foundation is the sole member and sole director of World Assets Ltd., a business company incorporated in the British Virgin Islands. World Assets Ltd. is the entity responsible for issuing the 75% of all Worldcoin tokens (WLD) that have been allocated to the Worldcoin community.

411. Arising from the sixth term of reference, on the source of money or consideration if any paid to the members of the public who presented themselves for registration and the potential beneficiaries, the Committee made the following findings.

**THAT:**

- 1) The Committee was not able to establish the source of money or inducement given to those who complete the Orb verification process.
  - 2) There was no fiat currency compensation paid to Kenyans for completing the Orb verification process, rather, Worldcoin was issuing 25 WLD tokens. People could then choose to trade those WLD tokens in the open market through peer-to-peer exchange.
412. Arising from the seventh term of reference, on whether Kenyans were exposed to any health hazards as a result of the activities of Worldcoin in the Country, the Committee made the following findings.

**THAT:**

- 1) The committee received submissions from witnesses that they developed health complications including stress and stigma which the Committee recommended that they should seek further medical check-up from competent medical practitioners to ascertain the health complications.
  - 2) The Ministry of Health is yet to receive any reports of health hazards caused by the activities of Worldcoin in Kenya.
413. Arising from the eighth term of reference, on the legal and regulatory gaps that permitted operations of Worldcoin in Kenya, the Committee made the following findings.

**THAT:**

- 1) There is need for a stand-alone legislation to regulate new and emerging technologies, including virtual assets, digital platform services, social media services and over-the-top services.
- 2) The Data Protection Act, 2019 and the regulations thereunder do not sufficiently address key issues like the establishment documents to be presented to the Data Commissioner to ascertain eligibility for issuance of a certificate as a Data controller and/or processor as a juristic person.
- 3) The provisions of the Data Protection Act on registration of data controllers and data processors does not expressly require foreign entities to provide proof of registration as foreign companies under Part XXXVII of the Companies Act as a prerequisite for registration.

- 4) The Data Protection Act, 2019 lacks proper mechanisms for the enforcement of the rights of the data subjects and procedures for thorough vetting of local and foreign data controllers and/or processors.
- 5) There is a lack of a comprehensive legal framework to regulate emerging markets in virtual assets. This has exposed the country to inherent risks including speculative trading, high price volatility, possibility of criminal activities, tax evasions, financing terrorism, money laundering, data theft and financial fraud.
- 6) There is disharmony between the Data Protection Act and Part XXXVII of the Companies Act which seem not to expressly require foreign companies to provide proof of registration as foreign companies under Part XXXVII of the Companies Act as part of establishment documents.

414. Arising from the ninth term of reference, on the emerging issues, the Committee made the following findings.

**THAT:**

- 1) Kenya ranks first on the adoption and use of cryptocurrency globally for peer-to-peer trading volume. Bitcoin, Ethereum and Ripple are the most used cryptocurrencies in Kenya.
- 2) Despite the introduction of a digital asset tax through the Finance Act, 2023, payable on the transfer of digital assets, there is no mechanism for monitoring transfers of digital assets to ensure compliance.
- 3) Information Communication and Technology is an enabler of development across all sectors. For the realization of digital transformation in Kenya, collaboration and a multi-agency approach will enhance adoption of technology.
- 4) Blockchain is a distributed database or ledger shared among computers on a common network. Each computer/node participates in the validation of transactions and the maintenance of the blockchain ledger. The nodes are responsible for storing a copy of the blockchain ledger, verifying the authenticity of transactions, and adding new blocks to the chain. The blockchain maintains a secure and decentralized record of transactions, ensuring that data remains immutable (cannot be altered) upon entry.
- 5) Cryptocurrencies on the other hand, are privately issued digital assets that depend primarily on cryptography and blockchain/distributed ledger technology (DLT). Cryptocurrency could be described as a decentralized, distributed record or “ledger” of transactions in which the transactions are stored in a permanent and near inalterable way using cryptographic techniques.

