Amnesty International Kenya

Amnesty International Kenya Data Protection Report

2021

KENYA AMNESTY INTERNATIONAL

Published by
Amnesty International

Riverside Studios, Riverside Lane
Off Riverside Drive, Nairobi
P.O Box 1527-00606
Nairobi, Kenya

Design, Layout & Printing
Druwashington Limited.

COMPARATIVE STUDY ON DATA PROTECTION REGIMES

AMNESTY INTERNATIONAL KENYA
NAIROBI

Acknowledgements

@Amnesty International Kenya

This comparative research was jointly commissioned by Amnesty International Kenya and the Open Institute.

We acknowledge the Lead Consultant, Henry Maina and his team for the amount of work put into this report. We thank those interviewed for their insights and our staff for interpreting, writing, and editing this report. We retain responsibility for the conclusions reached and invite readers to draw their own conclusions. Engage us and the rest of the country on our insights and call to action.

First Published November 2021

Riverside Studios, Riverside Lane
Off Riverside Drive
P.O. Box 1527 - 00606 Nairobi, Kenya
Tel: +254 020 - 4283000

Email: amnestykenya@amnesty.org
website: www.amnestykenya.org

List of Acronyms

AI:	Artificial Intelligence
CNIL:	Commission Nationale de l'Informatique et des Libertés National Commission on Informatics and Liberty
DDoS:	Distributed Denial of Service
DNA:	Deoxyribonucleic acid which is a complex molecule that contains all of the information necessary to build and maintain an organism.
EAC:	East African Community
EALA:	East African Legislative Assembly
GDPR:	General Data Protection Regulation 2016/679
GoK:	Government of Kenya
GPS:	Global Positioning System
ICO:	Information Commissioner's Office
NIIMS:	National Integrated Identity Management System
OECD:	Organisation for Economic Co-operation and Development
OHCR:	Office of the High Commissioner for Human Rights (UN Human Rights)
ODPC:	Office of the Data Protection Commissioner
OPC:	Office of the Privacy Commissioner of Canada
PIPEDA:	Personal Information Protection and Electronic Documents Act
SA:	South Africa
TOR:	Terms of Reference
UK:	United Kingdom
UK DPA 2018:	United Kingdom Data Protection Act, 2018
UN:	United Nations
UNCTAD:	United Nations Conference on Trade and Development
WFP:	World Food Programme

Executive Summary

Kenya recently set up the Office of the Data Protection Commissioner. This was after the passing and operationalising the Data Protection Act, 2019. This makes it a member of a small club of African states with a comprehensive data protection law and an oversight mechanism. Kenya joined a small club of 25 countries out of the 55 African Union member states.

Data Protection Authorities (DPA) are a cornerstone for any effective regime on protection, promotion and fulfilment of the right to privacy and data protection. DPAs have existed across Europe for over 50 years. In Africa, the first data protection laws are just about two decades and the data protection authorities are even younger.

In setting up the Office of the Data Protection Commissioner, it behoves Kenya to learn from the experiences of its predecessors drawing lessons and shunning pitfalls. The form, structure and functions of DPAs may differ in every jurisdiction but they share one thing in common-they must be formally and functionally independent to be effective.

This study sought to understand the conceptualisation of independence and how it manifests itself around the recruitment, tenure of office and dismissal of data protection commissioners as sole corporations or as members of commissions. It also looks at four other critical areas namely: human resources; funding and financial sustainability; enforcement and complaint handling mechanisms; and implementing regulations. The assessment of these critical components of independence sought to understand and isolate promising practices that can and ought to be emulated by the young Office of the Data Protection Commissioner in Kenya.

We find that the Data Protection Act, 2019 offers sufficient room for formal independence when compared to other similar agencies in Africa and beyond. However, the issue of how best to secure requisite funding will remain a thorny issue lest the ODPC adopts a fees-model to secure its resources.

We note that the Data Protection Commissioner must at all time seek to fulfill the data protection principles.

In sum, we raise a set of recommendations on independence; human resources; funding; complaints handling and enforcement; and regulations that will be necessary for the data protection authority to be credible, legitimate and effective guarantor of data subjects rights.

Table of Contents

Introduction

After about 50 years of development of data privacy law in the world,[1] At last Africa has increasingly started to be involved in the discourse. This is after the states missed being in the arena when the first three waves of legislative activity in data protection happened. Their entry into the arena and uptake of data protection laws in Africa, between 2000-2010, was painstakingly slow, as only 10 countries enacted comprehensive laws during that period.[2] The situation is now fast changing.

The last 10 years, have witnessed 15 more countries passing their laws including Gabon (2011), Angola (2011), Ghana (2012), Lesotho (2012), South Africa (2012), Mali (2013), Côte d'ivoire (2013), Madagascar (2014), Chad (2015), Equatorial Guinea (2016), Malawi (2016), Sao Tome and Principe (2016), Kenya (2019), Uganda (2019), and Egypt (2019).

Thus, the last two decades have witnessed Africa develop about 25 comprehensive data protection laws. Over 10 other countries have drafted legislations at different levels of enactments and five others have some laws and regulations that deal with sectoral data protections issues. Therefore, it is now clear that personal data protection is increasingly gaining its popularity and legal recognition in many jurisdictions around the world including Kenya. But one may ask why the increased rate of adopting data protection laws in Africa?

Most of the countries that have adopted comprehensive data protection laws have done so based upon their intrinsic merits. Similarly, technological developments and their attendant challenges of ensuring privacy and consumer protection of users have played a key role. Other influences have been regional instruments and international standard setting processes that have drawn attention to the desirability of compatible data protection regimes in the context of regionalisation and globalisation.[3]

The Data Protection Act, 2019 (The Act) was adopted by the National Assembly and assented to by the President of Kenya on 8 November 2019. It came into force on 25 November 2019 and is now the primary statute on data protection in Kenya. It gives effect to Article 31 (c) and (d) of the Constitution of Kenya, 2010. The law provides coherent guidance on the collection, storage, processing, dissemination and transfer of personal data in Kenya as well as legal recourse following the misuse of the same.

Kenya's first Data Protection Commissioner, Ms Immaculate Kassait, assumed office on November 16, 2020, to oversee the implementation of Data Protection Act, 2019, after almost a year of a lull.

1.1 Study Objectives

The overall objective was to undertake a comparative study that seeks inter alia to inform the establishment of an independent but functionally efficient and effective Data Protection Authority in Kenya. Specifically, it spells out six key tasks:

- Map out the best practices in establishing a financially and functionally independent Office of Data Protection Commissioner;
- Identify the best practices in funding and budgets for the Office of Data Protection Commissioner;
- Establish the requisite human resource capacity and skills required by the Office of the Data Protection Commissioner for the implementation of the Act;
- Outline, establish and compare complaints and enforcement mechanisms in other jurisdictions with a view to presenting the best practices;
- Identify regulations under section 71 necessary to give full effect to the Data Protection Act; Establish best practices for implementation of the Data Protection Act in a manner that promotes data governance and responsible use of data.

1. The genesis of modern legislation in this area can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), USA (1974), New South Wales (1975), New Zealand (1976), Germany (1977), and France (1978)

2. Cape Verde (2001), Seychelles (2003), Burkina Faso (2004), Mauritius (2004), Tunisia (2004), Senegal (2008), Morocco (2009), Benin (2009), Gambia (2009), Zambia (2009).

3. See, for example, United Nations General Assembly, Guidelines for the Regulation of Computerised Personal Data Files, 14 December 1990, and International Labour Office, Code of Practice on the Protection of Workers' Personal Data, November 1996.

1.2 Methodology

To conduct the study we deployed a comparative case study methodological approach and used a mixed research method to produce generalisable knowledge about causal questions-how and why particular approaches in constituting, funding and working of Data Protection Authorities (DPA) work or fail to work.

We selected a case studies approach as it was not feasible to undertake an experimental design. Interviews and document analysis were the main methods of data collection.

We accessed and assessed both primary and secondary data to analyse and synthesise similarities, differences and patterns across two or more cases. We used both qualitative and quantitative analyses to understand the designs of Data Protection Authorities (DPA) and their equivalents on what constitutes 'independence,' and how best DPAs have secured their funding, budgets and human resources.

1.2.1 Methods of Data Collection

We developed key informant interview guides and self-administered questionnaires and had them filled with purposely sampled respondents in five jurisdictions-Mauritius, South Africa, Canada, Ghana, and the United Kingdom. A separate interview guide was filed with the Kenya Data Protection Commissioner and experts in the country. The questionnaire annexed has five clear questions that broadly define the five areas of research and the data to be collected.

1.2.2 Sampling

Globally, 132 out of 194 countries have put in place legislation to secure the protection of data and privacy. We sampled countries for comparison purposes (the number was reduced or increased depending on the issue during the study). In identifying the comparators, we picked three African states (Mauritius (2004), Ghana (2012) and South Africa (2013), one European (UK) and one from the Americas (Canada (1985,2000). The choice of these countries and their respective data protection authorities was informed by the fact that they have relatively long years of experience and established a community of practice on the issue of data protection. Canada is also one of the few non-European Union countries that have received an adequacy protection determination, allowing transfer of personal data from EU to Canada for processing. Later on we included Australia (1988 and amended in 2004) and France (1978 and amended in 2004).

Given that the comparative research is on thematic areas, we purposely sampled any other countries as was relevant for this research and where data was readily available.

1.2.3 Limitations to the study

It was not feasible to draw lessons from all 132 countries because of limitations of time and resources. Further, due to Covid-19 social distancing restrictions, we were not able to do field visits and conduct observation sessions of different DPAs which would have offered opportunities to gain insights on the context and what makes certain policy or designs of the DPA work or not work. We therefore make generalisations from document analysis and interviews even as their levels of reliability may be a bit low.

2.0 Forms and Structures of Data Protection Authorities

A significant feature of nearly all successful data protection laws is an independent data protection supervisory authority (referred to in this study as a "Data Protection Authority" (DPA). The existence of such an authority is seen by most informed commentators as being a highly desirable, if not essential feature of an effective information privacy or data protection regime.

For instance, Article 28 of the EU Directive requires member countries to have an independent supervisory authority as does the Protocol to the Council of Europe Convention.[4] European Union scrutiny as to the "adequacy" of data protection in third countries is likely to have regard to the existence or absence of a national data protection authority.[5] Similarly, the African Union Convention on Cyber Security and Personal Data Protection in Article 11(1) requires each member state to establish an independent administrative authority to be in charge of protecting personal data.[6]

This study brings together some basic information as to the organization and role of DPA by reference to those already in existence and to EU, AU and UN instruments. It should not be assumed that existing DPAs are identical. DPAs in South Africa, Ghana, Mauritius, Hong Kong, Canada, Australia and New Zealand differ from their European counterparts in various ways.

Even within Europe there is a variety between populous states like the UK and France and small jurisdictions such as some of the Swiss cantons, the Isle of Man, and the Channel Islands (each of which has a DPA). Although the Data Protection Commissioners in Germany work in one of the world's wealthiest countries, the same cannot be said of the Data Protection Ombudsman in neighbouring Hungary.

Accordingly, there is already a broad range of experience to draw upon in designing new DPAs. Clearly, "one size fits all" cannot apply in the diverse African region which encompasses tiny Indian Ocean islands and the populous nations like Nigeria, Ethiopia and Sudan.

Nonetheless, study of the form and function of existing authorities is likely to be a useful starting point in the task of considering what might be adopted locally.

This part of the study presents some simple comparative information concerning the form of data protection authorities. The information is intended to be a starting point for jurisdictions that do not yet have a data protection authority which may wish to find answers to;

- **How are data protection authorities typically structured?**
- **What features do existing data protection authorities have in common and how do they**
- **differ?**
- **How have agencies been structured to guarantee their independence as human rights institutions and to perform the various tasks placed upon them?**

2.1 Main Structural Models

In setting up a new Data Protection Authority, there are a range of choices available to any government. The most common options involve vesting authority in:

- A single individual- typically called a "commissioner";
- A group of appointed individuals-typically called a "commission";
- An agency with additional functions compatible with data protection

Drawing from Blair Stewart paper, [7] this study discusses these and mentions two variations: a commissioner with a committee and contracting the services of another jurisdiction's DPA.

2.1.1 The Commissioner Model

The Commissioner model is probably the most widely used. It is found throughout Europe, Canada, Australia and in Hong Kong. It is the model adopted by Mauritius and Kenya but with some slight modifications.

Data protection laws using the Commissioner model provide for appointment of a Commissioner who establishes an office and employs staff to undertake the work. Some laws provide for the appointment of a deputy to undertake particular functions or to share the load generally. The Commissioner may delegate functions to staff.

The most common titles are "Data Protection Commissioner" or "Privacy Commissioner." Occasionally "Data Protection Ombudsman" or "Data Protection Registrar" have been adopted highlighting the complaint/investigation and registration functions respectively.

In jurisdictions where the functions are combined with freedom of information responsibilities, the title sometimes given is "Information and Privacy Commissioner."

The Commissioner model as described above may be judged to have four main advantages. First, having a single individual in charge allows for rapid appropriate reaction to data protection challenges and may avoid formalism. This then allows for high levels of flexibility and responsiveness. Second, a commissioner may develop a strong public profile to champion data protection. This leads to personification of data protection in a public figure. Third, the model can meet the needs of both large jurisdictions and very small ones. Fourth, there is no need for consensus of a committee or to await formal resolutions or periodic meetings. This results in simplified decision making processes.

However, the commissioner model also has its disadvantages. The main areas of concern are that: the effectiveness of the office will depend upon a good choice of Commissioner. If the country ends up with one who does not adequately perform then poor performance may impair the effectiveness of the law and tarnish the reputation of staff and successors. Second, a single commissioner can act as a bottleneck preventing the timely completion of the office's work. This challenge can most of the time be ameliorated by the use of delegation powers and competent deputy commissioners where they exist. The third disadvantage is that the personification of data protection in a single individual can encourage stakeholders to bypass institutional procedures to deal directly with the Commissioner.

2.1.2 The Commission Model

A data protection law using this model will provide an appointment process for members of a Commission.

4. Cate, Fred H. "The EU data protection directive, information privacy, and the public interest." Iowa L. Rev. 80 (1994): 431.

5. Schwartz, Paul M. "European data protection law and restrictions on international data flows." Iowa L. Rev. 80 (1994): 471.

6. African Union Convention on Cyber Security and Data Protection

7. Blair Stewart, "A Comparative Survey of Data Protection Authorities-Part 1: Form and Structure," Privacy Law and Policy Reporter 11,no.2 (2004).

All powers and functions conferred by the law are then to be exercised by the Commission although there will usually be power for the Commission to delegate particular functions to a presiding or other member, a sub-committee of the Commission or to staff.

Commissions may include a mixture of full time and part time members and terms of office may start and finish on different dates. The law may specify that certain constituencies are to be represented or that the appointment process ensures a mix of expertise relevant to a range of data protection functions.

The other title used to refer to the Commission is "the Board." The Commission model has been adopted in Sweden, France, South Korea, and Ghana just to mention but a few. The province of Quebec in Canada also works with the Commission model.

Five principal advantages of the commission model can be gleaned from the countries that adopted it. First, is the ability for the commission to obtain a range of specialist expertise which would necessarily be contained in a single Commissioner. Second, this model allows genuine representation of stakeholders relevant to data processing such as individuals or consumers, data holders, government, academics and business. Third, decision-making is by consensus and thus brings on board different perspectives and worldviews. Fourth, given the issue that different members of the commission have different start and exit dates, there is development and retention of institutional knowledge notwithstanding the change in individual membership from time to time. Fifth, the ability for constant renewal through the addition of replacement membership ensures higher performance and reduces cases of lethargy.

The Commission model too has some disadvantages. First, the expenses of maintaining a large committee of decision makers compared with a single Commissioner can be too high. Second, the model tends to allow for elaborate bureaucracies and inefficient decision making. Third, there is a high likelihood of disagreement and stalemate on contentious issues. Fourth, there is a difficulty of presenting a "public face" of data protection instead of a faceless committee. Sometimes this challenge is mitigated by emphasising a leading member of the Commission, such as a President or Chief Commissioner.

