OFFICE OF THE DATA PROTECTION COMMISSIONER

STRATEGIC PLAN FY 2021-2023

Promoting personal data protection by design

October, 2021

FOREWORD

The government takes note that many organisations, both public and private, hold information about citizens. This can be as simple as citizen's contact details or may be more detailed information, such as their online browsing history. This creates concerns about user privacy, or about the accuracy and the further use of the information by the collecting organisation and any other organisation it decides to share that information with. The Data Protection Act provides for the protection of any personal data regardless of whether the data is considered sensitive or not. Some provisions apply to the collection, storage, and processing of such data as well as the transfer of personal data to another country.

The Office of Data Protection Commissioner has made wonderful steps towards safeguarding personal data and information. The government continues to support the office since it recognizes the importance of safeguarding data privacy and need for guaranteed maximum support.

My ministry recognizes the importance of the Office of the Data Protection Commissioner and will continue to walk the journey with the Data Commissioner to implement this 3-year strategic plan to the full. This strategic plan is an embodiment of the commitment of the government to ensuring that the regulatory environment for personal data in Kenya is conducive and enabling in the digital era as envisioned in the Kenya Vision 2030 and Third Medium Term Plan 2018–2022.

The plan's vision of enhancing trust and building transparency of data protection in Kenya has been aligned to the Data Protection Act, the data protection guidelines, the government policy guidelines, and incorporated the Big Four Agenda. In implementing this strategy, it is expected there will be consideration in the way Covid-19 has accelerated the embrace of digital solutions. This presents opportunities and challenges in data collection, storage, and hence data protection. However, the right decisions must be made. We will continue to work with all stakeholders, both international and local, to ensure the priorities set out in this strategic plan are achieved and targeted outcomes realised.

Joseph Mucheru, EGH,
Cabinet Secretary,
Ministry of ICT, Innovation and Youth Affairs

PREFACE

Organizations will need to continuously improve data protection. The Data Protection Act 2019 provides a framework to place Kenya on the global and regional map as the Silicon Savannah. We have an opportunity to take back control of our data privacy. The time has come to ask; why do you need the personal information and what will it be used for? It is with this premise that we are happy to launch this first strategic plan for the Office of Data Protection Commissioner (ODPC).

The ODPC's data protection responsibilities will therefore go beyond traditional IT, legal, and security roles to provide a holistic view on data privacy, security, education and even opportunity across the organization. In our journey to safeguard personal data, we have already launched: the draft guidelines on obtaining consent from data subjects; draft manual on complaints; draft citizen service charter; draft guidelines on conducting data impact assessment; brand identity; and, an operational interactive website and social media platforms in place. This was in preparation for this strategic plan which has been developed in line with government guidelines as well as objectives of data protection.

The objectives of the data protection office include; overseeing the implementation of and being responsible for the enforcement of the Data Protection Act, establishing and registering data controllers and data processors; promoting self-regulation, exercising oversight on data processing, promoting international cooperation in matters relating to data protection among other mandates listed in the act. To realize these objectives, the strategic plan has prioritized issues of institutional capacity development, regulation and compliance services, and awareness creation on the importance of protecting personal data. These have been operationalized through developing strategic objectives, strategies and activities as set out in the strategy implementation matrix.

The strategic plan has been developed through an elaborate and consultative process involving internal and external stakeholders. Implementing this plan successfully will depend on the continued strategic policy guidance of the Cabinet Secretary, the commitment of staff, and support from all stakeholders. The plan has also been designed to take note of ongoing technological and societal changes. We commit to continuously and actively engage with our stakeholders to ensure we walk together on this transformative journey and ensure set objectives are realized.

I urge for support from all stakeholders to achieve our mission of protecting personal data in Kenya through compliance, enforcement, public awareness, and institutional capacity development.

Immaculate Kassait, MBS
Data Protection Commissioner,
Office of the Data Protection Commissioner

DEFINITION OF TERMS

Biometric data: This refers to any personal data resulting from specific technical processing based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, earlobe geometry, retinal scanning, and voice recognition.

Data controller: This refers to a natural or legal person, public authority, agency, or other body which alone, or jointly with others, determines the purpose and means of processing of personal data.

Data processor: This refers to a natural or legal person, public authority, agency, or other body which alone or jointly with others processes personal data on behalf of the data controller.

Data subject: This refers to an identified or identifiable natural person who is the subject of personal data.

Evaluation: This refers to a systematic and objective assessment of an ongoing or completed project. The aim is to determine the relevance and level of achievement of project objectives, development effectiveness, efficiency, impact and sustainability. Evaluations also feed lessons learned into the decision-making process.

Health data: This refers to data related to the state of physical or mental health of the data subject, and includes records regarding the past, present, or future state of the health, data collected in the course of registration for, or provision of, health services, or data which associates the data subject to the provision of specific health services.

Monitoring: This refers to the continuous assessment that aims at providing all stakeholders with early detailed information on the progress or delay of the ongoing assessed activities. It is an oversight of the activity's implementation stage.

Personal data: This refers to any information relating to an identified or identifiable natural person. Under the Kenya Information and Communications Act, 'personal information' includes a person's full name, identity card number, date of birth, gender, physical and postal address.

Pseudonymisation: This is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language, birth, personal preferences, interests, behaviour, location, or movements.

Sensitive personal data: This refers to sensitive personal data revealing a person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of a person's children, parents, spouse or spouses, sex, or sexual orientation.

The Act. This refers to the Data Protection Act,2019

CONTENTS

List of Tables

List of Figures

ABBREVIATIONS & ACRONYMS

AI	Artificial Intelligence
CAK	Communications Authority of Kenya
CCK	Communication Commission of Kenya
DPC	Data Protection Commissioner
DPO	Data Protection Officer
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
FCDO	Foreign Commonwealth Development Office
FY	Financial Year
GDPR	General Data Protection Regulations
GoK	Government of Kenya
ICT	Information Communication Technology
IoT	Internet of Things
IP	Intellectual Property
MCDA	Ministries, Counties, Departments and Agencies
MDA	Ministries Departments and Agencies
MERL	Monitoring, Evaluation Reporting and Learning
MTP	Medium Term Plan
NACOSTI	National Commission for Science, Technology and Innovation
PESTEL	Political, Economic, Social, Technology Environment and Legal
SAGA	Semi-Autonomous Government Agency
SDG	Sustainable Development Goals
SME	Small and Medium Enterprise
SoP	Standard Operating Procedures
UK	United Kingdom
SWOT	Strengths, Weakness, Opportunities and Threats

EXECUTIVE SUMMARY

The Office of the Data Protection Commissioner (ODPC) is established under the Data Protection Act, 2019 (The Act) which was assented to by President Uhuru Kenyatta on 8th November 2019. Consequently, assent to the bill gave way for the appointment of the first Data Protection Commissioner of the Republic of Kenya.

The purpose of the ODPC is to regulate the processing of personal data; ensure that the processing of personal data of a data subject is guided by the principles set out in Section 25 of The Act; protect the privacy of individuals; establish the legal and institutional mechanisms to protect personal data, and provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act. This is the inaugural strategic plan for the ODPC covering the years 2021-2024.

Aligned with Kenya Vision 2030, the Third Medium Term Plan (2018 – 2022) and the "Big Four" Agenda, this strategic plan has been developed at a time when many countries are implementing or planning to implement data protection laws largely desire to ensure collection and processing of data of subjects to be in accordance with the data protection law. The Constitution of Kenya guarantees the right to privacy as a fundamental right. To give effect to this constitutional right under Article 31(c) and (d), the Data Protection Act, 2019 provides for the regulation of the processing of personal data, including the rights of data subjects and obligations of data controllers.

This strategic plan recognises the unique role of the ODPC in safeguarding the right of citizens to the protection of their personal data and privacy, particularly in this era of ubiquitous computing. The plan shall guide the ODPC in achieving its mandate and to provide the focus for the next three years in light of the emerging global, regional, national and county trends in data protection and privacy. It also acts as a guide for assessing performance and achievements of results during this period, and also serve as a communication tool with international and national stakeholders on the strategic priorities. Finally, the plan shall be used to mobilize stakeholder support (financial and non-financial) to accelerate the operationalisation of the ODPC.

The ODPC in the spirit of enhancing trust and building transparency of data protection in Kenya has laid out strategies that focus on the best interests of all, or an organisation's stakeholders while considering all aspects of the organisation – from the vision and mission, to working relationships between staff and management, to the roles of various players (especially the role of project sponsors), to the organisation's structure and culture. The three focus areas of excellence are:

i) Institutional capacity development, which aims to build the capacity of the data protection institution and partnership to enhance data processing operations
ii) Regulatory services, which aims to establish a policy framework to safeguard private data
iii) Awareness creation, which aims to equip stakeholders with adequate capacity on data protection to promote self-regulation

Consequently, to achieve these areas of excellence, this plan provides for mechanisms for strengthening collaboration with government agencies, the media, data controllers and processors, data subjects, civil society and religious organisations, development partners and global and regional networks. The success of this plan and its implementation will call for concerted collaboration amongst all data stakeholders.

In cognizance of the sensitivity of data matters, and in addition to the outlined structures to be established, this strategic plan also provides for its operationalization. It also calls for strategic issues that need to be resolved or addressed to achieve the expected impact and proposed strategic direction in service delivery.

As aforementioned, this strategic plan focuses on three key result areas, and to deliver on these areas, this strategic plan has outlined strategic objectives, strategies, and targets to address emerging data protection priorities. It spells out the human and financial resources required. The estimated budget required for the implementation of the planned targets is KES 3,612,000,000.

The strategic plan has provided for an implementation and coordination framework as well as a framework for monitoring, evaluation and reporting to be done at various levels including a mid-term review and end of plan evaluation. The resultant reports and feedback from the process will assist in formulating corrective measures, realignment of priority areas and resources.

1 INTRODUCTION

1.1 Overview

The growth of the digital economy and technological advances, which largely depend on data, requires reciprocal legislation on data protection. Further, the changing domestic and global data protection ecosystem, calls for a collaborative effort to respond to public concerns and legislative imperatives in relation to data privacy, use of data and the digital skills agenda. Likewise, regimes will need to stay focused on the other aspects of regulatory, accessibility and availability of data for the common good of the society. Cognizant of this need, the Government of Kenya, through the Data Protection Act, 2019, which is an Act of Parliament, has responded by creating the Office of the Data Protection Commissioner. This document gives the strategic priorities of the ODPC for the next 3 (three) years. Further, it also indicates how the ODPC will implement and monitor the outcomes of the strategic priorities.

1.2 Background

The Constitution of Kenya ('the Constitution') guarantees the right to privacy as a fundamental right. To give effect to this constitutional right under Article 31(c) and (d), the Data Protection Act, 2019 was enacted and came into effect on 25 November 2019. The Act provides for the regulation of the processing of personal data, including the rights of data subjects and obligations of data controllers[1].

The Office of the Data Protection Commissioner was established with the enactment of the Data Protection Act and it is domiciled in the Ministry of ICT, Innovation and Youth Affairs. The Act provides that this office shall act independently in carrying out its powers. The office is expected to coordinate bodies and entities involved in data management in this country for the benefit of the Kenyan people. To achieve this, the office is expected to work collaboratively with both government, private, multinationals, civil society, and the general public to achieve its mandate.

The ODPC Strategic Plan FY 2021/2022 - FY2023/2024 recognises the unique role of the ODPC in safeguarding the right of citizens to the protection of their personal data and privacy, particularly in an era of pervasive computing. The plan is envisioned to serve as a tool of guidance to ODPC in achieving its mandate and to provide the focus for the next three years in light of the emerging global, regional, national, and county trends in data protection and privacy. The plans will also act as a guide for assessing performance and

[1] [1]Kenya Gazette Supplement Acts (2019). Kenya Gazette Supplement No. 181 (Acts No. 24).

achievements of results during this period, and also serve as a basis of engagement with international and national stakeholders on the strategic priorities. Finally, the plan shall be used to mobilize stakeholder support (financial and non-financial) to accelerate the operationalisation of the ODPC.

1.3 The mandate of the Office of the Data Protection Commissioner

The mandate of ODPC is derived from the Data Protection Act 2019 and includes, inter alia:

a) Regulate the processing of personal data;
b) Ensure that the processing of personal data of a data subject is guided by the principles set out in Section 25 of the Act;
c) Protect the privacy of individuals;
d) Establish the legal and institutional mechanism to protect personal data; and
e) Provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

1.4 Global, Regional and National Development Challenges

The desire to have data protection laws can be traced back to the 1970s. The concerns then were the emergence of computers and other communication technologies that had the capabilities to process large volumes of data remotely. Since then, several initiatives at international, regional, and national levels have been pursued albeit with different regulatory frameworks.

Many countries that are implementing or planning to implement data protection laws largely desire to ensure collection and processing of data of subjects to be in accordance with the data protection law. However, several challenges in the development and implementation of data protection laws exist. These challenges vary from country to country and they include; addressing gaps in coverage; addressing new technologies; managing cross-border data transfers; balancing surveillance and data protection; strengthening enforcement; institutional capacities; determining jurisdiction and managing the compliance burden[2]. Other challenges include creating a culture of trust online to ensure that the opportunities emerging in the information economy can be fully leveraged.

Globally, the regulatory environment on the protection of data is far from ideal. This is compounded by the fact that some countries do not have any legislation on data protection. In other places, the various pieces of legislation are incompatible with each other and hence create a loophole on how to enforce them. With the

[2] https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

emergence of new technologies and increased reliance on technologies like cloud-computing solutions, questions arise about what jurisdictions apply in specific cases. Such lack of clarity creates ambiguity for individuals, consumers, and businesses, restricts the scope for cross-border data exchange, and strangles economic growth. Moreover, as the global economy shifts into blue economies that are data-dependent and further into a connected information space, the relevance of data protection and the need for controlling data privacy will further increase. Therefore, a clear understanding of different approaches to and ways for establishing compatible legal frameworks at national, regional, and multilateral levels is important for facilitating international trade and online commerce. Further, the adoption of a core set of principles that seem to apply to a majority of national data protection laws and in regional and global initiatives could help establish compatible legislations with some room for flexibility in domestic implementation. For Kenya to attain some of the goals set out in the Third Medium Term Plan (2018– 2022) and the 28 sector plans[3], data protection will be key.

According to UNCTAD, national data protection laws should avoid obstacles to trade and innovation[4]. This may involve avoiding or removing data localization requirements that go beyond the basic options for the management of cross-border data transfers. A balance on flexibility and compatibility of the data regulation to different contexts and territories is therefore critical. Equally, the data protection legislation must strive to allow for innovations and to facilitate data sharing among different countries. There is therefore an urgent need to harmonize these regulatory frameworks to have coherence on the fundamentals of the data protection laws.