- 6) Blockchain slashes the cost of transactions and eliminate intermediaries like lawyers and bankers, and thus lowering the cost of doing business. With the increase in more internet technologies, the adoption of blockchain will require broad coordination and will take time to be adopted. Blockchain is the medium through which crypto-currency is transacted.
- 7) In blockchain, the data is chronologically consistent because it cannot be deleted or modified without consensus from the network and as a result, one can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions.
- 8) Unlike the fiat currency, cryptocurrency is a digital, encrypted and decentralized medium of exchange and that there is no central authority that manages and determines the value of the digital currency. Instead, the determination of the value of the virtual currency is through speculative tendencies of the users of the cryptocurrency.
- 9) Cryptocurrencies pose security concerns due to their potential for anonymity, borderless transactions, difficulty in tracing decentralization, lack of third-party intermediaries, and limited regulation in Kenya.

#### **4.2 General Observations**

415. Arising from the overall inquiry, the Committee made the following general observations.

#### **THAT:**

- 1) Worldcoin submitted that they are a project founded with the mission of creating digital identification platform (World ID) that aims to provide each person on earth with a convenient way to verify that they are real human and alive and not a bot (internet robot) and use the attendant data to train AI algorithms for future technological advancements. Further, Worldcoin's objective was to decentralize the global monetary system.
- 2) Worldcoin operated in Kenya despite lack of regulation in cryptocurrency but did not operate in the USA which they claimed lacked regulatory clarity on cryptocurrency leaving an impression that they exploited the weak legal framework in Kenya while respected that of USA despite the fact that both countries did not have regulations on cryptocurrency.
- 3) The rapidly evolving technological advancement present a global challenge in managing risks associated with Artificial Intelligence (AI), blockchain and virtual assets, demands the need for a more progressive and responsive regulatory framework in Kenya.



- 4) The requirement for virtual asset holders and virtual service providers to adhere to regulations across multiple jurisdictions makes it difficult to carry out cross border transactions. Additionally, registration of business in different markets is tedious as different countries have different guidelines on licensing and registration.
- 5) The Computer Misuse and Cybercrimes Act, 2018 does not clearly set out scope and elements of the offences under the Act.
- 6) The Data Commissioner is neither a member nor co-opted member of National Computer and Cybercrimes Coordination Committee (NC4).
- 7) The unregulated adoption and use of cryptocurrency as an attempt to fully decentralize the global monetary systems, poses threat to statehood.
- 8) There are two cases pending in Court relating to the operations of world coin being *Milimani High Court Judicial Review HCJR/E119/2023 (R vs. Tools for Humanity Corporation and Tools for Humanity GmbH and 7 Others ex parte Katiba Institute and Law Society of Kenya and 3 Others)* and in *Milimani High Court Criminal Miscellaneous Application No. E315 of 2023 (Office of the Data Protection Commissioner vs. Tools for Humanity Corporation and 2 Others)*.
- 9) The Ministry of Interior and National Administration through the Directorate of Criminal Investigations, the Communication Authority of Kenya, Ministry of Information, Communication and the Digital Economy, the Office of the Data Protection Commissioner, and the National Computer and Cybercrimes Coordination Committee are currently conducting investigations on the activities of the Worldcoin in Kenya.
- 10) The Committee was unable to reach Exp Momentum, a South African company through their last known address for invitation as a witness to the proceedings.
- 11) There is a general lack of awareness among Kenyans on the provisions of the Data Protection Act, 2019 pertaining to the rights of data subjects.
- 12) The Committee was unable to establish whether the data subjects were actually given the monetary consideration promised.