2.1.3 Multipurpose Agencies

Some jurisdictions have found it convenient to combine the functions of a DPA with other related or compatible functions. The motivation for combining the functions into a multipurpose agency usually relates to the cost of establishing separate agencies and perceived savings and synergies of a combined operation. Governments sometimes believe that the data protection oversight can be enhanced through bringing relevant information-related functions together.

The commonest combining of functions relates to the bringing together of data protection and freedom of information (FOI) oversight functions. Examples worth noting include, South Africa, United Kingdom (UK), Hungary, several Länder in Germany and in several Canadian provinces.

In some jurisdictions, data protection functions have been conferred upon existing Ombudsmen. For instance, in Manitoba and New Brunswick, the Ombudsmen receive privacy complaints under the provinces' privacy laws and carry out the other functions of a data protection agency.[8]

Consideration has been given in Australia to the desirability of combining some functions under public archives law with those of privacy and freedom of information.

Although not seriously considered for any major jurisdiction, the model is being pioneered in Northern Territory Information Act, 2003 which created an Information Commissioner with combined functions.

Some jurisdictions have adopted sectoral data protection laws. These are not generally addressed in this study. Such jurisdictions have found it appropriate to confer data protection functions such laws upon existing sectoral regulatory or complaints bodies. For instance, conferring data protection oversight functions upon existing bodies set up to receive consumer complaints about health services.

In the USA, the Federal Trade Commission has an education and enforcement role in respect of several major sectoral privacy laws as well as general trade and consumer protection functions.

In several jurisdictions, the national data protection agency may receive complaints but a role is assigned to judicial body to hear appeals or give binding determinations in cases which cannot be settled. Sometimes such bodies hear other cases as well especially where there is insufficient workload to justify a specialist tribunal. For example, in New Zealand complaints under the Privacy Act can ultimately be taken to a Human Rights Review Tribunal which, in addition to its privacy workload, determines proceedings alleging other breaches of human rights or health consumer rights.[9]

The multipurpose agencies are perceived to have a number of advantages. First, the potential of saving a lot of financial resources through the avoidance of establishing new oversight agencies. Second, this model permits the existence of larger agencies possessing broader expertise with better coordination between related jurisdictions. Third, the models works better or is more suitable for very small jurisdictions for which data protection workload does not readily justify establishing a separate body.

Multipurpose agencies have two main disadvantages:

the loss of clear data protection focus; and inefficiencies through the need for staff to become familiar with a range of functions, not all of which closely inter-relate.

2.2 Variations on the Models

Data Protection Authorities are sometimes established with elements of both the Commissioner and Commission models. The most common example is where the law establishing a commissioner also sets up an advisory committee to assist.[10] This approach seek to graft some of the advantages of a Commission, particularly the breadth of specialist expertise, onto a Commissioner set up.

Some jurisdictions with privacy laws sometimes do not establish their own Data Protection Authority but instead arrange for an agency established in another jurisdiction to undertake some or all of the functions associated with the DPA. This occasionally happens in federal jurisdictions where a State may contact a Federal DPA to receive and investigate complaints concerning a breach of data protection rules. An example is the Australian Capital Territory where the Australian Federal Privacy Commissioner provides services under contract to the State. It has been reported that Gibraltar, a UK colony, had considered a similar arrangement with the UK Information Commissioner.[11]

3.0 Independence of Data Protection Authorities

Data protection and privacy are often subject to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including protecting individuals' rights. The Data Protection Authorities have different and varied functions depending on the mandate bestowed on them by their founding statutes. But most of them largely take complaints, issue rulings, issue warnings, set rules, conduct audits, make reports, impose sanctions, and ensure the public access to information by being a registrar of all data controllers' processing activities.

The supervisory authority might be a single government official, ombudsman or a body with several members. Independence does mean that data protection authorities ensure the observance of the relevant laws free from the interventions of executive power.[12]

Two essential features of data protection supervisory authorities are autonomy and independence. Autonomy requires that an agency be empowered, both in legal and practical fashion, to initiate and undertake appropriate data protection work without having to seek the permission of another agency.

The need for independence relates to the subject matter with which the agencies deal-enforcement of human rights and taking measures to ensure that agencies comply with data protection controls.

It is important for DPAs to be able to operate free from political interference and to withstand the influence of vested interests.

Parallel to the development of national supervisory authorities under data protection law, have been the establishment and operation of national institutions implementing human rights generally-often called "human rights commissions." The UN Commission on Human Rights endorsed the Principles relating to the Status and Functioning of National Institutions for the Protection and Promotion of Human Rights (the "Paris Principles") in 1992.

These set out guarantees for the independence of national human rights institutions and of certain other matters relating to such institutions' competence, responsibilities, and methods of operation.

The centrality of autonomy and independence among other principles to any DPA are also reiterated by the Global Privacy Assembly (previously International Conference of Data Protection and Privacy Commissioners up to 2019) accreditation principles.[13]

To better understand the concept of independence, we borrowed from Gilardi's[14] independence index which has five group of indicators namely the agency's head status; the management board member's status; the general frame of the relationship with government and the parliament; financial and organisational autonomy;

8. See Freedom of Information and Protection of Privacy Act, 1998 and Personal Health Information Act, 1998 (Manitoba) and Protection of Personal Information Act, 1998 (New Brunswick).

9. The Human Rights Review Tribunal hears proceedings under the Privacy Act,1993, Human Rights Act, 1993 and the Health and Disability Commissioner Act, 1994 (New Zealand).

10. See for example Privacy Act, 1988 (Australia), Part VII and Personal Data (Privacy) Ordinance 1995 (Hong Kong), s.11.

11. Data Protection Act, 1998 (UK), s.54 (5).

12. For similar arguments see Annetje OTTOW, 'Independence of national supervisory authorities', Europa Institute Working Paper 2002/10,3.

13. Section 5.1 (e) Global Privacy Assembly, Rules and Procedures, Nov 2019, available at

14. Gilardi Fabrizio, "Independent Regulators" (Paper presented at the Organisation of Economic corporation and Development, Designing Independent and Accountable Regulatory Authorities for High Quality Regulation, Working Party on Regulatory management and Reform, Proceedings of an Expert Meeting, London, United Kingdom, 2005,) 102.

and the extent of delegated regulatory competencies or degree of exclusive regulatory power by the agency. The independence of the national data protection authority is generally achieved by circumscribing in law 11 key areas namely:

- Establishing the agency by primary legislation;
- Statute provisions relating to the appointment and removal from office;
- Providing clear term of appointment/tenure of office.
- Requirement that the DPA reports directly to the legislature;
- Provision for an administrative structure recognised in the jurisdiction as being appropriate for an independent agency;
- Provision that clearly constrain commissioners from carrying out other business or professions for the duration of appointment;
- A funding mechanism which affirms the need for independence;
- A provision to ensure immunity against personal lawsuit for actions carried out as part of official duties;
- Clear protection against remuneration being subject to political control;
- An ability for Commissioners to speak publicly on matters of concern; and
- An explicit statutory direction to act with independence.

In the next part of the study we elaborate on the recruitment process, removal from office and terms of office for the data protection authority.

3.1 Recruitment / Appointment Process

There are quite a variety of approaches taken in appointing data protection authorities as these depend upon national traditions and laws. Two common examples are: appointment by the legislature; and appointment by the head of state (the executive).

In a number of Parliamentary jurisdictions, the data protection authority is appointed as an Officer of Parliament. This approach is taken in many of the Canadian provinces. Sometimes the legislature does not actually appoint the Commissioner but has a role in nomination, approval or objection.

Each of the appointment approaches has its advantages and disadvantages. Three advantages are discernible from the legislative appointment process. First, the appointment processes by the legislature confers prestige and status upon the office. Second, the process tends to earn the appointee a high degree of public and parliamentary confidence. Third, there is an enhanced relationship between the data protection authority and the legislature.

However, the legislative appointment process can be encumbered by partisan political interests (politicisation of the appointment) leading to delays in appointment if there is a political deadlock.

Another common process is appointment by the head of state. For example, the UK Information Commissioner is appointed by the Queen by *Letters Patent*.[15] Letters of patent are a legal instrument of the head of state used without the need to seek the approval of the parliament. Similarly, in New Zealand and Australia, the Privacy Commissioners are appointed by their respective Governors-General.[16]

The Kenyan Data Protection Commissioner is nominated and, with approval of the National Assembly, appointed by the President of the Republic of Kenya. Prior to the nomination, the The Kenyan Data Protection Commissioner is nominated and, with approval of the National Assembly, appointed by the President of the Republic of Kenya.[17] Prior to the nomination, the President receives three qualified applicants in the order of merit for the position from the Public Service Commission, an independent constitutional commission that is charged with the responsibility of recruitment.

Given the above discussed approaches the appointment process of the Data Protection Commissioner in Kenya is a hybrid approach that borrows the strength of both a legislative led and head of state led recruitment processes. It also opens up the recruitment and ensures transparency by requiring public advertisement for the vacancy and publishing and publicising the names of applicants and the short listed applicants.

3.2 Removal from Office

High level appointment provisions, such as those by the legislature or head of state, are usually accompanied by special provisions allowing removal in appropriate cases. The appropriate cases are circumscribed by law, so as to prevent the removal, or threat of removal, for political or other improper purposes.

The precise reasons and the way they are expressed depend upon the legal tradition and the particular jurisdiction.

Typically they include: general inability to perform the duties of the office or neglect of duty; specific physical, mental, or legal disabilities preventing the office holder performing the duties of office (including, for instance, bankruptcy or being absent from the jurisdiction for an excessively long period); serious "misbehaviour" or "misconduct" which are given a strict, and limited, legal meaning in most jurisdictions.

Usually, if an appointment is made by the legislature or head of state, then dismissal or removal is by the same body. Sometimes where the appointment is by

the head of state, a role is nonetheless accorded for the legislature in the removal process. This is done to enhance the independence of the data protection authority and to emphasise the careful scrutiny that will be given before the termination of an appointment. For example, the Hong Kong Commissioner appointed by the Governor who may also remove the Commissioner. However, removal may only be done with the approval of the Legislative Council.[18]

The Information Commissioner in the UK can be removed at her/his own request or by the Crown. The dismissal by the Crown can only take effect in pursuance of an Address from both Houses of Parliament, [19] only if he/she is guilty of serious misconduct or he/she no longer fulfils the conditions required for the performance of her functions.[20]

A similar case obtains in Canada where the Privacy Commissioner holds office during good behaviour but may be removed for cause by the Governor in Council (Federal cabinet) at any time on address of the Senate and House of Commons.[21] In determining, whether there is a cause for dismissal, the cabinet is entitled to "assess whether the conduct of the [appointee] was consistent with the terms of his appointment to that office, including, in its judgment whether his conduct could undermine public confidence in the federal institution with which he had been appointed to serve." [22]

In the case of the Information Regulator in South Africa, a member can only be removed after the committee of the National Assembly makes a finding of misconduct, incompetence or incapacity. For the President to effect the removal, the National Assembly must pass such a resolution with a supporting vote of a majority of members of the National Assembly.[23]

In Mauritius, the Data Protection Act, 2017 is silent on the grounds and procedures of removal of the Data Protection Commissioner.

In Ghana, a member of the board may be removed through a letter from the President revoking the appointment[24] or when a minister determines that a member is for sufficient reasons unable to discharge their functions.[25] Compared to other jurisdictions, the removal process in Ghana allows for whimsical dismissal of members without any legitimate and verifiable reason like gross misconduct, bankruptcy, incompetence or incapacity.

This rather open provision for the President to remove a member was invoked by President Nana Akufo-Addo and he removed the pioneer Data Protection Commissioner/Executive Director, Ms Teki Akuetteh Falconer, in early 2017. The removed Data Commissioner has lodged a case in the High Court challenging her removal and seeking reinstatement.[26] The case is yet to be determined.

The removal process for the Data Protection Commissioner in Kenya, though not as insulated as in South Africa, UK and Canada, requires that a formal complaint be lodged with the Public Service Commission setting out the alleged facts constituting any of the five grounds of removal. [27] The Public Service Commission shall inform the Data Commissioner, in writing, of the reasons for the intended removal; and offer an opportunity to put in a defence against such allegations. [28]

After such notification, the Public Service Commission after consideration of the complaint and satisfactorily finding that the complaint discloses a violation of any of the five ground (inability to perform the functions, non-compliance with Chapter six of the Constitution of Kenya, bankruptcy, incompetence, or gross misconduct) shall expeditiously investigate the matter, report on the facts, and make a recommendation to the Cabinet Secretary.[29]

It is our finding that to ensure independence, the process of removal of a commissioner or a member of the commission must be clearly provided for in the primary legislation, spelling out the grounds of removal (a clear cause), offer an opportunity for an independent, credible and transparent investigatory process for the alleged crimes or breaches, and offer an opportunity for the National Assembly to vote on the resolution for removal.

15. Data Protection Act, United Kingdom, part 1, para.6, subpara.2.

16. Privacy Act 1993 (New Zealand),s. 12, and Privacy Act,1988 (Australia),s.19.

17. Data protection Act, 2019 (Kenya), s.6 (4).
18. Personal Data (Privacy) Ordinance, 1999, S. 5 (5).

19. Data Protection Act, United Kingdom, schedule 5, para.2, subpara.3.

20. Data Protection Act, UK, Sch 13 para.1

21. Interview with Daniel Therrien, Privacy Commissioner of Canada.

22. Wedge v. Canada (Attorney General), 1997 CanLII 5331 (FC)

23. The Protection of Personal Information Act, 2013 (South Africa), s. 41(6)

24. Data Protection Act, 2012 (Ghana), s. 5 (5)
25. Data Protection Act, 2012 (Ghana), s.5 (6).

26. Nyaaba Felix Engsalige, "Former CEO of Data Protection Commission sued Govt after Supreme Court Ruling," Modern Ghana, Published on July 2, 2019, available at , <accessed on February 17, 2021>.

27. Data Protection Act, 2019 (Kenya), s.11-12
28. Data Protection Act, 2019 (Kenya), s.12
29. Data Protection Act, 2019 (Kenya), s.12

3.3 Terms of Office

With regard to term of office, Section 2 of the Data Protection Act, 2019 guarantees that the "Data Commissioner shall be appointed for a single term of six years and shall not be eligible for reappointment. This guarantee compares well to the terms of office of different Data Protection Commissioners from the UK, Canada, South Africa, Ghana and Mauritius.

The UK Information Commissioner (Information Commissioner) is appointed by the Crown on recommendation from the Government. The Department of Digital, Culture, Media and Sport (DCMS) is the Information Commissioner's sponsoring department within government. The Commissioner is a corporation sole and can hold office for up to a single non-renewable term of 7 years. [30] The Commissioner and the staff are not to be regarded as servants or agents of the Crown.[31]

Similarly, the Canadian Privacy Commissioner holds office for a 7 year term but can be renewed more than once.

The Information Regulator in South Africa consists of the chairperson and four others who hold office for a period of five years. The law is silent on whether their mandate is renewable or not.

In Ghana, the president appoints the Executive Director (Commissioner) on a permanent full time contract.[32] Ten members of the board, including the chairperson, are appointed on a three year term.[33] Members of the board may be eligible for a non-renewable second term too.[34]

In Mauritius, the Data Protection Commissioner is recruited by the Public Service Commission and appointed by the President on a permanent basis just like that of Ghana. The current commissioner was appointed in 2007. The chairperson, deputy chairpersons and the Commissioner are appointed by the President of the Republic of Mauritius after consultation with the Prime Minister and the Leader of Opposition.[35] The Public Service Commission recruits and appoints the officers of the Data Protection Authority.

Data Protection laws frequently stipulate the maximum term. This is intended to be sufficiently long to ensure the appointee's independence. Many, but not all, jurisdictions allow for renewals or reappointments. Some allow only one extension of term. A few have a commissioner appointed on permanent terms like is the case in Ghana and Mauritius.

From the jurisdictions analysed, the terms of office of the Kenyan Data Protection Commissioner compare well with all the others. Common terms appear to range from 3-7 years. Kenya has a single non-renewable term of 6 years.