In the development of policies and strategies to ensure mutual benefit to both the subject and the data processor, the following common principles will be worthy of consideration: need to have a legitimate reason for any processing activity, obtained either through consent or some other justification designed to acknowledge competing private and public interests; the obligations concerning the quality (accurate, complete and kept up-to-date) of the personal data being processed; the data security (physical, logical or organizational) measures to protect against deliberate acts of misuse as well as the accidental loss or destruction of data.

In some countries, data protection laws apply equally to all those processing personal data. Other countries have different rules for specified sectors (e.g., health), types of processing entity (e.g., public authorities), or

[3] https://www.treasury.go.ke/wp-content/uploads/2020/11/KEY-HIGHLIGHTS-OF-MTP-III-PRIORITIES.pdf
[4] https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

categories of data (e.g., data about children). In such jurisdictions, some sectors are not subject to regulatory controls at all.

Evidence on the current developments on data protection can be cited on the European Union's General Data Protection Regulation (GDPR), United Kingdom's Data Protection Act of 2018[5], Ireland's Data Protection Act of 2018[6] , and South Africa's Protection of Personal Information Act 2013 (POPIA)[7] among others. The common themes of the laws implemented by these countries include: defined offices charged with the mandate of coordinating and implementing the data protection act and general adherence to the data protection principles; the defined scope on the admissibility of the act; clear fines in case of breach of the sections of the act; data subjects rights; obligations for controllers and processors; privacy policy requirements, access to personal data; special categories of data among others.

Most of the countries that have established data protection offices have also developed strategic plans to guide their implementation. For instance, UK has developed a strategic plan "Information Rights Strategic Plan 2019-2022". The focus of this strategic plan is: ensuring that access to information rights is upheld in a consistent and timely manner and operates effectively in a digital age; providing excellent customer service to individuals making requests and leading by example in fulfilling its statutory functions; raising awareness of access to information rights and making it easier for the public to exercise their rights; promoting the reform of access to information legislation so it remains relevant for the modern society and fit for purpose; and further developing and sustaining international collaboration and learning from the best initiatives around the world[8].

Ireland has also developed a draft strategic plan for the implementation of the data protection laws. The draft strategic plan identifies the following strategic goals: regulate consistently and effectively; safeguard individuals and promote data protection awareness; prioritise the protection of children and other vulnerable groups; bring clarity to stakeholders; support organisations and drive compliance[9].

In responding to similar challenges in Kenya, the Date Protection Act (2019) established the Office of the Data Protection Commissioner with a clear mandate as outlined in Section 1.3.

[5] https://www.gov.uk/data-protection
[6] https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html#lf18e4
[7] https://www.dataguidance.com/notes/south-africa-data-protection-overview
[8] Information Commissioner's Office (2019). "Information Rights Strategic Plan 2019-2022"
[9] Data Protection Commission (2021). Regulatory Strategy Consultation

1.5 ODPC's Development Role

Data protection is growing in importance as governments adopt digitisation of services and increasingly require the citizens to have an online presence to access them. As more businesses and citizens are moving to the cloud - often using unmanaged personal devices - the main focus is thus to improve information protection and advance privacy and compliance.

Through the establishment of a robust regulatory framework, the ODPC will ensure the public, private and civil society entities meet the data privacy requirements as contemplated in The Act. The ODPC shall therefore encourage self-regulation by all entities involved in data processing. At the same time, enforcement mechanisms shall be instituted to ensure compliance. In addition, ODPC shall endeavour to equip stakeholders with information and knowledge on data protection to promote compliance. This shall be done through training, public outreach and messaging to promote continuous improvement in incorporating privacy safeguards and best practices into every operation. Similarly, ODPC shall build its internal capacity to advance data protection. The focus shall be on building human capacities, strengthening operational processes and deploying a robust infrastructure for effective service delivery.

Kenya recognises the centrality of data in the growth of the digital economy. This can only be realised if data privacy is guaranteed and data subjects can adopt technological advancements. In Kenya's Vision 2030, the Third Medium Term Plan (2018 – 2022) and the "Big Four" Agenda. ICT, and by extension data, has been recognised as a key driver to promote socio-economic growth and productivity in other sectors. Therefore, ODPC will play a critical role in the attainment of the national development objectives. For instance, in the manufacturing agenda, ODPC will ensure that companies comply with the Act by protecting the data of employees, enhance an open data policy to promote healthy market competition and ensuring ethical use of technologies like machine learning, artificial intelligence, Internet of Things (IoT) and robotics. Within the housing agenda, ODPC shall ensure that personal data collected from private rental and retail platforms, as well as government initiatives such as "Boma Yangu", shall comply with the data protection regulations. In agriculture, ODPC shall ensure ethical compliance in initiatives employing smart farming and big data technologies (e.g., Digifarm[10]) that promise to help farmers increase yields, access markets and acquire inputs. ODPC shall support the Universal Health Coverage agenda by ensuring the data-intensive health sector is

[10] https://mercycorpsagrifin.org/wp-content/uploads/2019/05/DigiFarm-Platform-Case_Final_.pdf

compliant and health care providers benefit greatly by ethically sharing the patient data collected in various health information management systems, including the National Hospital Insurance Fund (NHIF).

2 SITUATION ANALYSIS

2.1 Overview

This chapter highlights the context in which ODPC operates in the path of achieving its mandate. The ODPC has been existence for only eleven (11) months and therefore conducting a comprehensive environmental analysis may be premature. However, there are strengths to leverage in formulating and implementing the ODPC Strategic Plan FY 2021/2022-2023/2024. These include a clear mandate and a substantive Data Commissioner among others. Nonetheless, the ODPC is yet to be fully constituted, has inadequate human resource capacity and lacks guiding regulations among other challenges. There are several opportunities to be exploited by the commission. They include the government's digitization process, government plans and policies, Vision 2030, MTP III through the Big Four Agenda; high levels of internet penetration in the country; expanded ICT infrastructure to mention a few. Cyber security of data and services as well as reputational and mandate risks are external threats that the ODPC also needs to guard against among other risks as detailed in section 4.4.

The chapter also outlines the achievements realised since the inauguration of the ODPC, key stakeholders' analysis and their level of influence in the formulation and implementation of the strategic plan. It also covers the strategic issues that formed the basis for the formulation of the strategic key result areas, strategic objectives and strategies in the ODPC's strategic plan for FY 2021/2022 - FY2023/2024.

2.2 Key Achievements

In the short span of its existence, the ODPC has been able to realise notable achievements towards the realisation of its mandate by working with key stakeholders. These achievements include:

1. Facilitated Roll out of Huduma Namba
    a. The establishment and Operationalization of the Office to provide guidelines in the roll out of Huduma Namba in Compliance of Court Ruling on continuation of implementation of Huduma Namba programme
    b. Issued advisory on Data Protection Impact Assessment for Phase II roll-out of the Huduma Namba
2. Draft Regulations
    a. 3 sets of draft regulations are in place:

b. Pre-publication engagement held with the committee on delegated legislation of the National Assembly

3. Human Resource
    a. 8 staff deployed from MIIYA and the National Treasury
    b. Organization structure & staff establishment approved by Public Service Commission
    c. Human Resource manual and career guidelines policies in place
    d. Job descriptions developed leading to approval of Grading and Salary Structure by Salaries and Remuneration Commission
4. Workstation set up (Functional office)
    a. Currently hosted at the headquarters of the Communication Authority of Kenya (CA)
    b. Future Office Space identified and Lease Agreement signed for office space at Britam Towers
    c. Estimation of partitioning works ongoing
    d. Interactive Website and Branding logo developed and operational
5. Guidance Notes developed on:
    a. conducting data protection impact assessments
    b. seeking consent from data subjects
    c. processing personal data for electoral purposes
6. Training Curriculum developed including:
    a. developed draft data protection curriculum – awaiting stakeholders' validation and approval by Kenya School of Government (KSG) council
    b. commissioned a training needs assessment
7. Policies, SOP's and manuals developed including:
    a. draft service charter
    b. framework for periodic audits
    c. draft ICT strategy and policy
    d. code of conduct and ethics approved by the Ethics and Anti-Corruption Commission (EACC)
8. 16 virtual and physical awareness creation and consultation forums with various stakeholders drawn from the public, private sector and development partners
9. Established a framework for handling complaints (including a Draft Complaints Manual). Currently slightly over 300 active cases of data breaches and complaints are being handled
10. Issued 9 advisories and guidance notes to data controllers and processors both in the private and public sector

11. Established international cooperation partnerships with FCDO, Commonwealth Common Thread Network and African Network of Data Protection Authorities

2.3 Environmental Analysis

A strategic situational scan was carried out to understand the operational environment for the ODPC. Considering the newness of the institution, conducting SWOT analysis was considered premature and may be based on assumptions rather than facts/evidence. Nonetheless, an assessment of the environment was conducted using **Critical Success Factor Analysis (CSFA)** techniques[11]. The outcomes of the CSFA were used in the identification of the priority key result areas, the strategic focus areas, strategic objectives and strategies.

In addition, the situational scan aimed at taking stock of the institution's functional resources, capacity and opportunities. The design and success of a new strategy for the organization depends on the strategic fit between the internal and the external conditions. A summary of the Critical Success Factor Analysis is presented in Table 1.

Table 1: Summary of the Critical Success Factor Analysis

Issues	Impact on the Strategic Direction
Existence of a legal framework on the establishment of the ODPC with a clear mandate	Strategic environment for implementation of the legal provisions of The Act at both levels of government
Clear Data Protection Regulations	Enhanced enforcement and compliance of The Act
Adequate budgetary allocation by the National Treasury, support from other government departments, agencies, county governments and development partners	Effective delivery of public projects and programs on data protection
Human resource capacity	Capacity to respond to data protection processes
Dynamic and agile administrative structure	Capacity to adopt to highly dynamic data protection environment
National government investments in the infrastructure and systems to keep pace with the dynamics of the 4th Industrial Revolution	Enabling a digital ecosystem that promotes data protection
Strong goodwill and positive reception of the ODPC by all stakeholders	Attracts partnerships and establish collaboration & networks
Government digitization programs	Leverage on the digitization program to entrench data protection

[11] **Critical success factor analysis** is a technique to identify the areas in which a business must succeed in order to achieve its objectives

Issues	Impact on the Strategic Direction
Standard operating procedures	Effective service delivery through quality Standard Operating Procedures (SOPs)
Cooperation with other countries and multinationals on data protection	Leveraging experiences on data protection.
Digital skills for professional and individuals on data protection	Enhanced capability and capacity to handle data protection tasks
Complacency, level of understanding, and familiarity with data protection processes and usage	Enforcement mechanisms for self-regulation
Disseminating information and knowledge on the provisions of the Data Protection Act	Enhanced understanding and levels of awareness on the data protection
Data protection skills, trust, positive attitude, and culture	Ability to protect data, share data to authorized controllers/processors and sense of data protection
Fourth Industrial Revolution (4IR) and associated rapid technological changes leading to a high rate of technological redundancy	Increased reliance on the 4IR and assimilation into the digital economy and establishment of a framework for adopting new and emerging technologies
Policies and procedures for setting-up register of data controllers and data processors	Accessible and well-regulated register of data controllers and data processors
Personal data is scattered across multiple applications, devices, locations and storage	Data aggregation and centralization framework
Data protection infrastructures and systems to coordinate data controllers, data processors, and data subjects	Coordinated monitoring of data controllers, data processors and data subjects
Big data storage and management that clash with the principles of data minimisation	Data centre positioning in the country
Alignment and compliance with data privacy laws of different countries and compliance to International & Regional conventions	Established collaboration framework on the international and national conventions
Enforcement of the rights and obligations of the public on data protection	Well informed citizenry on data protection
Data capture forms/documents disposal legal framework	Data archiving and protection for future references
The reluctance of data Superpowers (e.g., Facebook) to adhere to data protection regulations	Establish adherence mechanisms and references/arbitration mechanism
Lack of unified data regulations leading to difficulty in enforcing the data protection Act	Harmonize existing and subsidiary policies to create a uniform approach to the data-centric landscape in line with data protection requirements

Issues	Impact on the Strategic Direction
Increased cyber hygiene breaches may cause personal data loss and business disruptions	Strengthening and entrenching the cyber hygiene programmes
Working with the devolved levels of Government	Faster delivery of services and enhanced data protection inclusivity
Integrated technological infrastructure and data management systems	Enhanced interoperability and data sharing for effective data protection

2.4 Stakeholders Analysis (Interests and Influence)

Stakeholders are the entities who will be significantly impacted by the data protection act and its regulations. There is a need to understand the degree to which these stakeholders will be affected and highlight any difference in the extent of the impact of the regulations. In addition, ODPC would meet its mandate by knowing the expectations of stakeholders concerning the Data Protection Act. In line with this, stakeholders would be best served when they are aware of ODPC's expectations of them.

The stakeholder analysis considered the category, their expectations of ODPC, ODPC's expectation of them, their degrees of influence and interest. Influence refers to the ability to convince other people in your sector to implement your ideas[12], in this case how the stakeholder's personal data protection practices can influence ODPC strategy in enforcing data protection regulations. Interest refers to an organisation's technologies, processes and systems which are considered by ODPC to be of mutual benefit[13], in this case it refers to the extent of benefit of the stakeholder to ODPC's work. For instance, the ODPC will be immensely interested in the role of the Ministry of Interior and Coordination of National Government in processing and sharing personal data of subjects through the National Integrated Identity Management System (NIIMS), commonly known as "Huduma Namba"[14]. The use of the Huduma Namba will be influential in setting trends for use of personal data. The information on stakeholder analysis will assist in formulating ODPC's strategic action in transacting with the stakeholders. A summary of the stakeholder analysis is presented in Table 2.

[12] https://yourbusiness.azcentral.com/strategic-influence-12406.html
[13] https://www.lawinsider.com/dictionary/strategic-interest
[14] https://www.hudumanamba.go.ke/

Table 2 Summary of results of Stakeholder analysis

Name of stakeholder	Stakeholder's Expectation of ODPC	ODPC's expectation of the stakeholder
Ministry of ICT, Innovation and Youth Affairs, (MoIIYA)	+ Implementation of policy, legal and regulatory frameworks, periodic reports	+ Policy direction
National Treasury	+ Exercise prudent financial management + Timely submission of budgets and reports + Create and operationalize a reserve fund	+ Budget Provision
Parliament	+ Status reports + Response to parliamentary questions	+ Approval of budget allocation + Oversight + Legislation
Judiciary	+ Determination of disputes within the set frameworks	+ Appreciate personal data protection + Adjudicate disputes and interpret the law on personal data protection
Directorate of Public Prosecution	+ Appraise about The Act + Timely sharing of information	+ Collaboration during enforcement
Ministries Departments, Counties and Agencies (MDCAs)	+ Clear guidelines on data protection	+ Adherence to regulations + Collaboration + Compliance with the Act
Media	+ Timely and accurate information	+ Disseminate accurate information + Compliance with the Act
Data Controller and Data Processors	+ Timely provision of services and feedback	+ Compliance with the Act
Data subjects	+ Provision of institutional mechanism to resolve complaints + Awareness creation + Protect data privacy rights	+ Timely filing of complaints in prescribed format + Awareness of data privacy rights
Civil Society and religious organizations	+ Information sharing + Protection of the vulnerable groups	+ Collaboration on awareness creation + Compliance with the Act
Development partners	+ Information sharing	+ Collaboration

Name of stakeholder	Stakeholder's Expectation of ODPC	ODPC's expectation of the stakeholder
	+ Accountability of resources	+ Financial support + Compliance with the Act
Global and Regional networks	+ Information sharing + Benchmarking	+ Information and experience sharing + Benchmarking

2.5 Strategic Issues

ODPC has identified the following strategic issues that need to be resolved or addressed to achieve the expected impact and proposed strategic direction in service delivery. The strategic issues and strategic direction are presented in Table 3.