## CHAPTER FIVE

### 5.0 RECOMMENDATIONS OF THE COMMITTEE

416. Based on the Committee's findings and general observations, the Committee makes the following recommendations: -

**THAT:**

- 1) The Cabinet Secretary for Ministry of Information Communication and the Digital Economy through the ICT Authority in consultation with relevant stakeholders to develop a comprehensive oversight framework and policies on virtual assets and virtual assets service providers in Kenya, within six (6) months of the adoption of this report and submit the same to the National Assembly to take appropriate legislative measures.
- 2) Within six (6) months of the adoption of this Report, the Cabinet Secretary for the National Treasury in consultation with the relevant stakeholders to develop regulations and enforcement infrastructure to ensure that virtual assets and virtual assets providers and their activities are adequately regulated and monitored.
- 3) The Director of Criminal Investigations and the Director of Public Prosecutions within three (3) months from the date of adoption of this report, to conduct investigations into the operations of M/s Tools for Humanity Corp and M/s Tools for Humanity GmbH, Germany (Worldcoin) in Kenya and take the requisite legal action.
- 4) The Director of Criminal Investigations and the Director of Public Prosecutions within three (3) months of adoption of this Report to investigate into the activities of the local partners of M/s Tools for Humanity Corp and M/s Tools for Humanity GmbH, Germany (Worldcoin) in Kenya to establish culpability of persons including Sense Marketing Limited, involved in aiding and abetting their criminal activities and take necessary legal action.
- 5) Within seven (7) days of the adoption of this report, the Communications Authority to disable the virtual platforms of M/s Tools for Humanity Corp and M/s Tools for Humanity GmbH, Germany (Worldcoin), including blacklisting the IP addresses of related websites and to suspend their physical presence in Kenya until there is a legal framework for regulation of virtual assets and virtual asset service providers.
- 6) Parliament reviews the current legal framework, to; amongst other provisions -

- a) **Harmonize the Data Protection Act with Part XXXVII of the Companies Act to expressly require foreign companies to provide proof of registration as foreign companies under Part XXXVII of the Companies Act and to require foreign entities to provide proof of registration with local regulatory bodies before registration as data processors and/or controllers.**
  - b) **Provide for the requirement for full disclosure on how data controllers and processors will utilize and store personal and sensitive data collected in Kenya.**
  - c) **Provide discretion to the Office of the Data Protection Commissioner in imposition of administrative fines, by amending section 63 of the Data Protection Act, to align to global standards so as to ensure that entities take matters of data protection seriously.**
  - d) **Amend the Data Protection Act, 2019 to provide for a board where the Office of the Data Protection Commissioner reports or account to on its daily operations.**
  - e) **Provide clear tax remittance procedures on taxes imposed on transactions involving virtual assets under section 12F of the Income Tax Act.**
  - f) **Include Virtual Asset Service Providers as Reporting Institutions under the Proceeds of Crime and Anti-Money Laundering Act, 2009.**
  - g) **Review the Computer Misuse and Cybercrimes Act 2018 to fully deal with the current realities in the cyberspace including stationing multi-agency technical personnel at all border entry points to provide technical expertise on all technological equipment imported into the country.**
  - h) **Expand the scope of offences and develop the elements of offences under Part III of the Computer Misuse and Cybercrimes Act, 2018, and develop regulations under section 70 of the Act.**
  - i) **Review the Computer Misuse and Cybercrimes Act 2018 to co-opt the Data Commissioner or a representative of the Office of the Data Protection Commissioner as a member of the National Computer and Cybercrimes Coordination Committee.**
  - j) **Provide legislative intervention(s) to govern the collection of biodata from Kenyans which has implications on privacy, security, health concerns and human rights.**
- 7) **Within three (3) months of the adoption of this Report, the Data Protection Commissioner to report to the National Assembly on the measures it has taken to bring the provisions of the Data Protection Act, 2019 to the knowledge of the general public as required by section 8(g) of the Data Protection Act, 2019.**

- 8) Within six (6) months of the adoption of this Report, the Communication Authority of Kenya to develop a regulatory sandbox in collaboration with relevant authorities to regulate new data-based projects that rely on new and emerging technologies.
- 9) Within one (1) month of the adoption of this Report, the Cabinet Secretary for the Ministry of Interior and National Administration through the Director of Criminal Investigations, provides a report to the National Assembly on the status of their ongoing investigations into the activities of M/s Tools for Humanity Corp and M/s Tools for Humanity GmbH, Germany (Worldcoin) in Kenya and their findings, and thereafter report after every two (2) weeks until conclusion and necessary remedial actions are taken.
- 10) Within six (6) months of the adoption of this Report, the Data Protection Commissioner carries out an audit of all registered data processors and controllers as required by section 23 of the Data Protection Act, 2019 and submit a Report to the National Assembly.
- 11) The Managing Director for Kenyatta International Convention Centre (KICC) puts in proper measures to strengthen vetting procedures on clients of KICC before allowing them to use its premises.

SIGNED .....



DATE.....27.09.2023.....

HON. GABRIEL TONGOYO, MP

CHAIRPERSON, AD HOC COMMITTEE ON THE INQUIRY INTO THE ACTIVITIES  
OF WORLD COIN IN KENYA