3.4 Functions of Data Protection Authorities (Regulatory Competencies)

Depending on the jurisdiction, data protection authorities have well defined functions and regulatory responsibilities and competencies. Four most common of the responsibilities include: *investigative powers* such as powers of access to data forming the subject matter of processing operations and powers to collect all the information necessary for the performance of supervisory duties; *effective powers of intervention* such as that of delivering and publishing opinions before especially risky processing operations are carried out; ordering the blocking, erasure or destruction of data; imposing bans on processing; warning or monitoring controllers; referring matters to national parliaments or other political institutions; *the power to engage in legal proceedings* where data protection laws have been violated; and the power to act as an adjudication forum that can hear and determine data protection related complaints by individuals and representative groups.

For accountability, most jurisdictions provide that the decisions by the data protection authorities may be appealed against through the courts or specialist tribunals as in the United Kingdom. Also, the DPAs are required to regularly report on their activities to the national assemblies or ministries or heads of state.

Notwithstanding similar core responsibilities, it is probably the case that no two DPAs have identical mandates. However, some typical functions can be highlighted. These include:

- Compliance
- Educational
- Individual redress
- Legislative reporting
- Public reporting
- International cooperation
- Specialist advice and research

Independence is a multi-faced and complex concept whose full assessment requires taking into account both quantitative and qualitative variables most notably the process of operationalisation.

In sum, formal independence from government actors may be measured using quantitative methods but there is need to expand the analysis to include informal sources of influence beyond legal provisions such as politicisation and revolving doors. This is because these informal aspects are decisive in determining the de facto independence of Data Protection Authorities. In agreement with Gilardi and Maggetti, we add that it is also crucial that some DPAs can be independent in practice without being independent on paper. [36]

Independence is also a problem. In many countries, the agency is under the control of the political arm of the government or part of a Ministry of Justice or ICT and lacks the power or will to advance privacy or criticise privacy invasive proposals. For example Japan and Thailand, the oversight agency is under the control of the Prime Minister's Office.

The need for independence for the operation of DPAs remains a key concern globally given that governments sometimes have sought to influence their work. A case in point is the resignation en masse of the entire Greek Data Protection Commission in 2007 and the removal of the Executive Director/Commissioner in Ghana by the new government.

4.0 Human Resources

To understand the human resources requirements of the data protection authorities, the study sought to know three main things: whether the head of the DPA is empowered by law to recruit and manage own staff; how many staff some of the sampled DPAs may have; and how they are organised for efficient and effective delivery of their functions. We highlight the situation of a few DPAs. We start with the Swedish Authority for Privacy Protection, thought to be the oldest DPA in the world. It is a single purpose commission - it protects privacy. Its initial formations were started in 1973. We then follow up with a highlight of the human resources complement of the respective DPAs in Mauritius, UK, and South Africa. For Ghana we only highlight what the law provides.

Figure 1: Preliminary findings on formal independence of DPAs

	Law	Appointment	Dismissal	Reporting	Funding	Attachment
United Kingdom	1983	Executive	Parliament (both Houses)		Notification fees Ministry of Justice+ House of Commons	Administrative and financial attachment to Ministry of Justice
Sweden	1973	Executive	Special committee with Judges	Ministry of Justice	Government (Ministry of Justice)	Close attachment to the Ministry of Justice
Canada		Executive & Parliament	Executive& Parliament	Parliament	Government	No attachment
Mauritius	2004 (2017)	Executive	Executive	Parliament	Ministry of Technology, Communication & innovation	Close attachment to the Ministry of Technology, Communication & Innovation
South Africa	2013	Parliament	Executive & Parliament	Parliament		Attached to Ministry of
Ghana	2012	Executive	silent	Minister of Communication	Ministry of Communication	Administrative & financial attachment to the Ministry of Communication
Kenya	2019	Executive & Parliament	Executive		Parliament	Administrative & financial attachment to Ministry of ICT

30. Data Protection Act, 2018 (United Kingdom) Schedule 12 Para 2(4).
31. Schedule 12 paragraph 1 UK DPA 2018
32. Ghana Data Protection Act, 2012 Section 11 and Constitution of Ghana, Article 195.
33. Ghana Data Protection Act, 2012 section 9 (1)
34. Ghana Data Protection Act, 2012 section 5 (1)
35. Section 88 of the Constitution of Mauritius (as amended by act No 5 of 1997)

36. F. Gilardi and M. Maggetti, "The independence of regulatory authorities," in Handbook on the Politics of Regulation,ed D. Levi-Faur (Cheltenham: Edward Elgar, 2012,2.

The Swedish Authority for Privacy Protection is the supervisory authority under the respective national laws and other regional instruments that the country is a state party to.[37] Headed by the Director General (DG), the Swedish Authority for Privacy Protection employs about 95 employees, most of whom are lawyers.[38] The staff unit and six programmatic directorates for the core of the staff under the leadership of the Director General, management team which includes a Director for Legal Affairs and the International Cooperation and EU department.

The six directorates are: unit of Authorities, care and education; unit of Information Security and Supervision Process; Unit of Trade and Industry and Working Life; Unit of Legal System, Defence and Camera Surveillance; Administrative Unit; and Unit for Communication and External Relations. The number of staff has grown exponentially given that 7 years ago, the then Swedish Data Inspection Board, had just 40 employees.[39]

In Mauritius, the Office of the Data Commissioner is not empowered to recruit its own staff. The law provides that "the Commissioner shall be assisted by such public officers as may be necessary."[40] It is only after such public officers have been recruited and deployed to the Office of the Data Commissioner, that the Commissioner shall have administrative control over them.[41]

As of February 12, 2021, the Office of the Data Protection Commissioner in Mauritius has a total of 11 key staff. The office is organised in five units: the Commissioner's office (2 officers); Data Protection Officer's Unit (4 officers); the Registry Unit (4 officers); the Finance/Cash Office Unit (1 officer); and the IT unit. This includes the Data Protection Commissioner, Confidential Secretary, three management support Officers working in the registry, two office assistants, one assistant system analyst (seconded from CISD), one assistant finance officer, one principal data protection officer and 3 data protection officers.[42]

While the Mauritian Data Protection Commissioner's office is one of the oldest in Africa it still suffers from lack of requisite personnel 14 years after it was inaugurated.[43] Current staffing levels are skeletal as the office lacks officers to assist in undertaking investigations, prosecutions and legal or policy work as the Data Protection Commissioner is the only legal practitioner in the team of 11 key staff. Even the current skeletal team seems not to have clear terms of service and as such the office has kept losing two or more officers annually.[44] Clearly, the Mauritian Data Protection Authority suffers lack of requisite staff and it does not have any discretion in influential domain of personnel policy.

While we were not able to get timely responses on the human resources complement of the Data Protection Office in Ghana, the case of the dismissal of the pioneer Commissioner-cum-Executive Director is worth a mention. Advocate Teki Akuetteh Falconer who served as the first Executive Director of the Data Protection Commission of Ghana and facilitated implementation of Ghana's Data Protection Act was dismissed in July 2017 by the new administration of President Nana Addo Dankwa Akufo-Addo. She has lodged a case at the High Court of Ghana challenging her unlawful dismissal and seeking reinstatement among other reliefs.[45] Her case comes after the Supreme Court of Ghana declared that Chief Executives of public corporations were part of the Public Services of Ghana and cannot be ousted arbitrarily by an incoming administration.[46]

Having looked at three single purpose commissions, we highlight the human resources situation in a multipurpose agency- two dual mandates - Information Commissioner's Office (ICO); and Information Regulator. These agencies have a data protection and access to information mandate in the United Kingdom and South Africa respectively.

In contrast to the above-mentioned commissioner and commission model above, the British DPA represents a mixture between the two, having established a management board that "is responsible for developing strategy, monitoring progress in implementing strategy and providing corporate governance and assurance [as well as] managing corporate risks.[47] The management board does not only consist of executive (deputies and directors of the DPA) but also of external non-executive members, expanding the expertise of and providing new perspectives for the ICO.

The ICO is perhaps the largest DPA in Europe. It has 331 employees. It is headed by an Information Commissioner who is assisted by two deputy commissioners. The secretariat is led by a Deputy Commissioner/Executive Director in charge of regulatory Strategy Service and Deputy CEO. It is organised in four key directorates: Parliament and Government Affairs department; Policy and Engagement department; International Strategy and Intelligence; and Technology Policy and Innovation.[48]

In South Africa, the POPIA law empowers the regulator to recruit and manage members of staff as it may deem necessary for the discharge of its mandate.[49] Currently, the Information Regulator has about 35 staff members of the approved establishment of over 300. They plan to recruit more this year. The number could grow to a few hundred members of staff once the recruitment exercise for the approved positions is concluded. The secretariat led by the Chief Executive Officer is organised into seven (7) divisions which are in turn organised into units.

The seven divisions are: legal policy, research and information technology analysis; education and communication; protection of personal information; access to information; finance; corporate services; provincial services. **(see appendix 4 for the organogram).**

Challenges cited in Mauritius and Ghana are emblematic and incapacitate the data regulatory authorities because they are reduced into servants of the rulers in their respective countries. Data agencies in countries where the executive have vested interests suffer a blow especially when there is a change in the leadership of the country or respective ministries. Our finding is that political vagaries are part of the reasons for dismissal of head of agency in Ghana as the law left the dismissal issue gray.

- **To inform the Office of Data protection Commissioner in Kenya we also looked at select constitutional commissions and a regulator - Communications Authority.**

- **The Kenya National Commission on Human Rights has a staff 106 against a staff complement of 462.[50] It has its headquarters in Nairobi and five regional offices. On the other hand, the Commission on Administrative Justice**

To be able to operate optimally, it is emerging that DPAs require a set of officers not less than [40] from a mixture of professionals key among them lawyers, investigators (police, cybersecurity, data protection experts), prosecutors, corporate governance experts, communication and public education specialists.

For independence, it is critical that DPAs are vested with powers and obligations as an employer in relation to the people employed in the agency. This requires that the DPA is in charge of its own finances. Further, the DPA must develop competitive terms of service to enable it to retain highly qualified members of staff.

37. Data Protection Act, 2018 (Sweden),s.218; the Credit Information Act; the Patient Data Act; the Criminal Data Act; and the Debt Recovery Act.

38. The Swedish Authority for Privacy Protection website, available at < accessed on 30th March 2021>.

39. Brochure of the Data Inspection Board: What in earth does the Data Inspection Board do?: A Portrait of the Swedish Data Inspection Board, Swedish Data Inspection Board, Stockholm,5.

40. Data Protection Act, 2017 (Mauritius), s.4 (4)
41. Data Protection Act, 2017 (Mauritius). S 4 (5).

42. Mauritius Data Protection Office, Annual Report 2019, available at <Accessed February 17, 2021>

43. Annual Report: January- December 2019, p5. Available at <Accessed on 31 March 2021>.

44. Annual Report: January -December 2018, p8-9 Available at <Accessed on 31 March 2021>.

45. Centre for Global Development, "Bio: Teki Akuetteh Falconer," <accessed February 17, 2021>.

46. Nyaaba, Felix Engsalige, "Former CEO Of Data Protection Commission Sued Govt After Supreme Court Ruling," Modern Ghana, Published July 2, 2019,<accessed February 17, 2021>.

47. Schütz, Philip. "Comparing formal independence of data protection authorities in selected EU Member States." In Conference Paper for the 4th ECPR Standing Group for Regulatory Governance Conference. 2012.

48. Information Commissioner's Office, "Organisational structure," available at <Accessed Apr 6, 2021>

49. POPIA, 2013 (South Africa), s.47 (1)
50. Interview with KNCHR Chief Executive Officer, 5th March 2021.

5.0 Funding and Financial Sustainability

Appropriate funding and financial sustainability determine the extent to which a regulator can carry out its mandate fully, properly and act independently. DPAs require adequate funds for them to effectively monitor the implementation of data protection laws.

Generally, DPAs' budgets are approved by the legislature and form part of the national budget, which is a guarantee of transparency and accountability of regulators to citizens, and can strengthen independence. However, this approach can be prone to political interference. For example, in Australia, the Office of the Australian Information Commissioner (OAIC) suffered a major setback during the era of Prime Minister Tony Abott. It had to grapple with underfunding. Since then, multi-year budget decisions are preferred.[51]

The second and third approaches to funding of data protection authorities is through charges and fees for specific services and activities. The two approaches internalise regulatory costs to the regulated sector. It is thus a reliable source of funds for the DPA. It is also easier to administer and is consistent with regulatory independence, and promotes transparency.

For regulators funded through fees, an appropriate cost-recovery mechanism is essential to set the "right" fee and avoid a regulator that is under-funded, captured by industry or undermined by the executive arm of the government that be.

Aware of the approaches different jurisdictions take to fund data protection authorities, we assess budgets, funding and financial sustainability of the DPAs in Mauritius, Sweden, Canada, United Kingdom and South Africa. We did not receive timely responses from Ghana but we highlight what the law provides for in terms of funding.

5.1 Canada's OPC

The budget of the Office of the Privacy Commissioner in Canada is fully funded by the government. In the financial year 2019, a total budget/income of Canadian dollars $29,661,886 (about KSh 2.6 billion) was allocated. This was an increase in budget from the previous year.[52]

The source of budget for the ODPC in Kenya is both the government and fees levied on the regulated industry. This is the same as the Information Regulator (SA) and UK's Information Commissioner's Office ICO.

5.2 ICO in the United Kingdom

The funding of the Information Commissioner comes from three sources:

- **(i) Data protection charges paid by controllers, which are set by Secretary of State's regulations (the Data Protection (Charges and Information) Regulations 2018), and amount to 85% - 90% of the Office's annual budget;**
- **(ii) Grant in aid paid by the Government to the Information Commissioner. Grant in aid is mainly used to finance the operating costs of the Information Commissioner as regards non-data protection related tasks; and**
- **(iii) Fees charged for services. At present, no such fees are charged.**

The ICO has budgeted income of £61 million (about KSh 9.3 billion) for the year 2020/21. This budget has grown from an overall budget of £19.7m in 2011. A decade ago the notification fees, which amounted to £ 15.1m, constituted the most significant source of income, but could only be used for data protection and not for freedom of information related work. The growth in the budget is about 310 per cent.

5.3 South African Information Regulator

Funds for the South African Information Regulator consist of such sums of money that Parliament appropriate annually,[53] and fees by data subjects, processors and controllers as may be prescribed by the Minister in consultation with the Regulator.[54] The funding of the Information regulator in South Africa is a grant in aid paid by the government and through fees In the last three financial years where we were able to obtain data, treasury the allocated the DPA R 10million (Ksh 74.5 million) in 2016/2017; R26million (Ksh 194 million) for 2017/2018; and R27million (Ksh 201 million) for 2018/2019. The figures are not inclusive of the fees.

While the budgets of the DPAs in the UK and South Africa may seem relatively high compared to the rest, it must be noted that both serve dual mandate or what was described earlier in this study as multipurpose agencies, that is ensure respect for and to promote, enforce and fulfill the rights to privacy and the right to access to information.

5.4 The office of the Data Commissioner in Mauritius

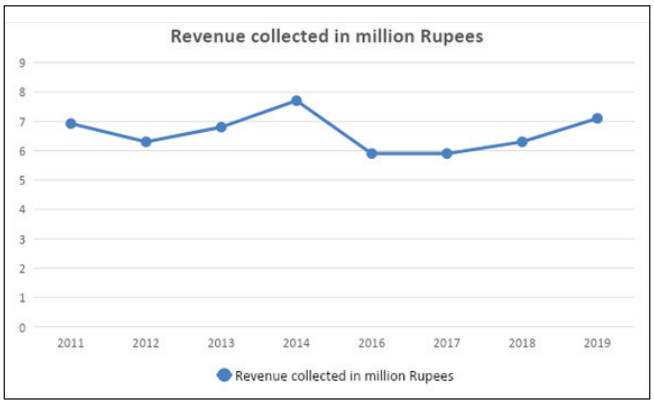
The Data Protection Office in Mauritius is funded only through charges and fees for services offered to data controllers and processors. The amount collected in

the last nine financial years has ranged from Rupees 5.6m - 7.1m (Ksh 14.5m-18.3m). Given the skeletal staff members, the revenue collected falls far short of targets. It is believed that with a full complement of staff the revenue collection could go higher. This assertion is supported by the fact that when the office had 18 members of staff in 2014, it is when the revenue collected was at its highest - R7.7 million (about KSh20 million).