Table 3 Strategic Issues and strategic direction

Strategic Issue	Strategic Direction
Standard operating procedures	Enhanced coordination of data protection service delivery
Multi-skilled team on data protection matters	Promote quality of service
Budgetary gaps	Enhanced financial sustainability
Data protection infrastructure and systems to coordinate data controllers and processors	Establish a robust data protection ecosystem
Decision making structures and reporting	Enhance coordination and accountability
Policies and procedures for setting up registers of data controllers and processors	Promote compliance
Working with multi-nationals under different jurisdictions	Promote collaboration by leveraging experiences
Compliance and enforcement mechanism	Promote adherence to The Act
Framework for reporting and complaints management	Data subject involvement
Public awareness and communication	Enhance adherence to The Act
Culture and value systems	Foster trust
Self-Regulation by data controllers and processors	Promote collaboration

3 STRATEGIC MODEL

3.1 Overview

The new programme/project developments across the globe require strategic programme/project management that dispel the illusions and misconceptions on the aspects of cost, scope changes, organisational performance, quality, focus, stakeholder contact among other aspects to increase value. Any strategic planning efforts must focus on the best interests of all, or an organisation's stakeholders while considering all aspects of the organisation – from the vision and mission - to working relationships between staff and management, to the roles of various players (especially the role of project sponsors), to the organisation's structure and culture[15]. This chapter, hence, presents the strategic model that will aid the formulation and implementation of the decisions about the ODPC's future direction in the next three years putting into consideration the strategic objectives, key result areas, enablers, and the underlying strategic foundation.

3.2 Vision, Mission Statement and Core Values

Vision

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

Mission

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

Core Values

The ODPC has adopted the following core values:

i) Collaboration and Teamwork
ii) Ethical organisational practices
iii) Transparency and accountability
iv) Inclusive and accessible
v) Organisational effectiveness

[15] Harold Kerzner, Strategic Planning for Project Management Using a Project Management Maturity Model (John Wiley and Sons, 2005)

3.3 Key Result Areas, Enablers, and Foundation

ODPC has identified Three (3) Key Result Areas (KRA), a number of strategic objectives and strategies on which implementation will be carried out, performance measured and results communicated or reported. Figure 1 illustrates the high-level conceptual framework on how these strategic elements link towards the attainment of the institution's mission.

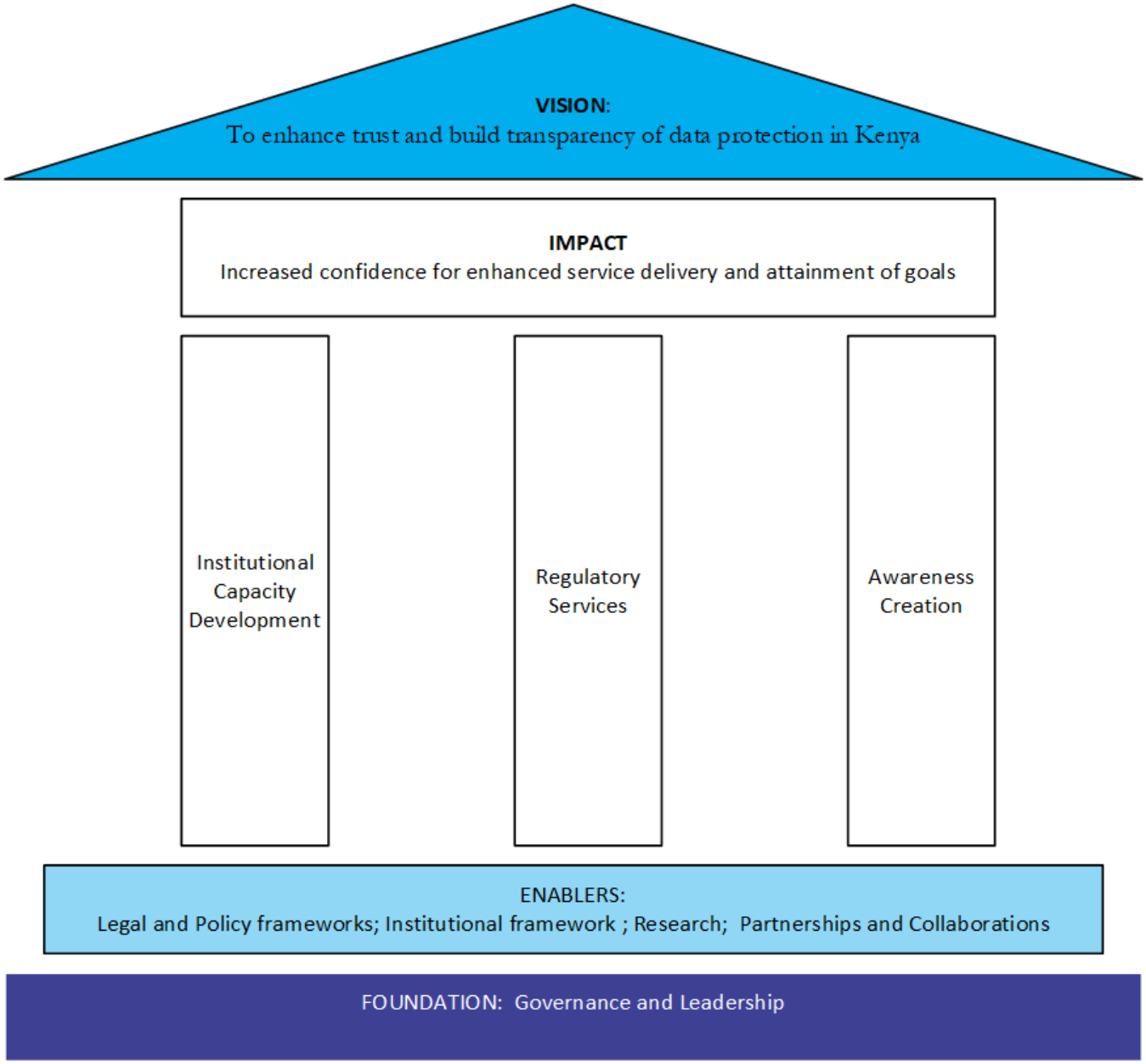

Figure 1 Conceptual framework of the Strategic Model

3.3.1 Key Result Areas

Key Result Areas (KRAs) are the critical cornerstones that address the strategic challenges identified in realization of ODPC mandate, mission and values. They form the areas of excellence that define the shape and distinctive thrust of the organization's growth and direction. These are the strategic focus areas in which ODPC must excel to achieve the vision. The proposed key results areas of excellence under the strategic plan are presented in Table 5.

Table 4 Areas of excellence and strategic direction

Area of excellence	Strategic direction
Institutional capacity development	Build the capacity of the data protection institution and promote partnerships to enhance data processing operations
Regulatory services	Establish policy frameworks to safeguard private data
Awareness creation	Equip stakeholders with adequate information/knowledge on data protection to promote compliance

From each of these key result areas, strategic objectives, strategies, initiatives, outcomes and outputs are derived.

3.3.2 Strategic Enablers

Enablers are critical strategic capabilities that will be provided by the Officer of the Data Protection in collaboration with other government departments and agencies to support the implementation of this strategy. The strategic enablers identified are; Legal, Institutional and Policy frameworks; partnership and collaboration; and, research. The table below links the Enablers with strategic intent to be implemented during the plan period.

Enablers	Strategic direction
Legal and policy framework	Progressively develop and review data protection laws to respond to the changing technologies in the processing of personal data.
Institutional framework	Establish an efficient organization that is responsive to stakeholders' expectations in the provision of services.
Partnership and collaboration	Develop and implement a synergistic data protection foundation that realises valuable partnerships and collaborations.
Research	Leverage on research to achieve a growing, dynamic and innovative environment able to assimilate and respond to emerging trends and concepts of data protection.

Arising from the above strategic enablers, strategic objectives, strategies, initiatives, outcomes and outputs are derived to be implemented and realized during the plan period.

3.3.3 Foundation for the Strategic Plan (2021 to 2023)

The Regulation of Personal Data Processing in Kenya will be anchored on the following foundations that will lead to the achievement of the vision, the planned outcomes and their associated targets.

Foundation	Strategic direction
Governance	Establish effective and transparent management structures
Leadership/Values	Transformative and goal-driven leadership

3.4 Strategic Objectives & Strategies

3.4.1 Key Result Area: Institutional capacity development

Institutional capacity often implies a broader focus of empowerment, social capital, and an enabling environment, as well as the culture, values, and power relations that individuals and organizations in the attainment of the set objectives. Achieving the required level of institutional capacity will require capacity development using various approaches, strategies and methodologies aimed at improving performance at different levels. It can also be achieved through processes by which individuals, groups, organizations, institutions and societies increase their abilities to perform functions, solve problems and achieve objectives, understand and deal with their development need in a broader context in a sustainable manner. Institutional capacity development is therefore a fundamental ingredient of any process of change and transformation.

Under this key result area, we seek to strengthen the capacity of the Office of the Data Protection Commissioner in areas such as human capacity, financial sustainability, structures & processes capabilities and establishment of linkages with relevant organizations. We also seek to nurture a collaborative, innovative and flexible environment that will foster excellence and expertise. We will nonetheless endeavour to continually develop our internal structures and capacities to manage our mandate effectively.

To achieve this, various focus areas, strategic objectives, and strategies have been identified to develop institutional capacity for effective delivery of the data protection services by the ODPC, as summarised in the table below.

Key Result Area	Focus Area	Strategic Objective	Strategies
Institutional Capacity Development	Human resource management and capacity development	Attract and develop competent human resources for timely service delivery	+ Development, approval and implementation of organization structure and staff establishment + Recruitment and deployment of staff as per approved staff establishment + Training of staff on emerging technologies, data protection issues and existing guidelines + Development and implementation of standard operating procedures for human resources + Development, approval and implementation of salary and grading structure + Develop, approval and implementation of staffing and staff benefits framework
	Information Communication and Technology	Leverage on ICT to improve service delivery	+ Automation of ODPC operations for security and efficiency in service delivery + Development, approval and implementation of ICT Policy and Strategy + Development and implementation of Policy on data protection Technologies + Engagement of local and international partners through MoUs on technology, knowledge and experience sharing and exchange + Regular assessment of the state of ICT preparedness on delivery of ODPC mandate
	Administration	To establish and maintain a conducive working environment	+ Establishment and adoption of standards of the working environment at ODPC

Key Result Area	Focus Area	Strategic Objective	Strategies
			+ Development and implementation of staff support and facilitation procedures + Development and implementation of a working environment plan. + Establishment of and implementation of space and resources provision plans for new staff + Development and implementation of a transportation and logistics policy
	Finance	To promote transparency and accountability in the utilization of financial resources	+ Development and implementation of good financial management practices and guidelines + Development and implementation of financial resource mobilization policies and guidelines to supplement Government budget allocation + Effectively participate in Sector Budget preparation and resource sharing to ensure adequate budget allocation + Development and implementation of an internal policy on finance utilisation and reporting to ensure compliance with the Public Finance Management Act, 2012 and relevant National Treasury Circular on management of public funds. + Establishment and implementation of guidelines on the preparation of periodic financial reports
	Procurement	To promote transparency and accountability in procurement of goods and services in line with the Public Procurement and Disposal Act and Regulation	+ Establishment and implementation of procurement and disposal procedures & guidelines + Development and implementation of ICT solutions in procurement framework

Key Result Area	Focus Area	Strategic Objective	Strategies
	Audit	To enhance good public sector governance	+ Development and implementation of a framework for conducting internal system audits + Establish and operationalize Audit Committee + Undertake quarterly and annual system audits to inform management of potential risks and propose mitigation measures + Implement the recommendations of the Public Accounts Committee of the National Assembly
	Risk Management	To Ensure the management of risk is consistent with and supports the achievement of the strategic and corporate objectives	+ Development and implementation of a risk management framework + Establish data protection risk profile + Collaborate with other stakeholders in addressing the data protection risks + Build staff capacity on risk management + Identification, assessment, and prioritization of potential risks + Coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events
	Strategic planning	To align policies with the National Development goals and budget	+ Review policies, legal and regulatory frameworks to align with government priorities + Conduct quarterly and annual reviews on the implementation of workplan and strategic plan to inform on progress + Development and implementation of a MERL framework to enhance effectiveness and efficiency

3.4.2 Key Result Area: Regulatory services

The ODPC is mandated to oversee the implementation of the Data Protection Act, 2019 through provision of regulatory services in the processing of personal data ecosystem. Key to this is the development, review and implementation of Personal Data laws which provide clarity on the obligations and responsibilities of various stakeholders. Stakeholders require clarity from ODPC on compliance requirements and enforcement procedures of The Act. To achieve this ODPC will develop, review and implement policies, frameworks and structures to promote compliance with the Act by data controllers and data processors as well as to safeguard the rights of data subjects. To achieve this, key strategies and programs for each of the identified strategies are needed. The goal is to regulate and promote compliance on data protection as summarised below.