Figure 2: Revenue collection per year (2011-2019)s

0	Financial Year	Revenue Collected (Rupees)
1	2011	6.92 million
2	2012	6.3 million
3	2013	6.8 million
4.	2014	7.7 million
5.	2015	5.6 million
6.	2016	5.9 million
7.	2017	5.9 million
8.	2018	6.3 million
9	2019	7.1 million

Source: Annual Reports of the Office of the Data Protection Commissioner



Revenue Collected in million Rupees

5.5 Ghana's Data Protection Commission

In Ghana, the Data protection Act, 2012 provides inter alia that there are four streams of possible funding for the Data Protection Commission: money approved by parliament, donations and grants to the Commission; money that accrue to the Commission in the performance of its functions; and any other money as may be approved by the Minister of Finance.[55]

5.6 Other DPAs and institutions

The Irish Data protection Commissioner is the oversight body for the Republic of Ireland with a population of about 5 million. Its funding by the government has increased year-on-year from € 1.7million (Ksh 216,360,000) in 2013 to € 16.9million (Ksh 2,150,870,000) in 2020.

To inform the Office of Data protection Commissioner in Kenya we also looked at twoconstitutional commissions and a telecommunications regulator - Communications Authority.

The Commission on Administrative Justice (CAJ) established by the Commission on Administrative Act, 2011. It is the oversight mechanism for access to information law and also deals with public service administrative malfeasance. The funding of the Commission by government has increased year-on-year from Ksh Ksh 216,241,303 in the financial year 2012/2013 to Ksh 492,389,280 in 2018/2019.[56] However, there was a 12 per cent reduction in the allocation of 2017/2018.

Another constitutional commission considered was the Kenya National Commission on Human Rights (KNCHR). It was established by the Kenya National Commission on Human Rights Act, 2011. It is the state's lead agency in the promotion and protection of human rights. The KNCHR has received a government budget allocation between Ksh 398,766,234 (2017/2018) and Ksh 251,000,000 (2012/2013).[57] The budget has increased since it was established except in 2016/2017 and 2017/2018 when it reduced by 5.8% and 4.2 respectively.

The Communications Authority established by the Kenya Information and Communication Act, 1998 [as amended]. It receives its funding through charges, license and services fees, fines. Its revenue has ranged at around Ksh 9.0 -8billion. In 2017/2018 it was Ksh 8.922 and their expenditure was Ksh 4.406 and remitted Ksh 4.5billion to the exchequer. In 2016/2017 the revenue was Ksh 8.78billion and the expenditure was Ksh 3.67billion.[56]

51. Brown, Ashley C. "The Funding of Independent Regulatory Agencies." online:

52. Ibid:

53. Protection of Personal Information Act, 2013 (South Africa), s. 52.

54. Protection of Personal Information Act, 2013 (South Africa), s.111 (1) & s,113.

55. Data Protection Act, 2012 (Ghana), s. 14.

56. Commission on administrative Justice, Annual Report 2018/2019; Annual Report 2012/2013 available at st March 2021>.

57. The KNCHR, Annual Report For the Financial Year 2017/2018; Annual Report 2012/2013 available at st March 2021>.

58. Communications Authority of Kenya, Annual Report for the Financial Year 2017/2018, available at st March 2021>.

The inaugural budgetary request for the office of the Data Protection Commissioner was KSh 500 million and it is projected to grow to 680million in the next financial year is KSh 680 million.[59] In a recent supplementary budget request its was allocated Ksh11 million to fight abuse of personal data by private sector firms and government entities. The agency requires enough funding and financial sustainability to be able to mount effective investigations and enforcement. The ODPC can also get donor funds provided that it alerts the Treasury and copy the same to the ICT Ministry.

6.0 Complaint Handling Mechanism and Enforcement

Data Protection Authorities have a duty to receive and act on all complaints by individuals. Sometimes the authorities on their own motion investigate issues they have identified. Therefore, the DPAs need a clear and comprehensive complaint handling mechanism. With EU member states, they are required to have one-stop-ship.

6.1 One-Stop-Shop (1SS) Mechanism

Data authorities in the EU member states have to ensure that a one-stop-shop mechanism is used to handle complaints and other data protection issues.[60] Article 56(1) specifies that the "supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor".

6.2 Standard Procedures of Handling Complaints

6.2.1 South Africa's Information Regulator

The Information Regulator (SA) is fairly new. It predates the ODPC in Kenya with a few years. They are still in the process of adopting the standard procedure(s) of handling complaints. The procedure in POPIA is as follows:

Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with personal information of a data subject:

- A responsible party or a data subject may submit a complaint to the Regulator in the prescribed manner and form if he or she or it is aggrieved by the determination of an adjudicator after investigating a complaint relating to a breach of an approved code of conduct.

On receipt of a complaint, the Regulator may conduct a pre-investigation; act as a conciliator where appropriate (only insofar as the interference with personal information is concerned); decide to take no action or an action; conduct a full investigation; or refer the complaint to the Enforcement Committee.

6.2.2 ICO's standard procedures of handling complaints

The ICO has a general duty to investigate complaints from members of the public. Complaints can be made via the ICO website or through the ICO's live chat function or helpline telephone number. Organisations must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it must be accompanied by reasons for the delay.[61] Once a concern is raised with the ICO, the ICO will record and consider it.

In some cases, the ICO will collate further information on similar issues, looking at the concern alongside others raised about the organisation. In cases where a clear and serious breach of the legislation has taken place, the ICO will take direct action on the specific concern raised. If it decides that there has been a serious failure to comply with the law, the ICO will provide advice and instruction to help ensure the organisation gets it right in future. If an organisation isn't taking its responsibilities seriously, the ICO may also take enforcement action.

6.2.3 OPC's standard procedures of handling complaints

As of November 1, 2018, organisations subject to PIPEDA must notify the Privacy Commissioner of Canada if they become aware of any breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals. Companies must also inform individuals affected by such breaches. It is mandatory for Organisations to keep records of all breaches of security safeguards for two years, whether these breaches were reported to the Privacy Commissioner of Canada or not.[62]

6.3 Enforcement

Most data protection authorities have deployed various lawful enforcement tools to ensure compliance. During the study, most of the DPAs assessed have deployed the traditional post -breach sanctions which are proving to have limited use for regulators dealing with the effects of improper data use.

Some of the enforcement actions identified across different DPAs studied include: undertaking; prosecution; enforcement notices and administrative/ monetary penalties. For instance, Canada's OPC investigates complaints initiated by individuals, or issues identified by the agency, and issues findings and non-binding recommendations. Under PIPEDA, private sector law, mandatory breach notification and record keeping can also be required of the data controller or data processor. Other enforcement options the OPC can pursue include:

- **Appearing before the Federal Court on behalf of a complainant (or on own behalf for investigations initiated by the Commissioner) for a de novo hearing on the alleged contravention. (Under the Privacy Act, this provision is limited to matters relating to individuals' right of access to their own personal information);**
- **Making public information that comes to light in the performance of the Privacy Commissioner's duties, (i) if the Commissioner considers it to be in the public interest Under PIPEDA), or (ii) annually in a report to parliament, or where urgent in a special report to parliament (under Privacy Act);**
- **Under PIPEDA, referring a matter to the Attorney General of Canada who can issue fines for certain offenses relating to whistle blower protection and data breach notification;**
- **Inspecting records of breaches of organisational safeguards under PIPEDA; and**
- **Entering into voluntary compliance agreements under PIPEDA.**

In Canada, the OPC does not have the power to impose criminal fines or administrative financial sanctions (there are certain limited provisions under CASL whereby authorities other than the OPC can impose administrative financial sanctions). Under the country's private-sector statute, the courts have the power to order organisations to pay damages to a complainant(s) following a court application brought pursuant to PIPEDA. Any such damages are civil in nature. There are no statutory minimums or maximums to the amount of damages a Court can impose, although the jurisprudence has generally involved awards of between Canadian $500 and $5,000 for PIPEDA cases.

Having assessed the traditional approach used by most of the DPAs, we realise that there is no clear timelines set within which matters must be resolved and neither is such an approach focusing on the most pressing issues of data protection in a country. We are, therefore, of the view that the Kenya ODPC adopts a new, a more proactive *ex-ante* approach that could help focus regulatory capacity on the most serious risks to protection of personal data. Such a model will require a motivated and well-resourced regulator that will need to be both agile and transparent in its functioning.

A risk-based regime would first seek to identify those entities that are likely to have a larger impact if the personal data held by them is breached or misused. This approach borrows from the thinking around data protection impact assessments under the GDPR, 2018 and section 31 of the Data Protection Act. The information to make such assessments would be gained through a two-pronged approach:

- **First, through the use of a methodology where the Data Protection Authority could assign risk scores to classify entities into (I) High risk data entities, (ii)medium risk data entities, and (iii) low risk data entities;**
- **Second, these risk scores could be analysed together with the results of privacy impact assessments that could be mandated to be undertaken by entities collecting personal data.**

Using this information the DPA could then use an enhanced toolbox that could be used in advance of a breach or following a breach of personal data to mitigate risks to individuals. While exercising this supervisory judgment to launch enforcement actions, the regulator will be required to be guided by certain principles for sound regulation.[63]

As a new regulator, one must employ both soft and hard enforcement tools. This would encourage bilateral communication about data practices between the new regulator and the entities it regulates.

"Such a responsive regulation will adopt a collaborative posture. Subsequent contraventions are addressed through gradual regulatory escalation. The magnitude of the escalation and the punitive effect of the regulatory response corresponds to the nature of the default. A regulatory pyramid depicting gradual escalation through enforcement actions can then be built. An example will be injunctions at the highest level of the pyramid and seeking information regarding suspected contraventions of the law at the lowest part of the

pyramid. In between are other 10 enforcement actions that the DPA can lawfully take.

59. Interview with the Data protection Commissioner, 12th March 2021

60. Thyve, Ulrik Fredrik. "One-stop-shop–or not? The Regulation of competent supervisory authority in the new EU General Data Protection Regulation–does the one-stop-shop mechanism live up to its promise?." Master's thesis, 2016.

61. UK GDPR, Article 33

62. Coos Andrada, "Data Protection in Canada: All You Need to Know about PIPEDA," Endpoint Protector. Published Jan 17, 2019. Available at <Accessed April 6, 2021>

63. Information Commissioner's Office, Data Protection Regulatory Action Policy, available at th March 2021>.

7.0 Implementing Regulations

The data protection regimes have procedures of formulating regulations and developing codes of conduct aimed at ensuring compliance with data privacy and personal data protection.

We propose that the Data Protection Commissioner prioritises the development, adoption and gazettement of seven sets of regulations. This section ends with a proposal on the code of practice as provided for in section 52 (3) of the Data Protection Act, 2019. The Code of Practice will not have any formal legal status and cannot set new rules. It only seeks to help those working in the media industry to understand and comply with the existing law in this area. The code of practice shall elaborate on the provisions on privacy in the Code of Conduct for Journalists in Kenya.

7.1 Registration of Data Controllers and Data Processors

Pursuant to Section 18 (2) of The Data Protection Act, 2019, the Data Commissioner is expected to prescribe thresholds required for mandatory registration of data controllers and data processors. The Data Commissioner is thus expected to develop a regulation that spells out the procedure of applications for data controllers and data processors and when such regulations come into force.

7.2 Data Protection (Fees) regulations

Pursuant to section 67 (c)The Data Protection Commissioner is required to provide a guideline on the reasonable fees the controllers are expected to pay. This must be published from time to time since some tiers may be reviewed. This would be helpful as the DPA seeks to register data controllers and processors under Part III (s. 18-22) of the law. It will also help when she decides to carry out periodic audits to ensure compliance as provided for by the law.[64]

In the UK, the ICO clarifies that the fees are set by Parliament to reflect what it believes is appropriate based on the risks posed by the processing of personal data by controllers.[65]

7.3 Data Subject Access Regulations

The data subject must understand that he, she or it is a key actor in the data economy because they provide the data. Other key actors are the data processor who analyses that data, and the independent authority to regulate the economy. Kenya's Data Commissioner should effectively structure her office and work round the clock to ensure data subject access regulations are enforced and remain effective.

7.4 Traffic Data Regulations

Kenyan law does not directly regulate online privacy. To be effective in data protection, it is thus important that some regulations or amendments to the Data Protection Act, 2019 be made to deal with among others collection of location and traffic data by public electronic communication service providers (CSP) and use of cookies (and similar technologies). For instance, there must be a law or regulation requiring every CSP that holds traffic data to have it erased or anonymised when it is no longer necessary for the purpose of the transmission of the communication. Traffic Data can also be processed by a CSP to the extent necessary for four main reasons namely: the management of billing or traffic; dealing with customer enquiries; the prevention of fraud; the provision of value-added service. Thus the regulation must provide that traffic data may be retained if it is being used to provide a value-added service. Secondly, for the retention to be lawful, voluntary and informed consent must have been given.

7.5 Cookie Compliance regulations

The Data Protection Act, 2019 is not express on the issue of cookies and similar technologies. This is another gap that could be remedied by development of separate regulations and/or amending the primary law. The use and storage of cookies and similar technologies require two critical things: one, clear and comprehensive information; and clear, informed and voluntary consent of the website user. The issue of clear and comprehensive information responds to the requirements of transparency and the right to of the data subject to be informed. It implies among others that if you use cookies you must: say what cookies will be set; explain what cookies will do (purpose); state the duration of any cookies you wish to set; state any third parties who may also process information stored in or accessed from the user's device; and obtain consent to store cookies on devices. However, it must be noted that consent is not required for cookies that are used for the sole purpose of carrying out transmission of communication over an electronic communications network, or strictly necessary for provision of a service requested by the user.

The United Kingdom's Privacy and Electronic Communications Regulations (as amended) (herein after PEC Regulations) is a good example. In Regulation 6, they cover the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as a computer or mobile device. While the PEC regulation 6 does not refer to cookies by name, it states *inter alia* that:

"1... a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of Paragraph (2) are met.

2. The requirements are that the subscriber or user of that terminal equipment-

a. is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

b. has given his or her consent.

7.6 Electronic Marketing Regulations/Guidelines

The application of the Internet and related digital technologies to achieve marketing objectives aimed at achieving profitable acquisition and retention of customers is a multi-faced approach that requires regulations. Businesses improve their customer knowledge thus allowing them to deliver integrated targeted communications and on-line services that match their individual needs. Electronic marketing conceives security and privacy issues especially because customers' data can easily be shared with other companies without asking for their permission or worse still, they can be duped by the purported 'marketers'. The Data Commissioner is expected to draft regulations to help monitor e-commerce businesses and ensure that on-line fraudsters are locked out.

7.7 Certification Guidelines/Schema

The Data Commissioner is required to offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations. Proper guidelines must be put in place to ensure that data controllers or data processors issued with certification remain in compliance in accordance with the law.

7.8 Prototype Code of Practice

Pursuant to Section 52 (3), the Data commissioner is expected to issue a Code of Practice for journalists and those working in the media industry. The Code of Practice is important for a number of reasons. First, it helps reiterate that data protection laws are complementary to freedom of expression and not contradictory. It, therefore, situates the journalism exemption and its import in protection, fulfillment and realisation of free-

64. Data Protection Act, 2019 (Kenya) s. 23

65. Information Commissioner's Office, "The data protection fee: A guide for controllers." Published February 21, 2018. <Accessed March 1, 2021>

dom of expression even as it ensures that journalists are not held accountable for breach of data protection law. Second, given that the media industry processes personal data but most of the time little in terms of good guidelines exist. This is made worse by the fact that media practitioners are also not clear on basic applicable principles and their obligations under the law.

The UK ICO has issued a guide that could form an equivalent parallel for the Data Commissioner in Kenya.[66] Key areas of highlight must include among others: technical guidance on how the Data Protection Act applies to journalism; subject access requests; and confidential sources.

7.9 Processing sensitive data

Sensitive personal data is personal data that needs more protection. The Data Protection Act, 2019 isolates among others family details; ethnic social origin; medical, genetic, and biometric data; marital status, sexual orientation to be sensitive personal data. It even permits the Data Protection Commissioner to prescribe further categories of personal data which may be classified as such.[67]

The law envisages the Data Protection Commissioner to ensure that at a minimum the processing of sensitive personal data meets all the principles of data protection and the ten conditions. To ensure such it would be prudent for her to develop a guidance note where she should specify the conditions and any further grounds on which specified categories of sensitive personal data may be processed as is the case in the UK.

Among the jurisdictions studied, the UK and South Africa have extra requirements on processing of sensitive personal data.[68] In the UK there must be a lawful basis under Article 6 of the UK GDPR and a separate condition for processing under Article 9. Article 9 of the UK GDPR lists 10 conditions. Five of these require a controller or processor to meet additional conditions and safeguards set out in the law,[69] and they must have an appropriate policy document.

The appropriate policy document must require the data processor or controller to undertake data protection impact assessment for processing such sensitive personal data.

In Canada, there are no additional rules for processing sensitive personal information under PIPEDA. It just requires that an organisation should generally seek express consent when the information is likely to be considered sensitive. This means that implied consent would generally be appropriate when the information is less sensitive. Also, the nature of information security safeguards varies depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. Thus, more sensitive information must be safeguarded by a higher level of protection.

7.10 Regulations for transfer of personal data outside Kenya

Flows of personal data to and from Kenya are necessary for international trade and international cooperation. However, the transfer of such personal data from Kenya to controllers and processors located outside Kenya should not undermine the level of protection of the individuals concerned.

Therefore, transfers to other jurisdictions or international organisations should be done in full compliance with Part VI of the Data Protection Act, 2019.[70] It is, therefore, incumbent upon the Data Protection Commissioner to issue guidance notes clarifying what is meant by transfer subject to appropriate safeguards,[71] and what such safeguards may include. Such a guidance note must address itself to the standard data protection clauses, "standard contractual clauses (SCCs)," approved codes of conduct, and binding corporate rules.[72] The guidance note should be informed by the Court of Justice of the European Union in the case of *Data Protection Commissioner v Facebook Ireland Ltd* and the *Maximillan Schrems.*[73] where the validity of the SCC's were examined.

A separate guidance note must also be developed and availed for personal data transfers within the law enforcement sector. Separately, the Data Protection Commissioner may also initiate adequacy talks with the European Union.[74] An adequacy finding will enable free and data flows from the EU to the Republic of Kenya. It will also make such approvals easy for countries that have already had adequate determination with the EU to take Kenya as a safe destination for data transfers.

66. ICO, Data Protection and Journalism: A Guide for the Media. Available at <Access on 20th Feb 2021>

67. Data Protection Act, 2019 (Kenya) s. 47 (1) and (3).

68. See the UK ICO Guidance on Special Category Data available at th Feb 2021>.

69. Data Protection Act,2018 (United Kingdom) Schedule 1

70. Data Protection Act, 2019 (Kenya) s.48-50.

71. Data Protection Act, 2019 (Kenya) s.48 (a)-(b) and s. 49

72. Standard Contractual Clauses for data transfer between EU and Non-EU countries available at th March 2021>.

73

74. Adequacy Decisions: "How EU determines if a non_EU country has an adequate level of data protection," available at th March 2021>.

75. Constitution of Kenya,2010 Article 249.

8.0 Conclusions

This study has attempted to draw on emerging lessons on creation, constituting, funding and rolling out an effective, efficient but independent data protection authority.

It has found that the Office of the Data Protection Commissioner as established by Data Protection Act, 2019 is as solid and compares well with similar institutions across the globe. It, however, falls short on some aspects of independence like determination of directorates and human resources, funding and development of requisite implementing regulations.

Complete legal independence would have been obtained if the authority were established as chapter 15 constitutional Commission.[75] Its independence in practice would depend on the Data Commissioner approach to building a credible, legitimate, efficient and accessible organisation that delivers its mandate especially enforcement with fear or favour to any actor in the public or private sectors. She must take advantage of the provisions of the law, especially Section 8(3) which states "the data commissioner shall act independently in exercise of powers and carrying out of functions under the Act." By properly applying this section of the law she should be able to guard against undue influence from the political elites under the guise that they are ensuring accountability.

To achieve the above and as the DPA must roll up its sleeves to start work, it must develop a futuristic strategic plan that spells out its clear funding and human resource needs and lobby to ensure requisite state/government funding. It must recruit, train and retain a well motivated calibre of staff able to help it service its mandate and functions. In the discharge of its functions, the Office of the Data Commissioner has an urgent obligation to quickly formulate the requisite regulations, guidance notes and public education materials. They also have to develop and roll out a robust complaint handling and information management system as a precursor to effective enforcement.

9.0 Recommendations

9.1 Independence

The law is a key determinant of formal and de facto independence of a Data protection Authority. And as currently provided for there is sufficient room to exercise such independence in practice. To bolster independence, which is core to its credibility and effectiveness, in practice we recommend that:

- **The Data Protection Commissioner develops a comprehensive Corporate Governance Framework for the office in accordance with the Constitution of Kenya, 2010 and the Data Protection Act, 2019;**
- **The Office of the Data Protection Commissioner is rolled out in a way that allows it to be receptive to changes in the industry, but guard against capture or pitfalls such as ties to incumbents;**
- **Set priorities and concentrate on issues of special importance or policy special cases that can secure credibility and legitimacy among key stakeholders; and**
- **Though the ODPC is domiciled in the ICT Ministry, we propose that the Data Commissioner, holding a post which requires that she acts independently, appears in person before the specific parliament committees handling serious personal data related issues as a practical measure of accountability to the people of Kenya.**

9.2 Human Resources and Regulatory Competences

We recommend that the ODPC comes up with a clear organogram that shows key nodes of the organisation and various units of the office such as the enforcement section, complaints section, investigations section, prosecution, international cooperation, legal unit and finance section among other key units as deemed necessary. The ODPC must envisage creation of strong and viable regional offices in select counties [see Appendix 1,4, 5 similar organisational structures of CNIL, ICO and Information Regulator];

- **That such a clear organogram should have an approved staff establishment of 150. In the first two years, the ODPC should have a minimum of 40-50 positions. With time, the office could be expanded and more positions created to have the number at around 110-150;**
- **The Commissioner in liaison with the Public Service Commission and salaries Remuneration Commission must develop clear human resources manuals with requisite policies and pay spine that there are clear terms of service to ensure it recruits, develops and retains highly qualified and motivated staff;**
- **Through a rigorous but transparent process, they advertise and recruit a mixture of professionals key among them lawyers, investigators (police, cyber security, data protection experts), prosecutors, corporate governance experts, administrators, human**

resources experts, communication and public education specialists who are competent and can be held accountable.

- Initiate a feedback loop that ensures reflexivity and allows periodic assessment of whether the regulator's performance and enforcement actions are effectively leading to the fulfillment of the overall regulatory objectives;

- There is a need to develop a clear format of how data protection functions are handled by the ODPC. It will help guide individuals and representative groups to understand the timeframes of lodging a complaint, information notice, assessment notice, inspection, enforcement notice and penalty notice; and

- ODPC to invest in robust and reliable technology. The technology solution acquired should follow a security-first approach to protect personal data such as using robust encryption techniques and securing data transfer channels. The key tools and technologies needed so as to enhance data protection include data flow mapping tools and automation, data transfer assessment automation, data protection maturity and planning tools. There are also risk assessment tools, data discovery and classification tools, vendor risk management tools, incident management tools and technologies, privacy rights tools (e.g. management of data subject rights requests), E-learning / training tools, IT risk and security management technologies, Cookies management tools as well as preference management tools. Others are mobile app consent management, privacy notice management tools, data governance tools, data Analytics, and data retention and deletion tools; and

- Deploy use of Memorandum of Understanding between the ODPC and other regulators and government agencies operating in different sectors like banking, telecommunications, health, education as key agencies whose sector may hold the biggest risk to personal data.

9.3 Funding and Financial Sustainability

Adequate and timely funding is critical for the independence and effectiveness of the Office Data Protection Commissioner. We, therefore recommend that:

- The National Assembly through the Parliamentary Committee on Budget to create a dedicated/separate vote head for the Office of the Data Protection Commissioner to guarantee its autonomy, direct control and accountability;

- The ODPC is allocated an annual budget of at least KSh 700 million for a start, then to be receiving an additional steady increase of 15 per cent each year subject to its absorption capacities;

- The ODPC develops and implement a clear fundraising strategy that most have clear deliverables on how to engage with necessary government agencies that make budgetary allocations;

- The ODPC maps out various bilateral and multilateral donors and diversify funding engagements to ensure financial sustainability; and

- The ODPC hastens the development of implementing regulations on fees as collection of registration and notification fees from data controllers and processors offers a pathway to her financial security and sustainability.

9.4 Complaint Handling Mechanism (s) and Enforcement

Develop and implement a web-based a clear complaint handling mechanism;

Create and implement a robust complaint handling system that enables the DPA to receive, organise and analyse complaints on time;

Roll out a programme of work as a pioneer towards risk-based data protection enforcement and compliance;
Develop, support and enforce a self-regulation model for managing technological innovation in uncertain scenarios. This model entails different governance measures that data controllers should rely on when controlling risks, such as data protection impact assessments, the appointment of data protection officers and regulatory strategies to implement data protection by design and by default;

In line with s. 31 of the Data Protection Act, adopt and develop a clear system to deploy privacy Impact Assessments/Data Protection Impact Assessment as critical tools of meta-regulation (risk-based approach to regulation);

ODPC has access to a wide range of enforcement tools and thus must also initiate a robust accountability

mechanism to ensure these tools are used fairly and consistently;

To improve transparency and confidence in the functions of the DPA, we recommend that the ODPC could publish, suitably anonymised, quarterly reports on the nature, volume and geographic concentration of complaints received in public domain;

Publish and publicise annual reports on enforcement actions undertaken and complaints acted upon. Reporting on enforcement actions consistently and in the same format will in term create a robust framework for ensuring accountability of the future ODPC;

Establish a well structured independent quasi-judicial forum for the regulator to adjudicate/resolve violations of the data protection regime;

Cooperate with international organisations and the supervisory authorities of other countries to support the effective enforcement of the law and to share best practices.

9.5 Regulations

Seek to revive and refocus the East African Community processes around the EAC Legal Framework on Cyber Law so as to clearly spell out minimum standards for data protection for EAC member states (Kenya, Uganda, Tanzania, Rwanda, Burundi, South Sudan and DRC);

Take all the necessary measures in the domestic law to give effect to the basic principles for data protection; and

Conduct regular consultative meetings with stakeholders to share new areas of concern and develop requisite implementing regulations.

Working definitions

Data breach: A data breach is a compromise of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data.[76] It can be described as anything that affects confidentiality, integrity or availability of data. Normally, it occurs when there is an unauthorised disclosure or a loss of personal data.

Data controller: Any natural or legal person, public authority, agency or any other body that determines the purposes and the means of the data processing.

Data processor: A data processor is any natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller.

Data recipient: Any authorised person to whom the data is disclosed, other than the data subject, the data controller, the sub-contractor and persons who, due to their functions, are in charge of processing the data

Data subject: Any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

Legal person: An individual, company, or other entity which has legal rights and is subject to obligations. Basically, a legal person is a human or non-human entity that is treated as a person for limited legal purposes, can sue and be sued, own property, and enter into contracts.[77]

Personal data: Any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number such as social security number or one or more factors specific to individual's physical, physiological, mental, economic, cultural or social identity like name and first name, date of birth, biometrics data, fingerprints or DNA. Personal data therefore refers to all information that has been provided by the client relating to one's personal needs.[78]

Regulation: Any general form of coercive rule setting by an authority or regime to influence activity and behaviour.

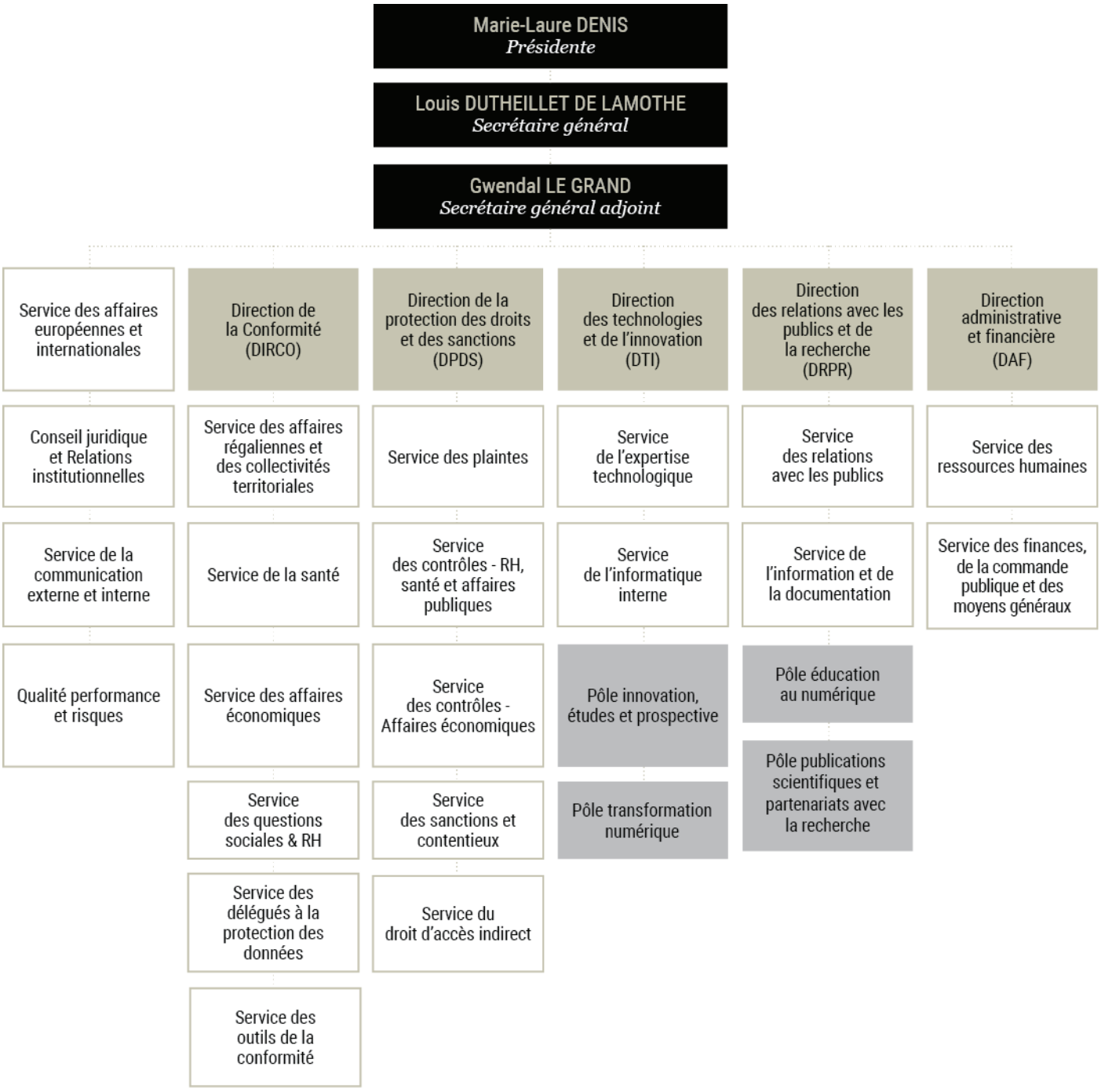
---

76. IT Governance, "What is a data breach?", <accessed February 9, 2021>,

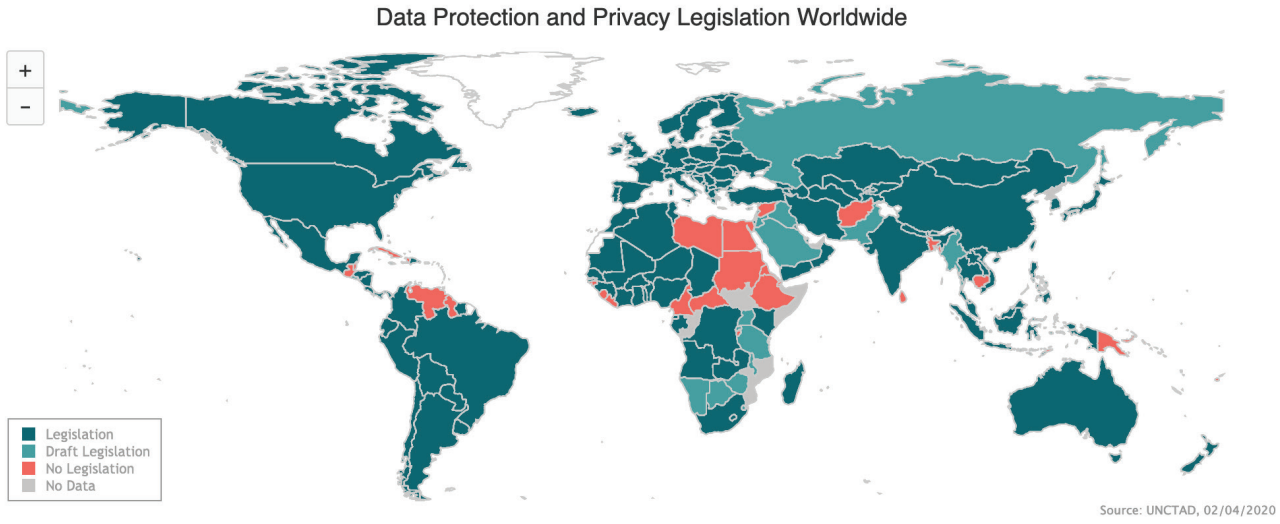
77. Cornell Law School, "legal person," <accessed February 10, 2021>,