Key Result Area	Focus area	Strategic objective (s)	Strategies
Regulatory Services	Regulation	To provide oversight over the processing of personal data	+ Establishment and maintenance of an accurate register of data controllers and data processors + Regulation of the processing of personal data through the enforcement of data protection laws + Development and issuance of guidelines for regulation of data controllers and data processors + Development and issuance of guidance notes to data controllers and data processors on Data Protection Impact Assessment + Conducting regular and random inspections + Receiving, documenting, investigating and resolution of complaints + Carry out quarterly and random audits of personal data processing systems + Review data protection impact assessment reports

Key Result Area	Focus area	Strategic objective (s)	Strategies
			+ Development and implementation of data protection training curriculum + Promotion of self-regulation through inspections and certification + Development and issuance of mark of quality on the processing of personal data
	Compliance	Enhance compliance with data protection laws	+ Auditing of the efficiency and effectiveness of the existing data protection laws and proposing amendments + Designing and implementing guidelines for managing complaints from data subjects + Development and implementation of Alternative Disputes Resolution Framework + Development and implementation of a framework for monitoring and evaluating personal data processing by data controllers and data processors on enabling the rights of data subjects + Preparation and Issuance of noncompliance notices + Development and issuance of Guidance Notes on compliance + Development and implementation of inspection guidelines + Training of ODPC personnel to conduct inspections of data controllers and data processors

Key Result Area	Focus area	Strategic objective (s)	Strategies
			+ Accreditation of external partners for purposes of assessing level of compliance of self-regulation + Development and implementation of system audit framework
	Enforcement	+ To Enhance execution of the process of ensuring compliance with laws, regulations, rules, standards, and social norms	+ Development and implementation of a framework for breach management + Development and issuance of guidelines on data breach notification + Conduct thorough investigations within the stipulated time frame and communicate findings to concerned parties + Development and issuance of enforcement notices for non-compliance + Preparation and Issuance of penalty notices and compensation notices to concerned parties + Collaboration with other government agencies to administer administrative fines and penalties + Establishment and maintenance of an updated register of noncompliance + Establishment and maintenance of an updated register of complaints + Identification and Deregistration of data controllers and data processors for non-compliance + Identification and publishing of a list of non-compliant data controllers and data processors + Obtaining and enforcing court orders

3.4.3 Key Result Area: Awareness Creation

ODPC will seek to inform and educate Data Controllers, Data Processors and Data Subjects about Personal Data Protection laws with an intention of influencing their personal data processing culture, values, attitudes, behaviours and beliefs.

The Act places the greatest responsibility for data protection with Data Controllers who determines the purpose and means of processing of personal data, however in order to promote compliance, all actors in the Data Protection Ecosystem are critical. These includes, Data Processors, Data Subjects and the Office of the Data Protection Commissioner. Further, data protection is often seen as a matter of cybersecurity and information management alone, that is, a job for IT, security and legal with the help of others. Compliance is much likelier to occur when the application of the law is clear and understood by all stakeholders. One of the biggest challenges in the application of the law is transforming the theory (i.e., legal requirements) into practice (i.e., compliant and sustainable operational behaviours) and adapting to the new norms. This challenge can be overcome by equipping data subjects, data controllers and processors with the necessary knowledge on how to deal with risks to private data and responding to threats. Indeed, education, including formal education, public awareness and training, are recognized as a process by which societies can reach their full potential, promote sustainable development and improve their capacity to address social and development issues.[16]

The Data Protection Act 2019 sub-article 24 (7) recognises the role of the Data Protection Officer in facilitating the capacity building of organisational staff involved in data processing operations and ensuring data controllers and processors comply with the provisions of The Act. Similarly, The Act also recognises the responsibility of the ODPC in ensuring that the members of the public are aware of how the law supports them to exercise their data protection rights as a means of fostering a culture of data privacy. To achieve these goals, the ODPC shall institute appropriate privacy awareness programs that will enable all stakeholders to: (i) identify the personal data under their control; (ii) understand how and why personal data processing is taking place; (iii) protect the personal data from an information security perspective and non-compliant data processing activities; (iv) deal appropriately with personal requests; and (v) respond promptly to any suspected personal data breaches. Again, the ODPC shall engage in continuous processing and monitoring of the well-developed data protection and privacy practices to inculcate a positive mindset in relation to privacy awareness.

[16] https://www.un.org/esa/dsd/agenda21/res_agenda21_36.shtml

Under this pillar, ODPC seeks to strengthen the capacity of the Office of the Data Protection Commissioner in areas such as public awareness and training, particularly for the youth, children and vulnerable populations. To achieve this, various strategic issues, programmes and initiatives have been identified to increase public awareness, build the capacity of all stakeholders to comply with The Act and monitor the effectiveness of communication and outreach for the effective realisation of the mandate.

Key Result Area	Focus area	Strategic objective(s)	Strategies
Awareness Creation	Training	+ Empower data controllers and processors through training programmes to enhance compliance with the provisions of the Act.	+ Development and implementation of a training curriculum + Establishment of partnerships with training institutions to roll out training programs + Conducting training on Data Protection targeting data controllers and processors
	Public Outreach	+ Empower data subjects through strategic initiatives to promote public awareness of fundamental rights to personal data privacy and security.	+ Establishment of public awareness initiatives on data privacy and security + Identification and adoption of appropriate communication channels for dissemination of key information on personal data protection + Development of key messages for dissemination
	Communication	+ To promote seamless and strategic communication within and among all stakeholders.	+ Development and implementation of communication policy and strategy + Regularly updating content on the ODPC website on trends in data protection + Management of the ODPC visibility on the social media platforms + Establishment and operationalization of a customer care service unit

3.4.4 Enablers of effective data protection regime:

This Strategic Plan identifies Legal and Policy frameworks; Institutional Coordination framework; Research; and, Partnerships and Collaborations as key enablers towards promotion of effective personal Data Protection regime.

The legal and policy frameworks govern and regulate information security aligning with models of information security within organisations as well as external environments. This encompasses the legal bases within which data protection falls. Such bases as envisaged in the Data Protection Act, 2019 include consent by the data subjects, contract with the data subjects, legal obligations (particularly by the controllers), interests of the data subjects, public interest, legitimate interests of the data controller as well as legal bases in other instances such as research and public authority. In order to derive quality value in the implementation stage of this strategy, various existing legal and policy frameworks have to be mapped and reviewed in terms of the extent to which they account for information security and privacy across the country.

Data protection, predominantly being a people and process driven also calls for the implementation of data security best practices and institutional frameworks. The overall goal of the Act is to create a baseline of institutional guidance through infrastructures and systems. To achieve this, institutions will be required to develop and implement guidelines within their bounds of operation aligned to the Act. These guidelines will be subjected to verification by ODPC during audit or inspections if need be. Some of these guidelines include training plans for their employees on data protection, Institutional Data Protection Policy, infrastructure and systems update reports as well as data security reports. Through a coordinated infrastructure, these institutional frameworks can be shared across the stakeholders and create room for more collaborative initiatives. For example, the institutional framework governing ODPC to enable regulations within the financial sector can be exchanged with the regulations of the medical services to enable enhanced institutional frameworks and knowledge exchange between the two.

Collaboration is key to realising an effective strategic plan. ODPC will derive a lot of value through collaboration and partnership from both local and international partners in areas such as development of institutional capacity, awareness creation, funds mobilization among other ways.

The role of Research in facilitating the identification of emerging issues and adoption of new innovative approaches in Personal Data Protection is critical during the plan period. Research spans across the various key result areas in the realisation of a successful strategic plan. As a dynamic discipline, conducting research will enable the ODPC to stay updated on technology trends, new local and global initiatives, identifying gaps

in the existing policies and frameworks as well as build a very strong human capital that is informed on innovations that can support security and privacy issues of the data subjects. Further, through research, ODPC will be able to identify the existing institutional gaps and develop ways to address these gaps including models of engagement on information and experience exchange and cooperation among various stakeholders. A summary of the strategic objectives and strategies for each enabler is presented below.

Strategic Enablers	Focus Area	Strategic Objective (s)	Strategies
Legal and Policy Frameworks; Institutional Coordination Framework; Partnership and Collaboration; and Research	Legal and policy frameworks	+ Improve the governance of personal data regulatory environment	+ Development and review of policy, legal and regulatory framework on data protection
	Institutional coordination framework	+ Enhance service delivery	+ Review and implementation of an effective organization structures and staff establishment to address identified gaps in human capital + Review and implementation of standards operating procedures to reflect changes in technology + Create and operationalize a reserve fund to finance operational and maintenance expenditure in compliance with the Act
	Partnership and collaboration	+ Promote local and international cooperation to ensure fulfilment of local and international obligations in data protection	+ Establishment of partnerships in the implementation of programmes + Cooperation and collaboration with other data protection authorities for experience and knowledge sharing + Implementation of international obligations on data protection
	Research	+ To keep pace with emerging trends and practices in personal data protection	+ Conduct regular targeted research on emerging trends and practices in personal data protection + Implementation of research findings and recommendations to enhance efficiency and effectiveness

3.4.5 Foundation: Governance and Leadership/Values

Good governance and strong leadership are primordial as a foundation for any organization and therefore ODPC will promote good governance and adoption of leadership principals and national values as envisaged in the Constitution in the implementation of its mandate. This will result in effective oversight, sound regulatory framework and accountability. ODPC will put in place Governance structures, coupled with the identification of national values champions. In addition, during the plan period, ODPC will develop and implement institutional Code of Conduct and Ethics as well as citizen service delivery charter.

The Code of Conduct and Ethics will provide a clear framework within which the staffs are expected to conduct themselves while the Service Charter will enhance Stakeholders' awareness on the services the office provides as well as inform them, of the standards of services they should expect from the office.

To enhance the relationship between the ODPC and the Stakeholders including members of the public, the following strategies will be adopted during the plan period;

i) evidence-based policy development
ii) efficient and effective regulatory frameworks and management systems
iii) responsible leadership
iv) transparency
v) institutional checks and balances
vi) the responsible exercise of the citizens voice with regards to concerns raised
vii) clear and enforceable accountability.

The table below summaries the strategic objectives and strategies to be implemented under the Governance and Leadership/ Values pillar;

Foundation	Focus Area	Strategic objective(s)	Strategies
Governance	Structures	+ Promote Good Governance in the regulation of personal data in the country	+ Develop and institutionalise governance structures that promote good governance for effective operations of the ODPC. + Establish a governance framework for the ODPC

Foundation	Focus Area	Strategic objective(s)	Strategies
			anchored on the Data Protection Act 2019 to enhance service delivery + Establish and operationalise all the relevant management committees + Institute reporting and communication channels
	Oversight responsibilities	+ Promote checks and balances to enhance transparency and accountability	+ Establish oversight roles to effectively manage accountability + Define oversight roles of the management team at the ODPC to enhance accountability + Develop and implement a citizen service charter
Leadership/Values	Talent and culture	Promote ethics and integrity	+ Establish institutional ethical practices, values and cultural principles within the ODPC + Develop and implement code of conduct and ethics

4 IMPLEMENTATION & COORDINATION FRAMEWORK

4.1 Overview

This chapter presents strategies for implementing the strategic plan alongside the organisation model. It also outlines the proposed organisation structure, staff establishment and accountability model. A summary of the budget and a risk plan is also presented.

4.2 Approved Organisational Model

A: Data Commissioner

The Data Commissioner as the Authorized and Accounting Officer shall be responsible for providing overall leadership and direction on the implementation of the strategic plan. The Data Commissioner shall lead and oversee the implementation of ODPC's strategic programmes/projects in accordance with its approved strategy.

B: Deputy Data Commissioners

Deputy Data Commissioners shall be responsible for overseeing the cascading and implementation of the strategic plan through the approved strategic activities. ODPC has four directorates have been established, namely: (i) Corporate Services Directorate; (ii) Data Protection Compliance Directorate, (iii) Complaints, Investigations and Enforcement Directorate; and, (iv) Research, Policy & Strategy Directorate. Each directorate will be headed by a Deputy Data Commissioner. The Deputy Data Commissioners shall supervise Assistant Data Protection Commissioners involved in Plan execution.

C: Assistant Data Protection Commissioners

Assistant Data Protection Commissioners shall head divisions. They shall be responsible for the project execution of the approved strategic activities of the strategic plan. The Assistant Data Protection Commissioners shall supervise the line staff and are accountable to the respective Heads of Directorates. 12 regional offices comprising clusters of counties shall also be created. These are presented in ANNEX III.

D: Heads of Units

Heads of units shall report directly to the Data Protection Commissioner. These units shall include Information Systems Unit, Supply Chain Management Unit, Internal Audit Unit and the Legal Unit. A summary of the organisation model is illustrated in Figure 2.

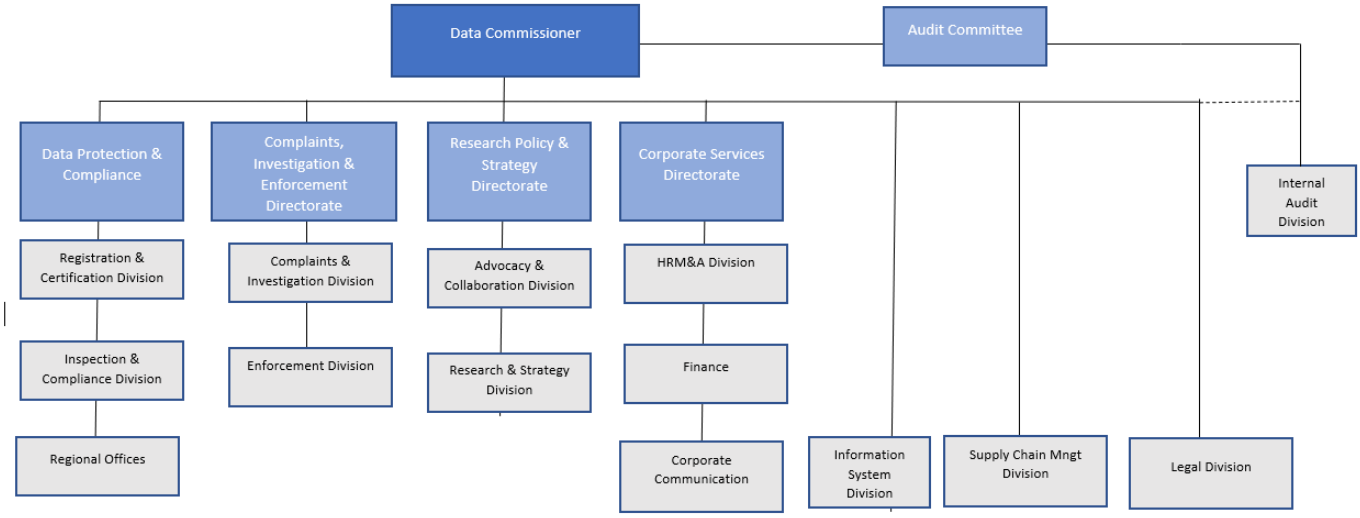

Figure 2: Approved organisational structure of ODPC

4.2.1 Leadership structure

The management team comprises the Data Commissioner, Heads of Directorates (the Deputy Data Commissioners), and the Heads of Divisions (the Assistant Data Protection Commissioners) in the various directorates. Three committees have also been established through which the Data Protection Commissioner will manage the technical and corporate affairs of the office. These committees include: Human Resource Management Advisory Committee, Data Protection, Compliance and Enforcement Committee, and Dispute Resolution Committee.

4.2.2 Staff Establishment

As of October, 2021, the ODPC had 10 staff members, in both technical and support services, deployed from Ministry of ICT, Innovation and Youth Affairs and the National Treasury for one year. The current staff establishment is illustrated in Figure 3.

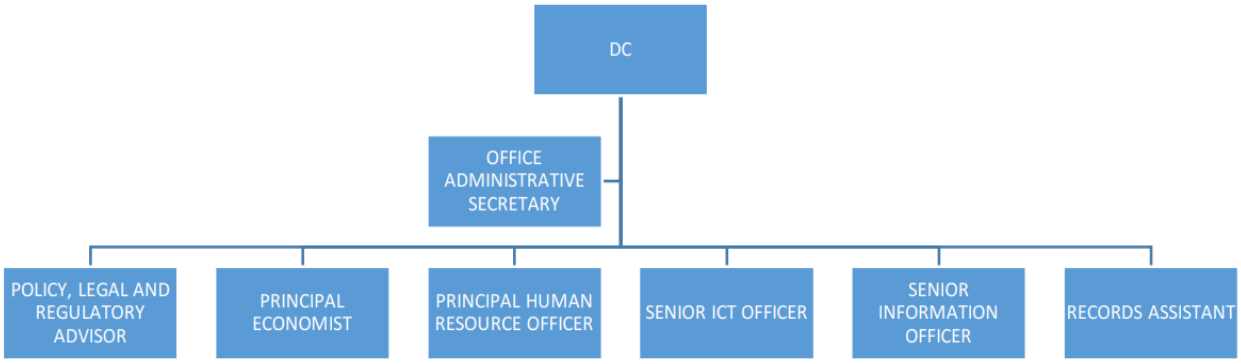

Figure 3 Current Staff Establishment of ODPC

A staff establishment of ninety-two (92) staff comprising 57 officers for technical services cadres and 35 officers in the support services cadre has been identified and approved by Public Service Commission for implementation. ODPC will prioritize staff recruitment in the FY 2021/2022 and FY 2022/2023. The approved staff is presented in Table 5.

Table 5 Summary of Approved Staff Establishment by cadre

Designation	Job Grade	Authorized Establishment
Office of the Data Commissioner		
Data Protection Commissioner	ODPC 1	1
Senior Office Administrator	ODPC 5	1
Personal Assistant	ODPC 4	1
Senior Driver	ODPC 8	1
Office Assistant	ODPC 11	1
Total		5
Deputy Data Commissioner - Data Protection and Compliance	ODPC 2	1
Sub Total		1
Registration and Certification Division		
Assistant Data Commissioner Registration	ODPC 3	1
Senior/Principal Data Protection Officer- Registration	ODPC 4/5	1
Data Protection Officer II/I Registration	ODPC 7/6	3
Sub Total		5
Inspection and Compliance Division		
Assistant Data Commissioner Inspection and Compliance	ODPC 3	1
Senior/Principal Data Protection Officer- Inspection and Compliance	ODPC 5/4	1
Data Protection Officer II/I Inspection and Compliance	ODPC 6/5	3

Designation	Job Grade	Authorized Establishment
Sub Total		5
Total		11
Regional Offices		
Principal Data Protection Officer	ODPC 4	8
Senior Data Protection Officer	ODPC 5	5
Data Protection Officer II/I	ODPC 7/6	13
Assistant Office Administrator II/I	ODPC 8/7	5
Sub-Total		31
Deputy Data Commissioner Investigations and Enforcement	ODPC 2	1
Sub Total		1
Complaints and Investigations Division		
Assistant Data Commissioner Complaints and Investigations	ODPC 3	1
Senior/Principal Data Protection Officer - Complaints and Investigation	ODPC 5/4	1
Data Protection Officer 11/1	ODPC 7/6	3
Sub Total		5
Enforcement Division		
Assistant Data Commissioner Enforcement	ODPC 3	1
Senior/Principal Data Protection Officer - Enforcement	ODPC 4/5	2
Process Servers/ Legal Clerks	ODPC 8/7	2
Sub Total		5
Total		11
Deputy Data Commissioner Research, Policy and Quality Assurance	ODPC 2	1
Sub Total		1
Advocacy and Collaboration Division		
Assistant Data Commissioner Advocacy and Collaboration	ODPC 3	1
Senior/Principal Data Protection Officer - Advocacy and Collaboration Officer	ODPC 5/4	2
Sub Total		3
Research and Strategy Division		
Assistant Data Commissioner - Research and Strategy	ODPC 3	1
Senior/Principal Data Protection Officer- Research and Strategy	ODPC 4/5	1
Data Protection Officer II/I	ODPC 7/6	2
Sub Total		4
Total		8

Designation	Job Grade	Authorized Establishment
Deputy Data Commissioner Corporate Services	ODPC 2	1
Sub Total		1
Human Resource and Administration (HRM&A) Division		1
Senior. Principal HRM&A Officer	ODPC 3	1
Principal HRM &A Officer	ODPC 5/4	1
HRM Officer II/I	ODPC 7/6	1
Senior Administration Officer	ODPC 5	1
Assistant/ Senior Assistant Records Management	ODPC 8/7	2
Security Officer	ODPC 8/7	1
Office Assistant	ODPC 11/10	2
Drivers	ODPC 10/9	2
Sub Total		11
Finance and Accounts Division		
Senior Principal finance Officer	ODPC 3	1
Senior/Principal Accountant	ODPC 4/5	1
Accountant II/I	ODPC 7/6	2
Sub Total		4
Corporate Communications Division		
Senior. Principal Corporate Communication Officer	ODPC 4	1
Corporate Communication Officer II/I/Senior/Principal	ODPC 7/6/5	1
Sub Total		2
Total		18
Supply Chain Management Division		
Senior. Principal Supply Chain Management Officer	ODPC 4	1
Supply Chain Management Officer II/1/Senior	ODPC 7/6/5	1
Sub Total		2
Internal Audit Division		
Senior Principal Director Internal Auditor	ODPC 4	1
Sub Total		1
Information Systems Division		
Senior. Principal Information Systems Officer	ODPC 4/3	1
ICT Officer II/I/Senior	ODPC 7/6/5	2
Sub Total		3
Legal Division		
Senior. Principal Legal Officer	ODPC 4/3	1

Designation	Job Grade	Authorized Establishment
Legal Officer II/I/ Senior/Principal	ODPC 6/5	2
Sub Total		3
Total		9
Total Technical		57
Total Support Services		35
Grand Total		92

4.2.3 *Proposed Organisational Structure*

Considering the need to cascade the operations of the ODPC to the devolved units of government and in recognition of the need to establish regional clusters as detailed in the Act, OPC propose the establishment of regional clusters coordination Division and County coordination unit. To handle and coordinate data subjects' queries, it is considered necessary to establish a customer care unit under the Directorate of Compliance, Investigation and Enforcement. Considering the critical role ICT will play in the data protection mandate of ODPC, it is also proposed that ODPC establishes the ICT & Innovation Directorate to enable ODPC to respond effectively to any technological issues touching on data protection. Similarly, considering the regulatory role of the ODPC and the need to keep abreast with the changing legal environment it is proposed that the establishment of a Legal & Advisory Directorate be prioritized to effectively provide timely legal advice and to handle children's data protection rights. To ensure continuous improvement on service delivery and appropriate response to potential risks associated with data protection, the plan propose the establishment of a Quality Assurance and Risk Management Division. Figure 4 illustrates the proposed organisational structure.

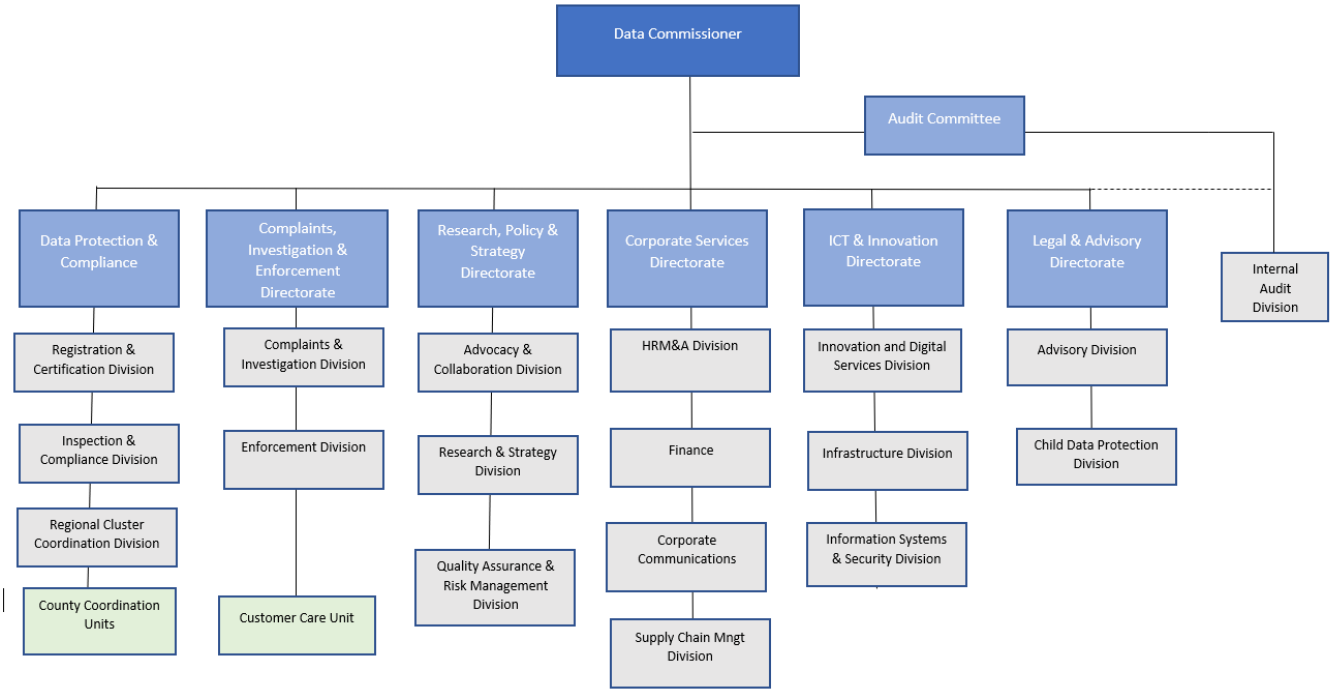

Figure 4 Proposed Organisational Model

Based on the proposed organisational model, we propose a staff establishment as presented in Table 6. Distribution of these roles is provided in ANNEX IV

Table 6 Proposed Staff establishment

Cadre	In-Post	Required	Variance
Technical Services	4	118	114
Support Services	6	114	108
Total	10	222	222

4.2.4 Accountability Framework

The overall responsibility of implementing this strategic plan rests with the data commissioner. The holder of the office will be charged with overseeing the actual implementation of the strategic plan to meet the strategic objectives set and, in particular, the targets as outlined in the implementation matrix at the end of this document. The Data Commissioner will be in charge of providing overall policy direction in the implementation of all activities outlined in the strategic framework, including the allocation and re-allocation of resources. Continuous monitoring of performance will be mainstreamed in the organization including preparation of semi-annual and annual progress reports. Specifically, annual reviews would include an

assessment of the assumptions and risks set out in the log frame. ODPC should work to tighten feedback and learning loops, to enable real-time adjustment of the programmes/project action points.

4.3 Strategies for implementing the Strategic plan

The Office of the Data Protection Commission will pursue the following strategies to ensure the effective implementation of this strategic plan.

4.3.1 Phasing and Sequencing Strategy

The organization recognizes that available resources are inadequate to implement its programmes and activities, despite their importance. It will therefore prioritize those with the greatest contribution and impact to its core mandate and ensure that resources are appropriately allocated in line with this. implementation of all programmes and activities will be scheduled to ensure that the most critical are given priority.

4.3.2 Results-Based Management Strategy

ODPC recognizes the importance of internal processes but will focus on the key outputs and impacts relevant to the needs of the general public. In pursuing this strategy, the ODPC will ensure that internal processes are designed and streamlined to facilitate quality service delivery.

4.3.3 Institutional Strengthening (IS) Strategy

Institutional strengthening will be part of our continuous improvement even as we align ourselves to meet the complexity and diversity of the data protection programs. We shall encourage change within our systems and procedure to embrace the much-needed IS strategies. We shall develop and establish an IS strategy whose objective is to remove obstacles that inhibit our staff and governance structures to realize our programming goals. We shall focus to enhance our organization's abilities to perform in meeting our mandate.

4.3.4 Human Resources Development Strategy

During this strategic plan period, our human resource approach will take a result-based perspective, directed at ensuring the organization has lean but effective and suitable personnel for its needs. ODPC shall carry out training and staff development to meet the missing gaps in skills and knowledge to empower our staff in meeting the programming needs. At the same time, ODPC will strive to understand and articulate the aspirations and views of our staff to meet the management's expectations.

ODPC will continue to pursue a collaborative, innovative, and flexible working environment and relationships that foster excellence and expertise in our staff and in how we operate. Staff working at ODPC should always feel valued and supported.

4.3.5 Financial Resources Management Strategy

A: Financial Resource Requirements. KES 3,612,000,000 in investments will be required to implement the strategic plan. A summary of the budget requirements is presented in Table 7.

Table 7 Summary Budget for implementation of the strategic plan

Key Result Area	Year 1	Year 2	Year 3	Budget Amount (KES')
Institutional Capacity Development	777,300,000	314,170,000	1,432,780,000	2,524,250,000
Regulatory Services	66,700,000	50,300,000	47,000,000	164,000,000
Awareness Creation	197,000,000	110,500,000	62,250,000	369,750,000
Enabler: Legal and Policy Frameworks; Institutional Coordination Framework; Partnerships & Collaboration; and, Research	70,000,000	25,500,000	13,500,000	109,000,000
Foundation: Governance and Leadership/Values	217,000,000	114,000,000	114,000,000	445,000,000
Total	1,328,000,000	**614,470,000**	**1,669,530,000**	**3,612,000,000**

B: Resource Gaps. The resources gap based on the overall projected budget for the implementation of the strategic plan is summarised in Table 8.

Table 8: Summary budget for implementation of the strategic plan

Budget Estimates	Resource Estimates		
	2022/2023	2023/2024	2024/2025
Recurrent	1,131,000,000	500,000,000	1,784,000,000
Estimated Total Budgetary Allocation	**270,000,000**	**473,000,000**	**1784,000,000**
Variance	861,000,000	27,000,000	0

4.3.6 Resource Mobilisation Strategies

This strategic plan has been developed with a cost component in mind. Its success is hinged on ODPC's abilities to secure funding to implement our strategic programmes/initiative. ODPC shall use this strategic plan for resource mobilization and seek to work with like-minded partners. Strict and prudent financial management practices should be espoused during the implementation period. The ODPC should be keen to plan, organize, and monitor the financial resources given to it even as the ODPC manages the resources on

behalf of the partners and other stakeholders. The ODPC shall be transparent to enhance credibility to the society they serve and in the eyes of the funding organizations.