78. Barak, "Information on Data Protection & GDPR Regulation 2016/679," <accessed February 12, 2021>,

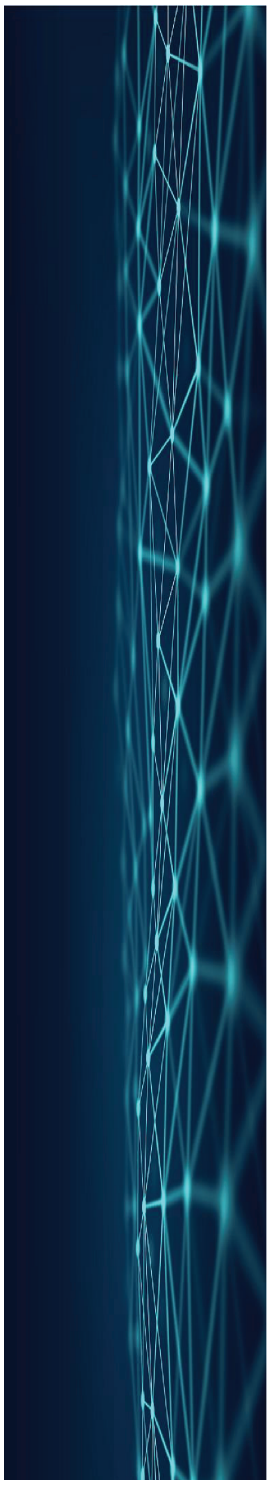
APPENDIX 1: Organisation chart CNIL 2020



APPENDIX 2: Organisation chart CNIL 2020



APPENDIX 3: Mauritius Data Protection (Fees) Regulations 2020



Data Protection Office

COMMUNIQUE TO THE PUBLIC

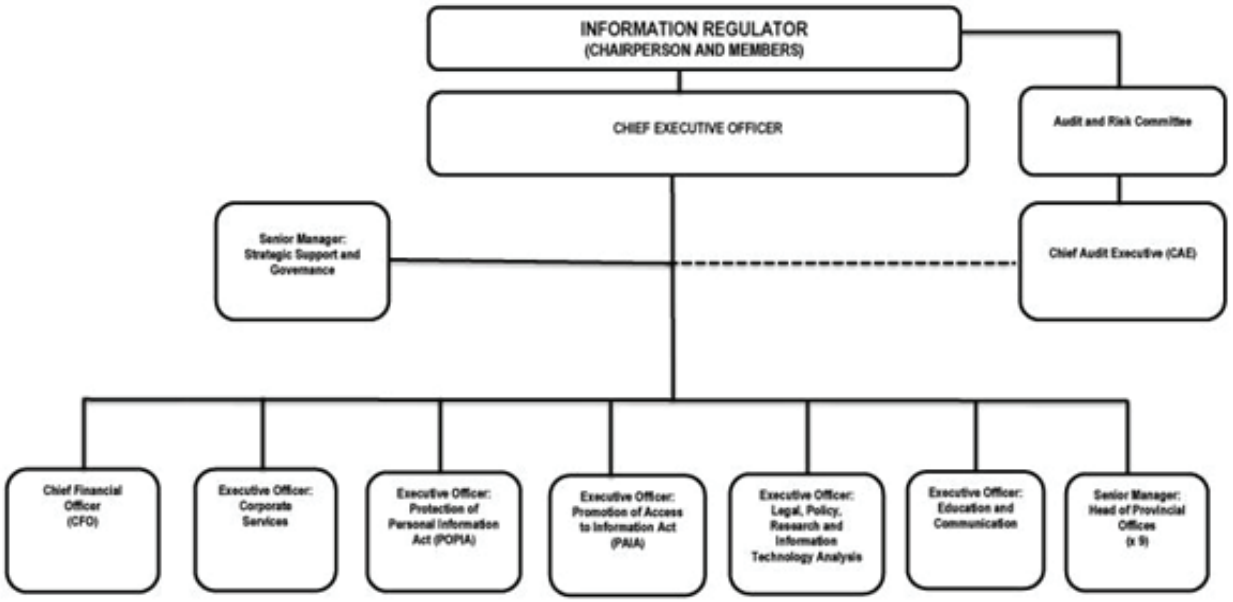
Data Protection (Fees) Regulations 2020

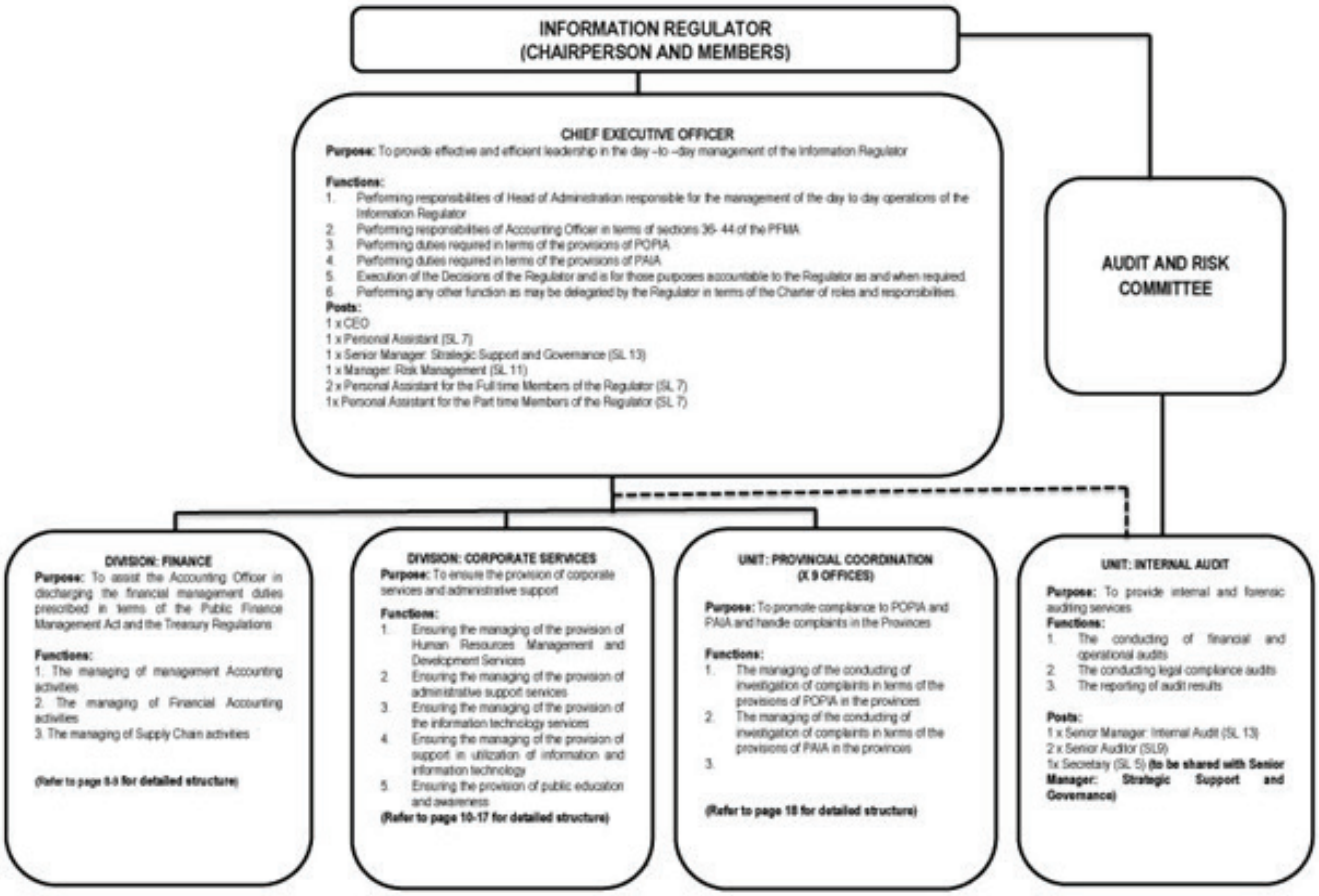
(*Government Notice No. 152 of 2020*)

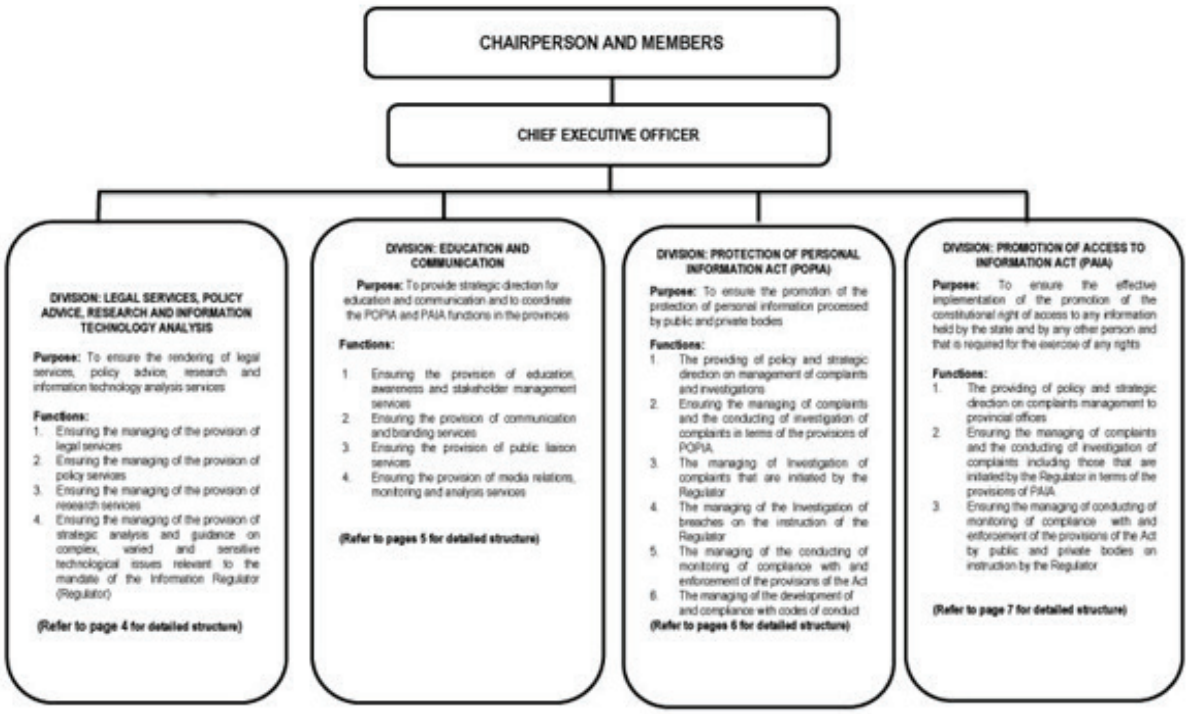
1. The Data Protection (Fees) Regulations 2020 concerning the new fees for registration of controllers and processors will come into force on 01 August 2020.
2. All controllers and processors will be required to make a fresh registration as from 01 August 2020 in accordance with the new Regulations.
3. Applications for registration may be submitted online, by post or in person at the office.
4. A registration certificate will only be issued where the Commissioner considers that an applicant meets the criteria to be registered as a controller or processor and this certificate will be valid for a period of 3 years by virtue of section 16 of the Data Protection Act 2017 ('DPA') .
5. New application forms for registration are available on the homepage of the Data Protection Office website at *http://dataprotection.govmu.org*.
6. Upon the entry into force of the new Regulations, all existing controllers and processors will have a moratory period of 3 months to make their registration(s). The registration date will be 01 August 2020.
7. Failure to register or renew the registration certificate(s) after the moratory period may amount to an offence under the DPA and consequently a fine not exceeding 200,000 rupees and imprisonment for a term not exceeding 5 years on conviction may be imposed.
8. In view of the large number of applications that would be received, this Office recommends payment by cheque drawn to the order of 'Governmen t of Mauritius'.
9. Controllers and Processors must consult the guide that has been uploaded on our website to assist them in filling the relevant form(s).
10. The holder of a registration certificate must apply for its renewal not later than three months before the date of its expiry by virtue of section 18 of the DPA.
11. Should there be any queries related to registration and renewal, please contact us by phone (4600251) or email (dpo@govmu.org).