It is expected that the financing options will include:

i) Government of Kenya
ii) Internally generated income
iii) Innovative funding models including
    a) Resource mobilization through Partnerships
    b) Strategic Alliances with Key Sector Players
iv) Support by the International Community

4.4 Risk Analysis and Mitigation Measures

Risk management encompasses the identification, analysis, and responding to risk factors. Effective risk management means attempting to control, as much as possible, future outcomes by acting proactively rather than reactively. This calls for putting in place strategic mitigation measures that offers the potential to reduce both the possibility of a risk occurring, its potential impact, and severity.

ODPC shall pursue a strategy of continuous and regular risk assessment of potential risk and instituting corrective mitigation measures. In so doing ODPC will explore how to achieve an explicit and balanced risk profile in the strategic programmes/projects it will undertake, including high-risk programming with the potential for transformative impact. ODPC shall develop a data protection risk register that can allow to identify and mitigate against data protection risks, as well as demonstrate compliance.

The goal of conducting risk analysis and instituting mitigation measures is to ensure internal processes focus on the key outputs and impacts relevant to the needs of the stakeholders. In pursuing this approach, the ODPC will ensure risks do not affect the implementation of the strategy for enhanced service delivery. Some of the potential risks and mitigation plans to be instituted by ODPC are presented in Table 9.

Table 9 Summary of risk analysis and mitigation measures

Risk Categories	Risks	Overall Rating	Mitigation Strategies	Owner of the Risk
Strategic risk	+ Delayed development of the SOPs, internal policies, guidelines. + Lack of cooperation from key stakeholders + Limited capability and capacity of Stakeholders	High	+ Come up with the right up-front strategy, + Identify and qualify the right stakeholders and team to drive decisions. + Mid-term review of the strategic plan + Monitoring and evaluation of the strategic plan	DPC
Cyber risk	+ Cyber Security threats	High	+ Develop security policies and processes to reduce the overall risk or impact of a cybersecurity threat. + Install security solutions such as firewalls and antivirus software. + Continuously monitor network traffic, as well as organisation's cybersecurity posture + Training of personnel to ensure they have the latest skills regarding cyber security	+ DPC + ICT & Innovation Directorate
Legal and Compliance risk	+ Inadequate legislative and regulatory frameworks both internally, nationally, and in counties + Non -compliance with the Act + Delayed resolution of disputes + Improper data use + Pervasive technology	High	+ Collaborate with the MoICT in advocating for National Assembly to pass appropriate legislation + Create and maintain a strong, ethical, and compliant approach to data protection and keeping up with changes in the industry. + Complaints and Enforcement Directorates to monitor and enforce compliance frameworks	+ DPC + Complaints & Enforcement Directorate

Risk Categories	Risks	Overall Rating	Mitigation Strategies	Owner of the Risk
			and use relevant services to stay on top of things. + Strict measures and consequences in cases of non-compliance + Continuous updates to the staff on any changes in the laws and legislation + Regular audits by the internal audit function.	
Operation risk	+ Delay in procurement + Inadequate staffing and human capacity development + Inadequate resource allocation + Weak implementation capacity + The programmes/projects with a multiplicity of actors and this makes them complex given that they are implemented by independent institutions and may become difficult to monitor and supervise + Conflict of interest with international and local partners	Medium	+ Identify and manage loss events proactively with timely operational risk intelligence. + Invest in a comprehensive and unified system to manage all your ORM requirements efficiently. + Develop second-line oversight to ensure operational excellence and business-process resiliency (relevant committees) Map processes, risks, and controls. + Develop comprehensive policies and procedures in relation to the operations such as procurement, human resources, IT policies and procedures. + Regular audits by the internal audit function and annual external audits + ICT, ICT systems, regular audits of ICT systems + Develop a working performance management system	+ DPC + Corporate Services Directorate + ICT & Innovation Directorate

Risk Categories	Risks	Overall Rating	Mitigation Strategies	Owner of the Risk
			+ Develop working mechanisms for proper safeguarding of the organization's assets	
Financial risk	+ Insufficient budget to operationalize the ODPC mandate + Delayed funding + Delayed payment of bills	High	+ Account for all areas of the office's main business of data protection, from human resources to operations. + Evaluate business operations for efficiency. + Have a strong foundation for your HR practices. + Use metrics for every decision. + Be prepared to cover a loss. managers to get creative at preventing a loss of vital services + Put in place a strong and working internal control system + Monitor the internal control system on a regular basis + Ensure monthly management reports are done and completed within the stipulated timeline submitted to the top leadership + Ensure annual external audits are carried out + Timely requests for exchequers + Timely release of funds + Compliance to financial management Act	+ DPC + Head of Finance
Reputation risk	+ Corruption or perceived corruption + Dissatisfaction with service delivery by the stakeholders	High	+ Protect the organization against data breaches. + Be vigilant about customer service mishaps.	+ DPC + Complaints & Enforcement Directorate

Risk Categories	Risks	Overall Rating	Mitigation Strategies	Owner of the Risk
	+ Inadequate knowledge on data privacy and protection +		+ Keep employees happy to prevent reputation risk. + Make values truly operational, have ethical conduct. + Manage external reputation risks. + Encourage a culture of upholding ethical values + Constitute a Public Relations unit that will be the correspondence with external stakeholders + Comply with the service standards and regulations	+ Head Of Advocacy + Corporate Services
Political Risk	+ Uncertain political goodwill + Change in government	High	+ Establish consultations and regular engagements with political leaders + Have consultations with national government ministries, departments and political leaders. + Have the legal officers monitor the political climate of the country.	+ DPC + Head Of Communication + Head Of Strategy and Policy
IT risk - system failure, IoT vulnerability, improper data use	+ Overreliance on vendors + Malfunctioning of IT systems and equipment + Different data formats and data curation methods + Technological changes + Increased demand for digital services	High	+ Have built-in security as a part of the design process + Have multiple layers of protection against a single risk + Have a better access control for users + Regular monitoring and patching of security + Clear communication to consumers regarding data streams and information use + Setting protocol that can prevent illegal sharing of data.	+ Data Commissioner + Head Of ICT + Head Of Finance

Risk Categories	Risks	Overall Rating	Mitigation Strategies	Owner of the Risk
			+ Developing clear policies about using personal devices on the organisation's secure network. + Encourage a culture of upholding ethical values + Regularly update software to the latest versions + Train staff in IT policies and procedures. + Use data backups that include off-site or remote storage + Secure computers, servers and wireless networks	

5 MONITORING, EVALUATION & REPORTING

5.1 Overview

This chapter presents the monitoring, evaluation and reporting framework for the strategic plan. Monitoring and evaluation will involve a systematic and continuous process of collecting and analysing data on targets, output indicators and outcome indicators. The results of the monitoring, evaluation and reporting will be used to provide an evidence-driven approach to decision making to inform corrective actions, improve implementation of strategic activities and inform future planning of the ODPC. The M&E framework is presented in ANNEX II.

5.2 Monitoring Implementation of the Strategic Plan

Implementation of the strategic plan will be closely monitored to determine the status and establish the need for adjustments in the context of a dynamic internal or external environment. Monitoring shall include the systematic collection of data and analysing information based on the targets, outputs, outcomes, performance indicators, and feedback reports from Directorates, Divisions, and Units of the ODPC. The collected information will be analysed to prepare monthly, quarterly and annual reports.

5.3 Evaluation of the strategic plan

Evaluation will involve a systematic and objective process of examining the relevance, effectiveness, efficiency, and impact (both expected and unexpected) and sustainability of the strategies. The ODPC shall conduct annual, mid-term, and end-term evaluations of the strategic plan to establish the extent to which the outputs and outcomes expected have been realised. Annual evaluations shall be tied to individual employee performance targets and aggregated at the directorate level to inform the extent to which collective efforts are influencing the strategic implementation. Moreover, the annual report shall inform the annual budget and reporting on performance contracting obligations. Mid-term evaluation of the strategic plan shall examine the progress towards achieving set targets and generate recommendations that will be used to improve the strategic plan implementation process. End-term evaluations shall be conducted at the end of the strategic planning period to assess to what extent set targets have been accomplished. Results from the end-term evaluation shall be used to inform the next cycle of the strategic planning process.

5.4 Reporting

Reports shall track progress towards attainment of ODPCs results and generation of strategic information to inform decision making by stakeholders at the organizational and at the national level. All directorates,

divisions, and units in the ODPC will be involved in quarterly, bi-annual, and annual reporting on the progress of achievement of results and objectives based on the key output and outcome indicators. Result-based management will be adopted where every individual contributes towards the realization of this strategic plan.

- Individual performance targets will be set and agreed upon between Directorates and their respective staff members. For support services, the performance targets must be aligned to the strategic direction of the mandate of the Organization
- Performance evaluation will be carried out quarterly with the final evaluation to be done at the end of the year
- Departmental meetings will be held to monitor the implementation of action plans cascaded from the strategic plan
- Annual strategic review workshops will be held to evaluate the impact of planned actions and the level of achievement of the strategic objectives

An illustrative template for reporting is presented in Table 10.

Table 10 Monitoring & Evaluation Reporting Framework

Strategic Issues	Output/Outcome	Activity	OVI/KPIs	Baseline	Target	Achievements	Variance	Lessons Learned
SP Issues 1								
Objective 1								
SP Issues 2								
SP Objective 2								

6 ANNEXES

6.1 ANNEX I: IMPLEMENTATION MATRIX

6.1.1 *Key Result Area: Institutional Capacity Development*

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
Institutional Capacity Development	Human Resource Management and Capacity Development	Attract and develop competent human resources for timely service delivery	Recruitment and deployment of Staff as per approved staff establishment	Enhanced capacity	Recruited and deployed staff	No. of staff recruited	222	92	103	222	182,160,000	183,050,000	837,270,000	DPC, ICT & Innovation Directorate
			Training of staff on emerging technologies, data protection issues and guidelines	Enhanced knowledge on emerging technologies, data protection issues and guidelines	Well trained staff on emerging technologies, data protection issues and guidelines	No. of staff trained on emerging technologies, data protection issues and guidelines	200	40	40	120	39,470,000	39,470,000	428,410,000	
			Development and implementation of approved organization structure and staff establishment	Efficient service delivery	Approved Organization structure staff establishment	Organization structure staff establishment in place	1	1	0	0	1,000,000	-	-	
			Development and implementation of Standard Operating Procedures for human resources	Standardized operating procedures on human resources	Implemented SOPs for HR	SOPs for HR in place	1	1	0	0	5,000,000	-	-	
			Development, approval and implementation of Salary and Grading Structure	Harmonized salary and grading structures	Approved salary grading structure	Salary grading in place	1	1	0	0	2,000,000	-	-	
			Development, approval and implementation of staffing and staff benefits framework	Harmonized staff benefits	Approved staff benefits framework	Staff benefits framework in place	1	1	0	0	2,000,000	-	-	

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
	Information and Communications Technology (ICT)	Leverage on ICT to improve service delivery	Development, approval and implementation of ICT policy and strategy	Coordinated and structured ICT utilization	Approved ICT policy and strategy	ICT policy and strategy in place	1	1	0	0	5,000,000	-	-	DPC, ICT & Innovation Directorate
			Automation of ODPC's operations for security and efficiency in service delivery	Automate, secure and sustain ODPC operations	ODPCs operations automated	Automated ODPC operations in place	1	0.25	0.5	1	494,960,000	80,000,000	80,000,000	
			Development and implementation of Policy on data protection technologies	Standardized data protection technologies	Approved Policy on data protection technologies	Data protection technologies policy in place	1	0	0.5	0.5	-	2,000,000	25,000,000	
			Engagement of local and international partners through MOUs on technology, knowledge and experience sharing and exchange	Enhanced Technology exchange	Partners Engagement	No. of MoUs signed and executed	10	3	3	4	2,800,000	2,800,000	9,800,000	
			Regular assessment of the state of ICT preparedness on delivery of ODPC mandate	Enhanced understanding on the state of ICT preparedness	An ICT preparedness assessment report	An ICT preparedness assessment report available	1	1	0	0	5,000,000	-	-	
	Administration	To establish and maintain a conducive working environment	Establishment and adoption of standards of the working environment at ODPC	Good working environment	Developed standards of the working environment at ODPC	Standards of the working environment established and adopted	1	1	0	0	1,000,000	-	-	Data Protection Commissioner, Corporate Services Directorate
			Development and implementation of a working environment plan	Good Working environment	Developed working environment plan	Working environment plan in place								
			Establishment and implementation of space and resources	Available working space and resources	Working resources provisioning plan	Working resources provisioning plan in place	1	1	0	0	2,100,000	-	-	

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			provision plans for new staff	for new staff										
			Development and implementation of staff support and facilitation procedures	Enhance ability to perform assignments	Staff support and facilitation procedures	Staff Support and facilitation procedures in place	1	1	0	0	100,000	-	-	
			Development and implementation of a transportation and logistic policy	Available transpiration and logistic support	Working resources provisioning plan	Working resources provisioning plan in place	1	1	0	0	1,000,000	-	-	
	Finance	To promote transparency and accountability in the utilisation of financial resources	Development and implementation of good financial management practices and guidelines	Prudent finance management	Approved good financial management practices and guidelines	Good financial management practices and guidelines in place	1	1	0	0	1,000,000	-	-	Data Protection Commissioner, Corporate Services Directorate
			Development and implementation of financial resource mobilisation policies ang guidelines to supplement government budgetary allocation	Enhanced financial sustainability	Approved financial mobilization policies and guidelines	Financial mobilization policy in place	1	1	0	0	2,500,000	-	-	
			Effectively participate in Sector Budget preparation and resource sharing to ensure adequate budget allocation	Adequate finance resources allocation by National Treasury	Adequate allocation of adequate financial by the National Treasury	% Financial allocation by the National Treasury	100%	80%	90%	100%	-	-	-	
			Development and implementation of an internal policy on finance utilisation and reporting to ensure compliance with the Public Finance Management Act,	Enhanced finance management	Approved internal policy on finance utilization nd reporting	Internal policy on finance utilization end reporting in place	1	1	0	0	2,000,000	-	-	

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			2012 and relevant National Treasury circulars on management of public funds											
			Establishment and implementation of guidelines on preparation of periodic financial reports	Good financial reports	Approved policy guidelines on preparation of periodic financial reports	Policy guidelines on preparation of financial reports in place	1	1	0	0	2,500,000	-	-	
	Procurement	To promote transparency and accountability in procurement of goods and services in line with the Public procurement and Disposal Act and Regulation	Establishment and implementation of procurement and disposal procedures & guidelines	Streamlined procurement and disposal	Adoption of Public Procurement and disposal Act	% level adoption of Public Procurement and disposal Act	100%	50%	100%	100%	-	-	-	Data Protection Commissioner, Corporate Services Directorate
			Development and implementation of ICT solutions in procurement framework	Enhanced coordination of the procurement activities	Adopt ICT solution in procurement	Adopt ICT solution in procurement	1	0.5	0.5	0	2,750,000	50,000	-	
	Audit	To enhance good public sector governance	Development and implementation of a framework for conducting internal systems audits	Enhanced internal system audits procedures	Approved framework for conducting internal systems audits	Framework for conducting internal systems audits in place	1	0	1	0	-	500,000	-	Data Protection Commissioner, Corporate Services Directorate
			Establish and operationalise Audit committee	Effective oversight of ODPCs operations	Fully constituted audit committee	Audit committee in place	120	5	60	120	800,000	1,000,000	20,000,000	
			Undertake quarterly and annual system audits to inform management n potential risks and propose	Continuous system improvements	Quarterly and annual system audit	Quarterly and annual system audit report	15	5	5	5	250,000	250,000	250,000	

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			mitigation measures											
			Implement the recommendations of the Public Accounts committee of the National Assembly	Compliance with the Public Investment and Disposal Act	Implemented recommendations	Implementation status	3	1	1	1	50,000	50,000	50,000	
	Risk Management	To ensure the management of risk is consistent with and supports the achievement of the strategic and corporate objectives	Development and implementation of a risk management framework	Effective Risk management	Approved risk management framework	Risk management framework in place	1	0	0	1	-	-	5,000,000	Data Protection Commissioner, Corporate Services Directorate
			Establish data protection risk profile	Well documented data protection risks	Data protection risk profile	Data protection risk profile in place	1	1	0	0	500,000	-	-	
			Collaborate with other stakeholders in addressing the data protection risks	Coordinated approach in addressing data protection risks	Collaboration with stakeholders on data protection entered	No. of collaboration with stakeholders signed	10	2	2	6	1,000,000	1,000,000	3,000,000	
			Build staff capacity on risk management	Enhanced staff knowledge and competencies on risk management	A Well capacitated staff on risk management	No. of staff trained on risk management	30	5	10	15	900,000	1,000,000	2,250,000	
			Identification, assessment, and prioritization of potential risks	Effective mitigation and handling of potential risks	Priority potential risks	Priority potential risks list in place	1	1	0	0	1,560,000	-	-	
			Coordinated and economical application of resources to minimize, monitor, and control the probability and/or	Enhanced staff knowledge and competencies on risk management	A Well capacitated staff on risk management	No. of staff trained on risk management	60	5	10	45	900,000	1,000,000	6,750,000	

Key Result Area	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			impact of unfortunate events											
	Strategic Planning	To align policies with the National Development goals and budget	Conduct quarterly and annual reviews on the implementation of workplans and the Strategic Plan to inform on progress	Enhanced realization of the strategic goals	Quarterly and annual reviews on the implementation of workplans and the strategic plan	Quarterly and annual workplans and Strategic Plan Review reports	3	1	1	1	2,000,000	1,000,000	10,000,000	Data Protection Commissioner, Corporate Services Directorate
			Review policies, legal and regulatory frameworks to align with government priorities	Aligned policies, legal and regulations	Reviewed policies, legal and regulatory frameworks	Aligned policies, legal and regulations in place	3	1	1	1	5,000,000	1,000,000	5,000,000	
			Development and implementation of a MERL framework to enhance effectiveness and efficiency	Effective MERL	Approved MERL framework	MERL framework in place	1	1	0	0	8,000,000	-	-	
											775,300,000	314,170,000	1,432,780,000	

6.1.2 Key Result area: Regulatory Services

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
Regulatory Services	Regulation	To establish an accurate register of data controllers and data processors	Establishment and maintenance of an accurate register of data controllers and data processors	Data controllers and processors are registered	A register of data controllers and processors developed and implemented	% of registered data controllers and data processors	100%	50%	75%	100 %	2,000,000	3,000,000	3,000,000	DPC, Data Compliance Directorate, Registration & Certification Division
			Regulation of the processing of personal data through enforcement of data protection laws	Compliance with the data protection regulations on processing of personal data	Updated register of data controllers and processors	% of data controllers and processors with updated information	100%	10%	75%	100 %	5,000,000	7,000,000	5,000,000	
			Development and issuance of guidelines for regulation of data controllers and data processors	Guidelines developed for regulation of data controllers and data processors	SoPs on regulation of data controllers and processors developed and implemented	SoPs developed and implemented	1	1	0	0	2,000,000	-	-	
			Development and Issuance of guidance notes to data controllers and data processors on Data Protection Impact Assessment	Guidance notes for data controllers and data processors are developed	Compliance guidance notes for data controllers and processors	Guidance notes developed and disseminated to data controllers and processors	1	1	0	0	3,000,000	-	-	
			Conduct regular and random inspections	Compliance with the data protection regulations on processing of personal data	Successful random investigations	Number of successful random investigation conducted	18	6	6	6	5,000,000	5,000,000	5,000,000	
			Receiving, documenting, investigating and resolution of complaints	Complaints management	Receiving, documentation, investigation and resolution of complaints	% level of successfully resolving of complaints received,	100%	100 %	100 %	100 %	3,000,000	3,000,000	3,000,000	

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
						documented and investigated								
			Carry out quarterly and random Audit of Personal Data Processing Systems	Quarterly Audit of Personal Data Processing Systems	Audit guidelines for Personal Data Processing Systems	Audit guidelines developed and utilised accordingly	1	100 %	0	0	2,200,000	50,000	-	
			Review Data Protection Impact Assessment Reports	Review the outcome of the Data Protection Impact Assessment Reports	An analysis of the outcome of the Data Protection Impact Assessment Report	A completed review of the outcome of the Data Protection Impact Assessment Report	100%	25%	75%	100 %	1,000,000	2,000,000	2,000,000	
			Development and implementation of Data Protection Training Curriculum	A Data Protection Training Curriculum	An up to date Data Protection Curriculum	A Date Protection Training Curriculum is developed	1	100 %	0	0	2,000,000	-	-	
			Promotion of Self -Regulation through Inspections and Certification	Inspection and Certification guidelines for Self-Regulation	Inspection and Certification guidelines	% of self-regulated data controllers and data processors	100%	25%	75%	100 %	2,000,000	3,000,000	3,000,000	
			Development and issuance of mark of quality on Processing of Personal Data	A Mark of Quality on Processing of Personal Data	Development and the issuance of a Mark of Quality on Processors of Personal Data	% of data processors issues with a Mark of Quality	100%	25%	75%	100 %	1,000,000	2,000,000	2,000,000	
	Compliance	Enhance Compliance with Data Protection Laws	Auditing of the efficiency and effectiveness of the existing Data Protection Laws and proposing amendments	Assessment of the efficiency and effectiveness of the Data Protection Laws	Establish the efficiency and effectiveness of the Data Protection Laws	An annual report on the efficiency and effectiveness of the Data Protection Laws	100%	100 %	100 %	100 %	1,500,000	2,000,000	2,000,000	DPC, Data Compliance Directorate, Registration & Certification Division
			Designing and implementing a framework for	Rights of data subjects upheld	Data subjects complaints management	Completed framework for	1	1	0	0	500,000	-	-	

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			managing complaints from data subjects		framework developed and implemented	complaints management								
			Development and implementation of Alternative Disputes Resolution Framework	Development of an Alternative Dispute Resolution Framework	Establish an Alternative Dispute Resolution Framework	A completed Alternative Dispute Resolution Framework	1	1	0	0	5,000,000	-	-	
			Development and implementation of a guidelines for monitoring and evaluating personal data processing by data controllers and data processors on enabling the rights of data subjects	Rights of data subjects upheld	Guidelines for monitoring and evaluating personal data processing by data controllers and processors developed and implemented	Guidelines for monitoring and evaluating personal data processing by data controllers and processors in place	100%	50%	50%	100 %	1,000,000	1,000,000	1,000,000	
			Preparation and Issuance of noncompliance notices	Developed non-compliance notices	Non-compliance notices developed	Template non-compliance notices	100%	100 %	100 %	100 %	500,000	500,000	500,000	
			Development and issuance of Guidance Notes on compliance	Developed non-compliance guidance notes	Non-compliance guidance notes developed	Non-compliance guidance notes	100%	100 %	100 %	100 %	500,000	500,000	500,000	
			Development and implementation of inspection guidelines	Consistent and efficient inspections of data controllers and data processors practices on use of personal data	Guidelines for conducting data protection inspections developed	A completed manual with guidelines for conducting inspections	100%	25%	50%	100 %	1,000,000	3,000,000	3,000,000	
			Training of ODPC personnel to	Training of ODPC personnel on	ODPC personnel trained to	Number of ODPC staff trained to	100%	100 %	100 %	100 %	5,000,000	5,000,000	5,000,000	

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			conduct inspections of data controllers and data processors	conducting inspections of data controllers and data processors	conduct inspections	conduct data protection inspections								
			Accreditation of external partners for purposes of conducting self-regulation.	Compliance with the data protection regulations on processing of personal data	List of external partners for conducting self-regulation	Number of accredited external partners for coordinating self-regulation	100%	50%	75%	100 %	1,000,000	1,750,000	1,500,000	
			Development and implementation of system audit framework	Efficient and effective conducting of ODPC affairs	Audit guidelines developed and implemented	% level of implementation of audit guidelines	100%	50%	50%	100 %	1,000,000	1,000,000	-	
	Enforcement	Enhance execution of the process of ensuring compliance with laws, regulations, rules, standards and social norms	Development and implementation of a establish a framework for breach management	Transparency in the management of breaches of personal data	Guide notes for breach notification by data controllers and data processors	% of data breaches reported to ODPC by data controllers and data processors	100%	25%	75%	100 %	2,000,000	2,000,000	2,000,000	DPC, Data Compliance Directorate, Registration & Certification Division
			Development and issuance of guidelines on data breach notification	Awareness of breaches when they happen	Guidelines on data breach notification	A guideline on how to report a breach to the ODPC	1	1	0	0	500,000	-	-	
			Conduct through investigations within the stipulated time frame and communicate findings to concerned parties	Aware of the status of reported non-compliance investigations	Periodic report on non-compliance investigations	% of investigated non-compliant data controllers and data processors	100%	25%	50%	100 %	1,500,000	1,500,000	1,500,000	
			Collaboration with other government agencies to administer	Procedures for serving non-compliance notices to	Template for non-compliance penalty notices developed	A completed template for non-compliance	1	1	0	0	1,500,000	-	-	

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			administrative fines and penalties	data controllers and data processors		enforcement notices								
			Development and issuance of enforcement notices for non-compliance	Enhanced compliance to data protection act	Enforcement notices for non-compliance issued	Number of Enforcement notices for non-compliance issued	1	1	0	0	1,000,000	-	-	
			Preparation and Issuance of penalty notices and compensation notices to concerned parties	Enhanced compliance to data protection act	Penalty notices and compensations notices to concerned parties issued	% level of successfully executing penalty notices and compensations notices to concerned parties	100%	100 %	100 %	100 %	4,000,000	2,000,000	2,000,000	
			Establishment and maintenance of an updated register of noncompliance	Existence of a register of non-compliance	Develop and maintain a register of non-compliance	A regularly updated register of non-compliance	1	1	0	0	1,500,000	-	-	
			Establishment and maintenance of an updated register of complaints	Awareness of the existence of a register of complaints	Develop and maintain a register of complaints	A regularly updated register of complaints	1	1	0	0	1,500,000	-	-	
			Identification and Deregistration of data controllers and data processors for non-compliance	Deregistration guidance notes of data controllers and data processors for non-compliance	Develop of deregistration guidance notes of data controllers and data processors for non-compliance	Guidance notes on the deregistration process of data controllers and data processors for non-compliance	1	1	0	0	1,500,000	-	-	
			Identification and publishing of list of Non-Compliant Data Controllers and Data Processors	Development of a guidance notes to create a template list of non-compliant	Develop guidance notes on the identification and publication of non-compliant data	Guidance notes on the identification and publication of a list of non-compliant data	1	1	0	0	1,500,000	-	-	

Key Result Area	Focus Area	Strategic Objective	Strategy	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
				data controllers and data processors	controllers and data processors	controllers and data processors								
			Obtaining and enforcing Court Orders	Development of a guidance notes on obtaining and enforcing court orders	Develop guidance notes on obtaining and enforcing court orders	Guidance notes on obtaining and enforcing court orders	1	1	0	0	5,000,000	5,000,000	5,000,000	
										Total	66,700,000	50,300,000	47,000,000	

6.1.3 Key Result area: Awareness Creation

Key Result Area	Focus Area	Strategic Objective(s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
Awareness Creation	Training	Empower data controllers and processors through training programmes to enhance compliance with the provisions of the Act.	Development and implementation of a training curriculum	Enhanced compliance of data controllers and processors to the Act	Training curriculum developed and implemented	% Level of implementation of training curriculum	100%	50%	75%	100%	15,000,000	2,500,000	1,250,000	DPC, Research Policy & Strategy Directorate, Advocacy & Collaboration Division, Corporate Communication Division
			Establishment of partnerships with training institutions to roll out training programs		Partnerships with training institutions established	Number of partnerships with training institutions established	30	20	25	30	10,000,000	2,000,000	2,000,000	
			Conducting training on Data Protection targeting data controllers and processors		Training for data controllers and processors conducted	Number of trainings conducted	32	16	8	8	12,000,000	4,000,000	4,000,000	
	Public Outreach	To empower data subjects through strategic initiatives to promote public	Establishment of public awareness initiatives on data privacy and security	Increased public awareness on fundamental	Public awareness initiatives established	% Level of public awareness	90%	30%	70%	90%	35,000,000	4,000,000	2,000,000	DPC, Research Policy & Strategy Directorate, Advocacy &

Key Result Area	Focus Area	Strategic Objective(s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
		awareness of fundamental rights to personal data privacy and protection	Identification and adoption of appropriate communication channels for dissemination of key information on personal data protection	rights to personal data privacy and security.	Key informationdeveloped and disseminated via identified communication channels	Number of key information disseminated	30	20	25	30	15,000,000	5,000,000	5,000,000	Collaboration Division, Corporate Communication Division
			Development of the key messages for dissemination		Key messaging content developed and disseminated	Number of key messaging content developed and disseminated	30	20	25	30	15,000,000	8,000,000	8,000,000	
	Communication	To promote seamless and strategic communication within and among all stakeholders protection.	Development and implementation of communication policy and strategy	Increased public trust	Communication policy developed and implemented	% Level of implementation of communication policy	100%	50%	70%	100%	10,000,000	10,000,000	10,000,000	DPC, Research Policy & Strategy Directorate, Advocacy & Collaboration Division, Corporate