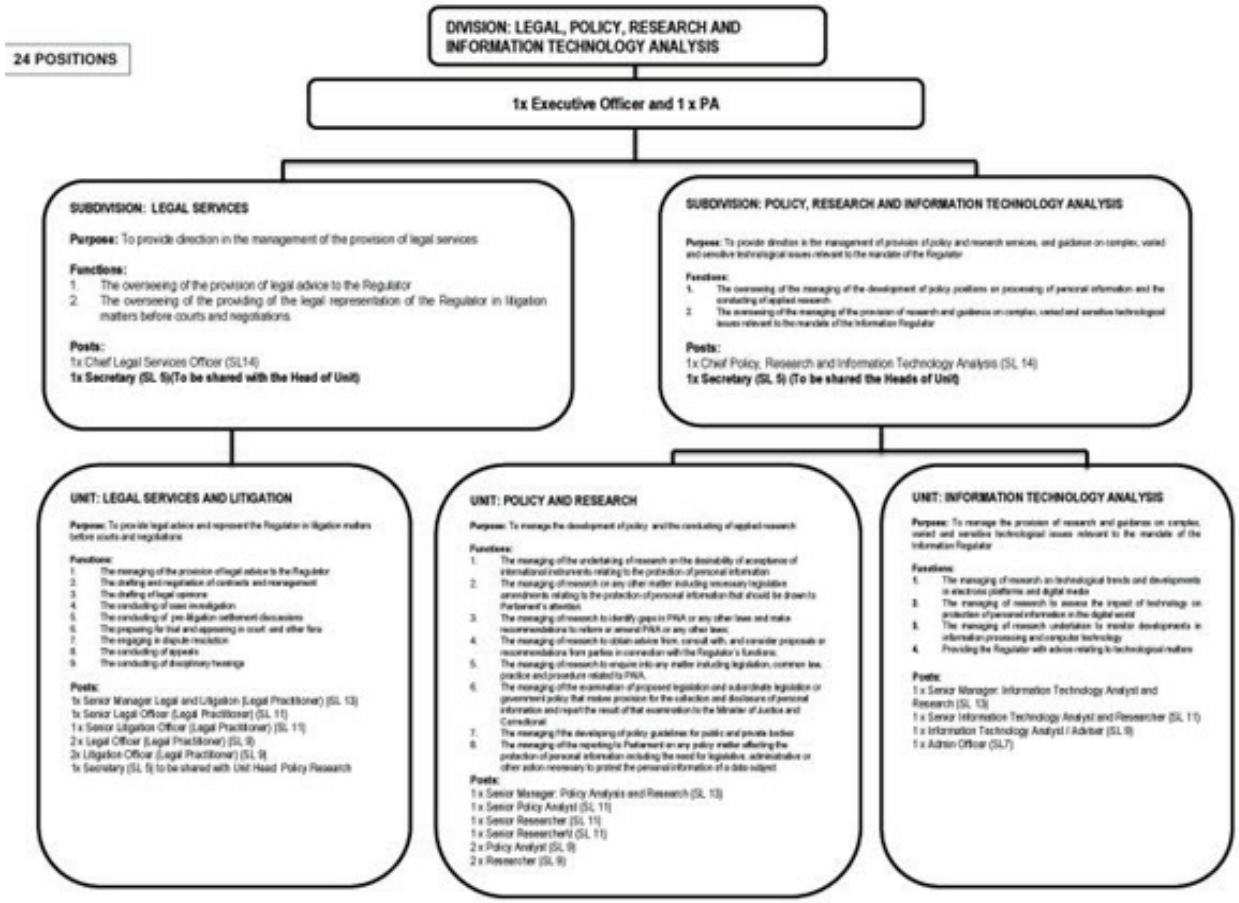
The Data Protection Commissioner
Data Protection Office
This 20th July 2020

APPENDIX 4: Information Regulator Approved Organisational Structure Revised 11 Sept 2020

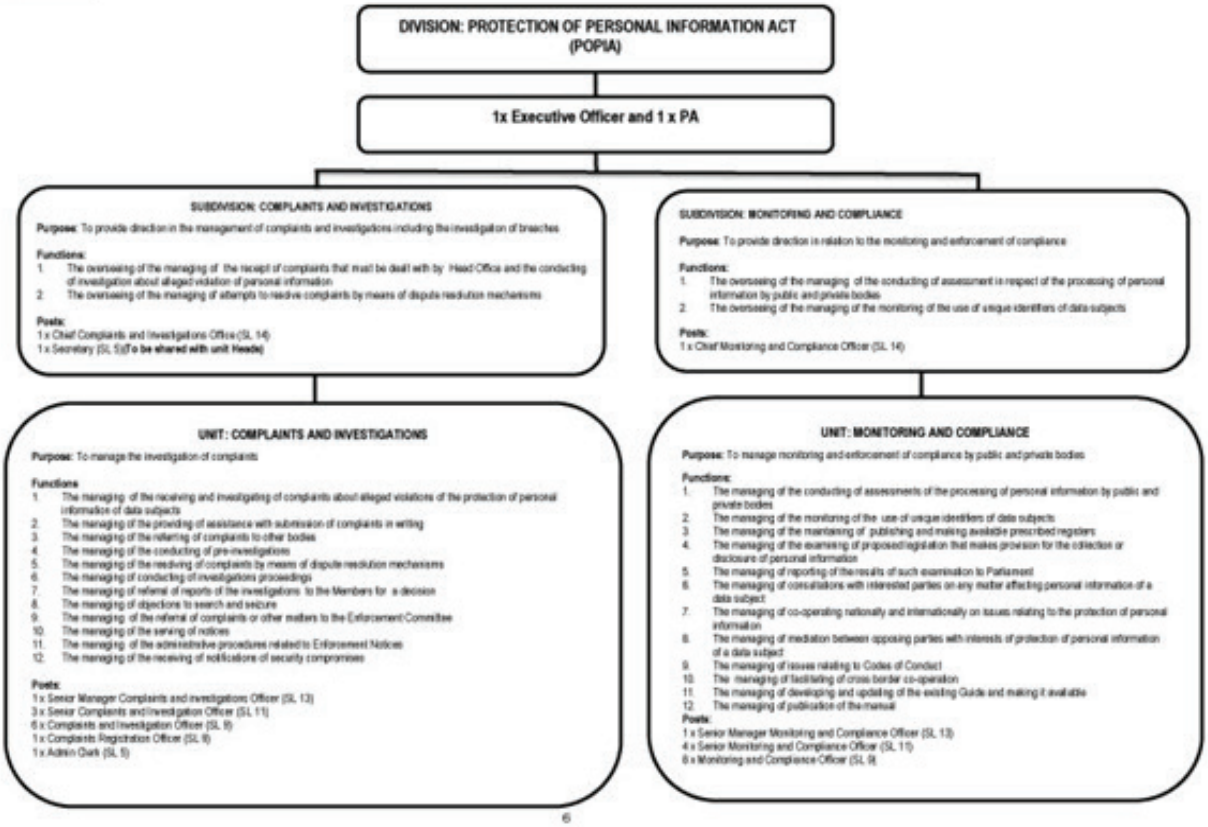




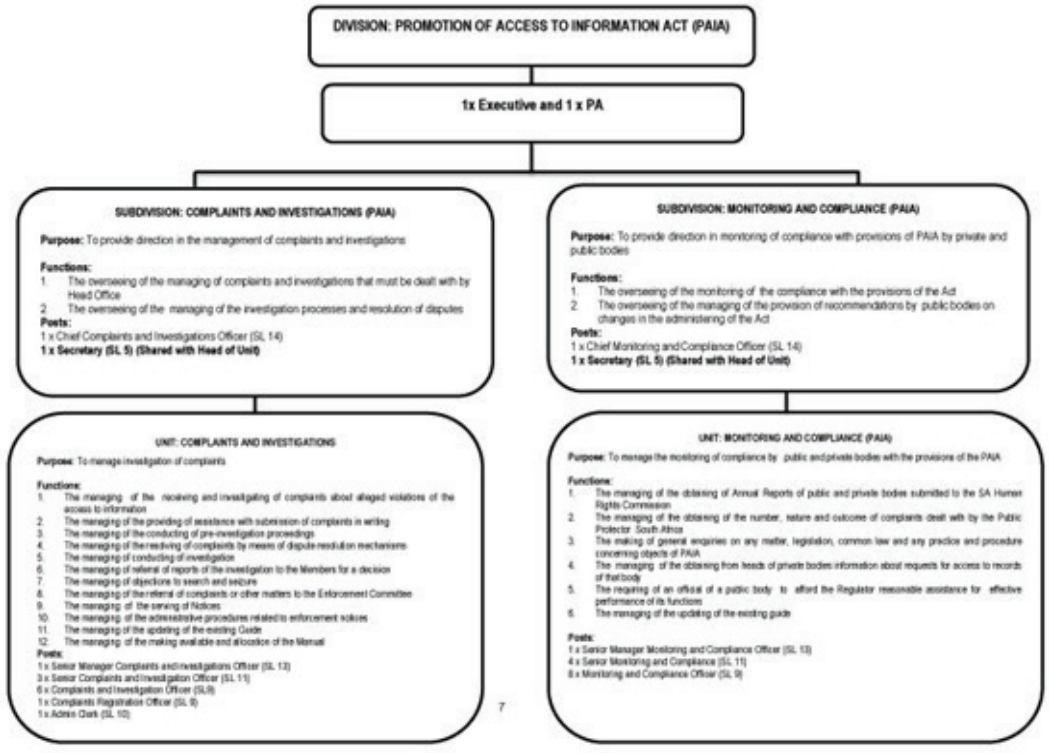

CHAIRPERSON AND MEMBERS
CHIEF EXECUTIVE OFFICER
DIVISION: LEGAL SERVICES, POLICY ADVICE, RESEARCH AND INFORMATION TECHNOLOGY ANALYSIS
Purpose: To ensure the rendering of legal services, policy advice, research and information technology analysis services
Functions:
1. Ensuring the managing of the provision of legal services
2. Ensuring the managing of the provision of policy services
3. Ensuring the managing of the provision of research services
4. Ensuring the managing of the provision of strategic analysis and guidance on complex, varied and sensitive technological issues relevant to the mandate of the Information Regulator (Regulator)
(Refer to page 4 for detailed structure)
DIVISION: EDUCATION AND COMMUNICATION
Purpose: To provide strategic direction for education and communication and to coordinate the POPIA and PAIA functions in the provinces
Functions:
1. Ensuring the provision of education, awareness and stakeholder management services
2. Ensuring the provision of communication and branding services
3. Ensuring the provision of public liaison services
4. Ensuring the provision of media relations, monitoring and analysis services
(Refer to pages 5 for detailed structure)
DIVISION: PROTECTION OF PERSONAL INFORMATION ACT (POPIA)
Purpose: To ensure the promotion of the protection of personal information processed by public and private bodies
Functions:
1. The providing of policy and strategic direction on management of complaints and investigations
2. Ensuring the managing of complaints and the conducting of investigation of complaints in terms of the provisions of POPIA
3. The managing of investigation of complaints that are initiated by the Regulator
4. The managing of the investigation of breaches on the instruction of the Regulator
5. The managing of the conducting of monitoring of compliance with and enforcement of the provisions of the Act
6. The managing of the development of and compliance with codes of conduct
(Refer to pages 6 for detailed structure)
DIVISION: PROMOTION OF ACCESS TO INFORMATION ACT (PAIA)
Purpose: To ensure the effective implementation of the promotion of the constitutional right of access to any information held by the state and by any other person and that is required for the exercise of any rights
Functions:
1. The providing of policy and strategic direction on complaints management to provincial offices
2. Ensuring the managing of complaints and the conducting of investigation of complaints including those that are initiated by the Regulator in terms of the provisions of PAIA
3. Ensuring the managing of conducting of monitoring of compliance with and enforcement of the provisions of the Act by public and private bodies on instruction by the Regulator
(Refer to page 7 for detailed structure)

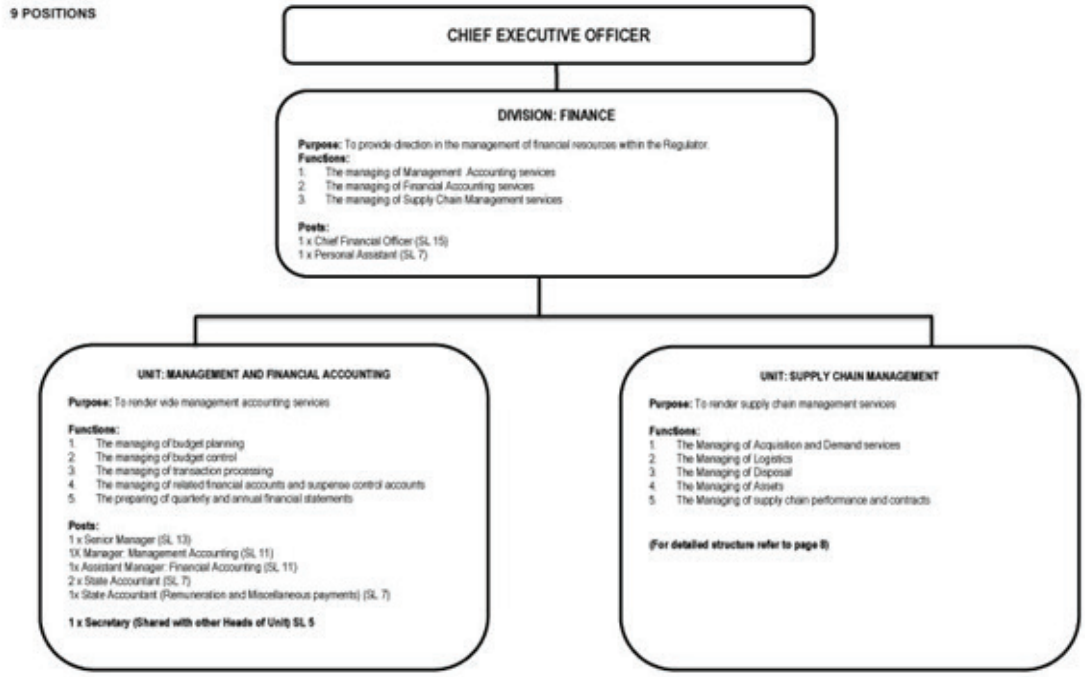

24 POSITIONS
DIVISION: LEGAL, POLICY, RESEARCH AND INFORMATION TECHNOLOGY ANALYSIS
1x Executive Officer and 1 x PA
SUBDIVISION: LEGAL SERVICES
Purpose: To provide direction in the management of the provision of legal services
Functions:
1. The overseeing of the provision of legal advice to the Regulator
2. The overseeing of the providing of the legal representation of the Regulator in litigation matters before courts and negotiations.
Posts:
1x Chief Legal Services Officer (SL14)
1x Secretary (SL 5)(To be shared with the Head of Unit)
SUBDIVISION: POLICY, RESEARCH AND INFORMATION TECHNOLOGY ANALYSIS
Purpose: To provide direction in the management of provision of policy and research services, and guidance on complex, varied and sensitive technological issues relevant to the mandate of the Regulator
Functions:
1. The overseeing of the managing of the development of policy positions on processing of personal information and the conducting of applied research
2. The overseeing of the managing of the provision of research and guidance on complex, varied and sensitive technological issues relevant to the mandate of the Information Regulator
Posts:
1x Chief Policy, Research and Information Technology Analysis (SL 14)
1x Secretary (SL 5) (To be shared the Heads of Unit)
UNIT: LEGAL SERVICES AND LITIGATION
Purpose: To provide legal advice and represent the Regulator in litigation matters before courts and negotiations
Functions:
1. The managing of the provision of legal advice to the Regulator
2. The drafting and negotiation of contracts and management
3. The drafting of legal opinions
4. The conducting of case investigation
5. The conducting of pre-litigation settlement discussions
6. The preparing for trial and appearing in court and other fora
7. The engaging in dispute resolution
8. The conducting of appeals
9. The conducting of disciplinary hearings
Posts:
1x Senior Manager Legal and Litigation (Legal Practitioner) (SL 13)
1x Senior Legal Officer (Legal Practitioner) (SL 11)
1 x Senior Litigation Officer (Legal Practitioner) (SL 11)
2 x Legal Officer (Legal Practitioner) (SL 9)
2x Litigation Officer (Legal Practitioner) (SL 9)
1x Secretary (SL 5) to be shared with Unit Head Policy Research
UNIT: POLICY AND RESEARCH
Purpose: To manage the development of policy and the conducting of applied research
Functions:
1. The managing of the undertaking of research on the desirability of acceptance of international instruments relating to the protection of personal information
2. The managing of research on any other matter including necessary legislative amendments relating to the protection of personal information that should be drawn to Parliament's attention
3. The managing of research to identify gaps in PAIA or any other laws and make recommendations to reform or amend PAIA or any other laws
4. The managing of research to obtain advice from, consult with, and consider proposals or recommendations from parties in connection with the Regulator's functions
5. The managing of research to enquire into any matter including legislation, common law, practice and procedure related to PAIA
6. The managing of the examination of proposed legislation and subordinate legislation or government policy that makes provision for the collection and disclosure of personal information and report the result of that examination to the Minister of Justice and Correctional
7. The managing if the developing of policy guidelines for public and private bodies
8. The managing of the reporting to Parliament on any policy matter affecting the protection of personal information including the need for legislative, administrative or other action necessary to protect the personal information of a data subject
Posts:
1 x Senior Manager: Policy Analysis and Research (SL 13)
1 x Senior Policy Analyst (SL 11)
1 x Senior Researcher (SL 11)
1 x Senior Researcher/d (SL 11)
2 x Policy Analyst (SL 9)
2 x Researcher (SL 9)
UNIT: INFORMATION TECHNOLOGY ANALYSIS
Purpose: To manage the provision of research and guidance on complex, varied and sensitive technological issues relevant to the mandate of the Information Regulator
Functions:
1. The managing of research on technological trends and developments in electronic platforms and digital media
2. The managing of research to assess the impact of technology on protection of personal information in the digital world
3. The managing of research undertaken to monitor developments in information processing and computer technology
4. Providing the Regulator with advice relating to technological matters
Posts:
1 x Senior Manager: Information Technology Analyst and Research (SL 13)
1 x Senior Information Technology Analyst and Researcher (SL 11)
1 x Information Technology Analyst / Advisor (SL 9)
1 x Admin Officer (SL7)