Key Result Area	Focus Area	Strategic Objective(s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
			Regularly updating content on the ODPC website on trends in data protection		Up to date information on trends of personal data privacy and protection	Number of public engagement forums ontrends in personal data privacy and protection	48	24	24	48	30,000,000	12,500,000	12,500,000	Communication Division
			Management of the ODPC visibility on the social media platforms		Social media channels established and in use	Customer Satisfaction index	95%	30	70	95	15,000,000	12,500,000	12,500,000	
			Establishment and operationalization of a customer care service unit		Customer care unit established	Customer Satisfaction index	95%	30	70	95	40,000,000	50,000,000	5,000,000	
										Total	197,000,000	110,500,000	62,250,000	

6.1.4 Enablers: Legal and Policy frameworks; Institutional Coordination framework; Research; and, Partnerships and Collaborations

Enabler	Focus Area	Strategic Objective (s)	Strategies	Expected outcome	Expected output	Output indicators	Targets (3 years)	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
Legal and Policy Frameworks; Institutional Coordination Framework; Partnership and Collaboration; and Research	Legal and Policy Frameworks	Improve the governance of personal data regulatory environment	Development and review of policy, legal and regulatory frameworks on data protection	Enhance personal data protection	Approved legal and policy framework	Legal and policy framework in place	1	1	-	-	20,000,000	-	-	DPC, Research Policy & Strategy Directorate, Advocacy & Collaboration Division, Corporate Communication Division
	Institutional Coordination Framework	Enhance service delivery	Review and implementation of an effective organization structures and staff establishment to address identified gaps in human capital	Efficient internal and external operations on data protection	Approved organization structures and staff establishment	Organization structures and staff establishmentin place	1	1	-	-	10,000,000	-	-	DPC, Research Policy & Strategy Directorate, Advocacy & Collaboration Division, Corporate Communication Division
			Review and implementation of standards operating procedures to reflect changes in technology	Ease of assimilation of new technologies to the operations at ODPC	Assimilated new technologies	Up to date SoPs on technology	3	1	1	1	500,000	500,000	500,000	
			Create and operationalize a reserve fund to finance operational and maintenance expenditure in compliance with the Act	Enhanced operationalsustainability	Approved operational reserve fund	Operational reserve fund in place	1	-	1	-	-	2,000,000	-	
	Partnership and Collaboration	Promote local andinternational cooperation to ensure fulfilment of local andinternational	Establishment of partnerships in the implementation of programmes	Coordinated implementation of programmes	Partnerships and Collaboration in programme implementation	Signed MoUs on partnerships and collaboration	8	5	2	1	1,000,000	1,000,000	1,000,000	DPC, Research Policy & Strategy Directorate, Advocacy & Collaboration Division, Corporate Communication Division
			Cooperation and collaboration with other data protection authorities for	Adoption of good data protection practices	Cooperation with other data protection authorities	Collaborations entered	8	5	2	1	3,000,000	1,000,000	1,000,000	

		obligations in data protection	experience and knowledge sharing											
			Implementation of international obligations on data protection	Compliance with international obligations on data protection	International obligations on data protection implemented	Adopted international obligations on data protection	8	5	2	1	3,000,000	1,000,000	1,000,000	
	Research	To keep pace with emerging trends and practices on personal data protection	Conduct regular targeted research on emerging trends and practices on personal data protection	Keeping pace with emerging trends and practices on data protection	Research findings	Documented Research findings	3	1	1	1	20,000,000	10,000,000	5,000,000	
			Implementation of research findings and recommendations to enhance efficiency and effectiveness	Enhanced efficiency and effectiveness	Research findings and recommendations	Implemented research findings	3	1	1	1	12,500,000	10,000,000	5,000,000	
										Total	70,000,000	25,500,000	13,500,000	

6.1.5 Foundation: Governance and Leadership

Foundation	Focus Area	Strategic Objective(s)	Strategies	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
Governance	Structures	Promote good governance in the regulation of personal data in the country	Develop and institutionalise governance structures that promote good governance for effective operations of the ODPC	Good governance	Institutionalized governance structures	% Level of implementation of the governance structures	100% implementation of good governance structures	50%	75%	100%	100,000,000	50,000,000	50,000,000	DPC, Corporate Services Directorate, HRM&A Division
			Establish a governance framework for the ODPC anchored on the Data Protection Act 2019 to enhance service delivery	Effectiveness inODPC's operations	Governance framework established	% Level of implementation of the good governance framework	100% effectiveness of ODPC operations	50%	75%	100%	100,000,000	50,000,000	50,000,000	DPC, Corporate Services Directorate, HRM&A Division
			Establish and operationalise all the relevant management committees	Operational Efficiency	Constituted relevant managed committees	Management committees in place	Fully constituted management committees	1	1	1	4,000,000	4,000,000	4,000,000	
			Institute reporting and communication channels	Streamlined communications	Reporting and communication channels	Reporting and communication channels instituted	Fully instituted reporting and communication channels	1	-	-	500,000	-	-	
	Oversight Responsibilities	Promote checks and balances to enhance transparency and accountability	Establish oversight roles to effectively manage accountability	Effective management of accountability	Oversight roles established	Oversight roles in place	Fully assigned and consistent execution of oversight roles							DPC, Corporate Services Directorate, HRM&A Division
			Define oversight roles of the management team at the ODPC to enhance accountability	Improved management accountability	Oversight roles	Management oversight roles defined	Fully defined management oversight roles	1	-	-	500,000	-	-	
			Development and implementation of a citizen services charter	Upholding standards of quality, transparency and	Citizen charter	% level of compliance with Citizen charter	100% level of compliance with Citizen charter							

Foundation	Focus Area	Strategic Objective(s)	Strategies	Expected outcome	Expected output	Output indicators	Targets for three years	Target			Budget			Responsibility
								Y1	Y2	Y3	Y1	Y2	Y3	
				accountability										
Leadership/Values	Talent and culture	Promote ethics and integrity	Establish institutional ethical practices, values and cultural principles within the ODPC	Increased public Confidence in ODPC	Institutional ethical practices, values and cultural principles	% Level of adoption of ethical practices, values and cultural principles	100% adoption of ethical practices, values and cultural principles	30%	60%	100%	10,000,000	10,000,000	10,000,000	DPC, Corporate Services Directorate, HRM&A Division
			Develop and implement code of conduct and ethics	Ethical institution	Code of conduct and ethics	Code of conduct and ethics developed and implemented	Approved code of conduct and ethics	1	-	-	2,000,000	-	-	
										Total	217,000,000	114,000,000	114,000,000	

6.2 ANNEX II: MONITORING & EVALUATION FRAMEWORK

6.2.1 *Key Result Area Institutional Capacity Development*

Key Result Area	Output indicators	Target		
		Baseline	Midline	Endline
Institutional Capacity Development	No. of staff recruited	10	192	222
	No. of staff trained on emerging technologies, data protection issues and guidelines	10	1	222
	Organization structure staff establishment in place	1	0	1
	SOPs for HR in place	0	1	1
	Salary grading in place	1	0	1
	Staff benefits framework in place	0	1	1
	ICT policy and strategy in place	0	0	1
	Automated ODPC operations in place	0.25	0.5	1
	Data protection technologies policy in place	0	0.5	1
	No. of MoUs signed and executed	3	6	10
	An ICT preparedness assessment report available	0	1	1
	Standards of the working environment established and adopted	1	0	1
	Working environment plan in place	0	1	1
	Working resources provisioning plan in place	0	1	1
	Staff Support and facilitation procedures in place	0	1	1
	Good financial management practices and guidelines in place	0	1	1
	Financial mobilization policy in place	1	0	1
	% Financial allocation by the National Treasury	55%	90%	100%
	Internal policy on finance utilization end reporting in place	0	0	1
	Policy guidelines on preparation of financial reports in place	0	1	1
	% level adoption of Public Procurement and disposal Act	10%	100%	100%
	Adopt ICT solution in procurement	0	1	1

Key Result Area	Output indicators	Target		
		Baseline	Midline	Endline
	Framework for conducting internal systems audits in place	0	1	1
	Audit committee in place	5	60	120
	Quarterly and annual system audit report	5	5	15
	Implementation status	1	1	3
	Risk management framework in place	0	0	1
	Data protection risk profile in place	0	1	1
	No. of collaboration with stakeholders signed	0	4	10
	No. of staff trained on risk management	0	15	30
	Priority potential risks list in place	0	1	1
	No. of staff trained on risk management	0	15	60
	Quarterly and annual workplans and Strategic Plan Review reports	0	2	3
	Aligned policies, legal and regulations in place	0.5	2	3
	MERL framework in place	0	1	1

6.2.2 *Key Result Area: Regulatory Services*

Key Result Area	Output indicators	Baseline	Target	
			Midline	Endline
Regulatory Services	% of registered data controllers and data processors	0	75%	100%
	% of data controllers and processors with updated information	0	75%	100%
	SoPs developed and implemented	0.5	1	1
	Guidance notes developed and disseminated to data controllers and processors	0.5	1	1
	Number of successful random investigation conducted	0	12	18
	% level of successfully resolving of complaints received, documented and investigated	0	100%	100%
	Audit guidelines developed and utilised accordingly	0	100	100%
	A completed review of the outcome of the Data Protection Impact Assessment Report	0	75%	100%
	Data Protection Training Curriculum is developed	75%	100%	100%
	% of self-regulated data controllers and data processors	0	75%	100%
	% of data processors issues with a Mark of Quality	0	75%	100%
	An annual report on the efficiency and effectiveness of the Data Protection Laws	0	100%	100%
	Completed framework for complaints management	0.5	1	1
	A completed Alternative Dispute Resolution Framework	0	1	1
	Guidelines for monitoring and evaluating personal data processing by data controllers and processors in place	0	50%	100%
	Template non-compliance notices	0	100%	100%
	Non-compliance guidance notes	0	100%	100%
	A completed manual with guidelines for conducting inspections	0	50%	100%
	Number of ODPC staff trained to conduct data protection inspections	0	100%	100%
	Number of accredited external partners for coordinating self-regulation	0	75%	100%
	% level of implementation of audit guidelines	0	50%	100%
	% of data breaches reported to ODPC by data controllers and data processors	N/A	75%	100%
	A guideline on how to report a breach to the ODPC	N/A	1	1
	% of investigated non-compliant data controllers and data processors	N/A	50%	100%

Key Result Area	Output indicators	Baseline	Target	
			Midline	Endline
	A completed template for non-compliance enforcement notices	N/A	1	1
	Number of Enforcement notices for non-compliance issued	N/A	1	1
	% level of successfully executing penalty notices and compensations notices to concerned parties	N/A	100%	100%
	A regularly updated register of non-compliance	N/A	1	1
	A regularly updated register of complaints	N/A	1	1
	Guidance notes on the deregistration process of data controllers and data processors for non-compliance	N/A	1	1
	Guidance notes on the identification and publication of a list of non-compliant data controllers and data processors	N/A	1	1
	Guidance notes on obtaining and enforcing court orders	N/A	1	1

6.2.3 Key Result Area: Awareness Creation

Key Result Area	Output indicators	Baseline	Target	
			Midline	End line
Awareness Creation	% Level of implementation of training curriculum	N/A	75%	100%
	Number of partnerships with training institutions established	N/A	15	20
	Number of trainings conducted	N/A	8	24
	% Level of public awareness	N/A	70%	90%
	Number of key information disseminated	N/A	15	20
	Number of key messaging content developed and disseminated	N/A	15	20
	% Level of implementation of communication policy	N/A	70%	100%
	Number of public engagement forums on trends in personal data privacy and protection	N/A	24	36
	Customer Satisfaction index	N/A	70	95%

6.2.4 Enablers: Legal and Policy Frameworks; Institutional Coordination Framework; Partnership and Collaboration; and Research

Enabler	Output indicators	Baseline	Target	
			Midline	End line
Legal and Policy Frameworks; Institutional Coordination Framework; Partnership and Collaboration; and Research	Legal and policy framework in place	N/A	-	1
	Organization structures and staff establishment in place	N/A	-	1
	Up to date SoPs on technology	N/A	1	3
	Operational reserve fund in place	N/A	1	1
	Signed MoUs on partnerships and collaboration	N/A	2	8
	Collaborations entered	N/A	2	8
	Adopted international obligations on data protection	N/A	2	8
	Documented Research findings	N/A	1	3
	Implemented research findings	N/A	1	3

6.2.5 Foundation: Governance and Leadership/Values

Enabler	Output indicators	Baseline	Target	
			Midline	End line
Governance	% Level of implementation of the governance structures	N/A	75%	100%
	% Level of implementation of the good governance framework	N/A	75%	100%
	Management committees in place	N/A	1	1
	Reporting and communication channels instituted	N/A	1	1
	Oversight roles in place	N/A	1	1
	Management oversight roles defined	N/A	1	1
	% level of compliance with Citizen charter	N/A	75%	100%
Leadership/Values	% Level of adoption of ethical practices, values and cultural principles	N/A	60%	100%
	Code of conduct and ethics developed and implemented	N/A	1.00	100%

6.3 ANNEX III: Regional Office Clusters

	Cluster	Regional Headquarters
1.	Nairobi, Kiambu, Kajiado	Nairobi
2.	Kitui Makueni, Machakos	Machakos
3.	Mombasa, Kilifi, Kwale, Lamu, Taita Taveta	Mombasa
4.	Laikipia, Murang'a, Nyeri, Nyandarua, Kirinyaga	Nyeri
5.	Kisii, Migori, Nyamira	Kisii
6.	Kisumu, Siaya, Homabay	Kisumu
7.	Kakamega, Busia, Vihiga	Kakamega
8.	Trans-Nzoia, Bungoma, Turkana, West Pokot,	Kitale
9.	Uasin Gishu, Elgeyo Marakwet, Nandi	Eldoret
10.	Samburu, Isiolo, Marsabit	Isiolo
11.	Embu, Tharaka Nithi, Meru	Meru
12.	Garissa, Wajir, Mandera, Tana River	Garissa

6.4 ANNEX IV: Proposed Staff Establishment by Role

Cadre	Description	Number
Technical Services	Data Protection Commissioner	1
	Deputy Data Protection Commissioner	6
	Assistant Data Protection Commissioner	18
	Principal Data Protection Officer	31
	Senior Data Protection Officer	31
	Data Protection Officer I &II	31
	Sub Total	**118**
Support Services	Senior Principal Officer	18
	Principal Officer	18
	Senior Officer	13
	Officer I & II	13
	Assistant Officer	7
	Clerical Officer	7
	Driver	7
	Office Assistant	2
	Office Administrator I & II	2
	Security Officer	2
	Personal Assistant	1
	Process servers/Legal Clerks	4
	Sub total	**94**
Total		**222**