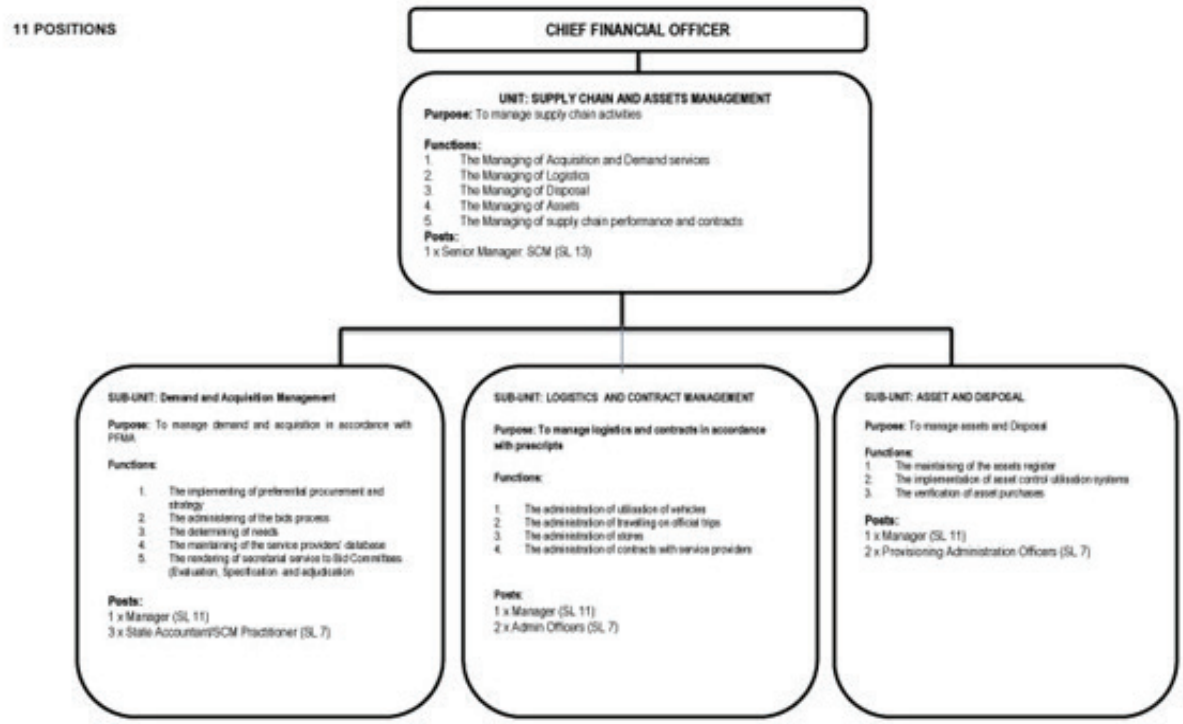
32 POSITIONS

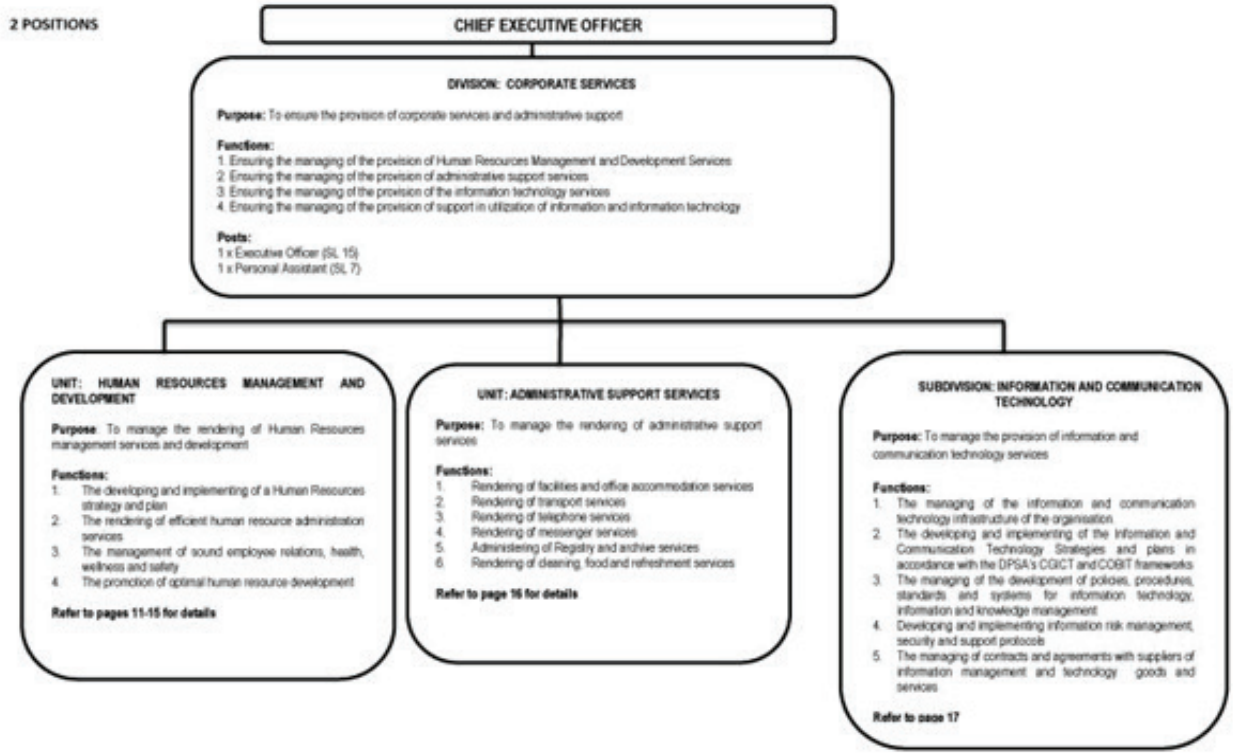


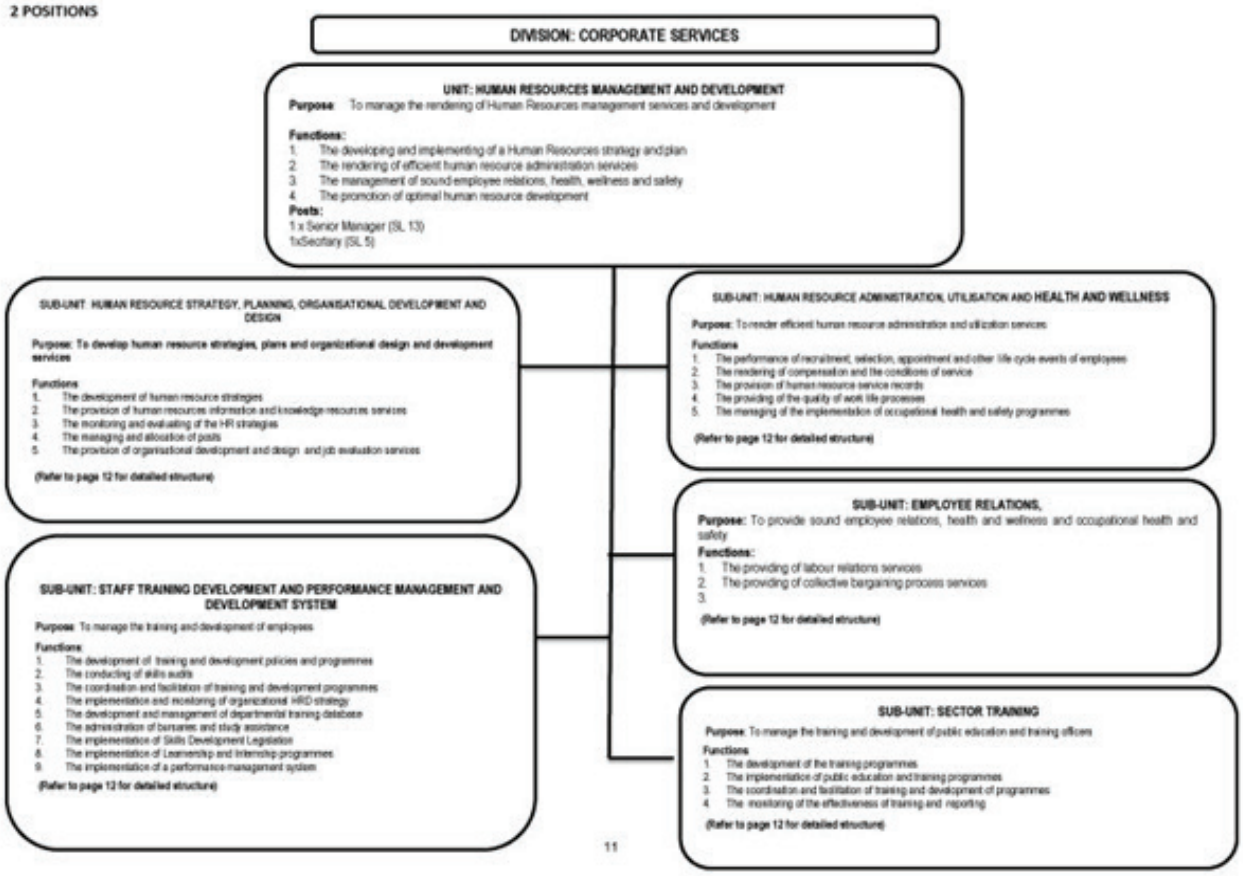
OSITIONS

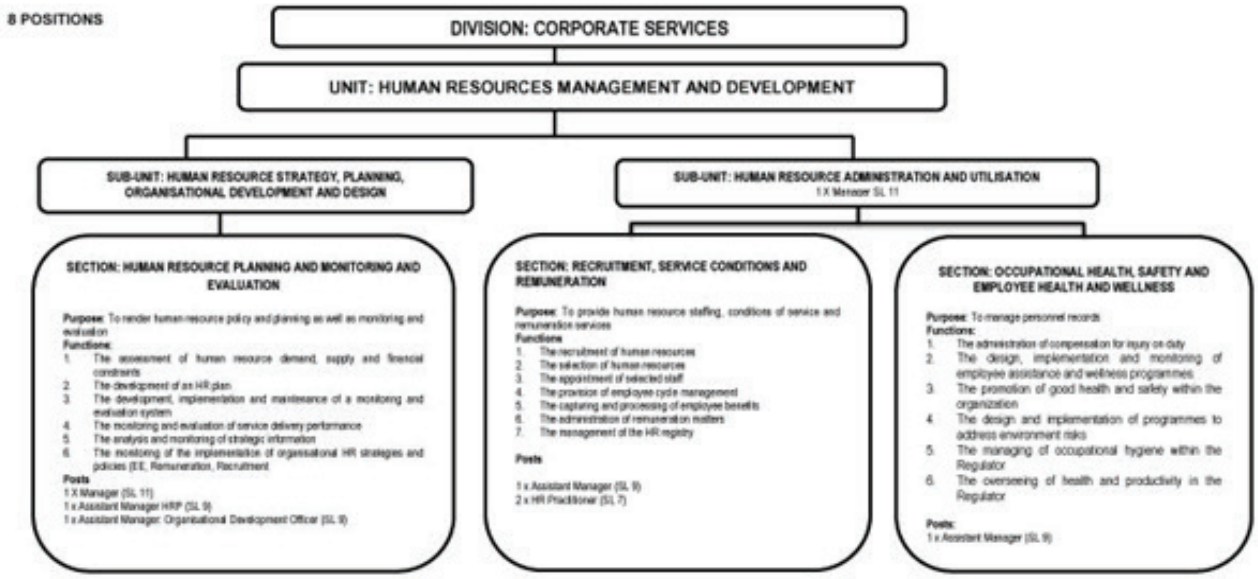


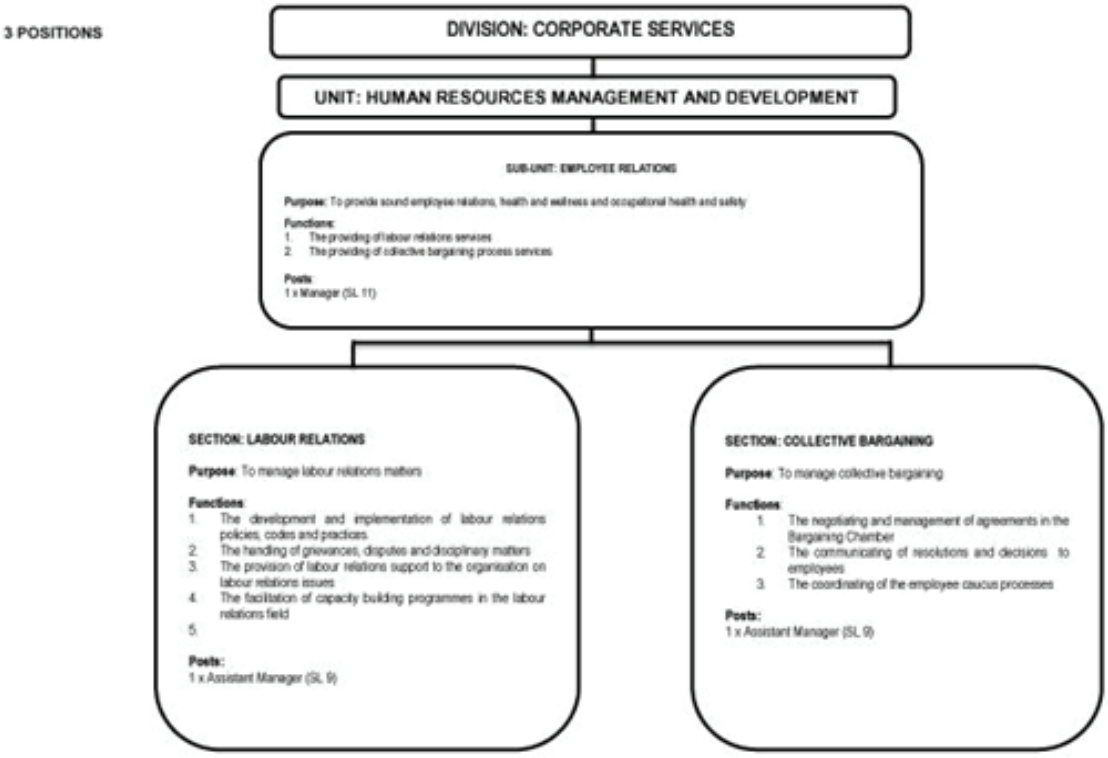

9 POSITIONS
CHIEF EXECUTIVE OFFICER
DIVISION: FINANCE
Purpose: To provide direction in the management of financial resources within the Regulator.
Functions:
1. The managing of Management Accounting services
2. The managing of Financial Accounting services
3. The managing of Supply Chain Management services
Posts:
1 x Chief Financial Officer (SL 15)
1 x Personal Assistant (SL 7)
UNIT: MANAGEMENT AND FINANCIAL ACCOUNTING
Purpose: To render vide management accounting services
Functions:
1. The managing of budget planning
2. The managing of budget control
3. The managing of transaction processing
4. The managing of related financial accounts and suspense control accounts
5. The preparing of quarterly and annual financial statements
Posts:
1 x Senior Manager (SL 13)
1X Manager: Management Accounting (SL 11)
1x Assistant Manager: Financial Accounting (SL 11)
2 x State Accountant (SL 7)
1x State Accountant (Remuneration and Miscellaneous payments) (SL 7)
1 x Secretary (Shared with other Heads of Unit) SL 5
UNIT: SUPPLY CHAIN MANAGEMENT
Purpose: To render supply chain management services
Functions:
1. The Managing of Acquisition and Demand services
2. The Managing of Logistics
3. The Managing of Disposal
4. The Managing of Assets
5. The Managing of supply chain performance and contracts
(For detailed structure refer to page 8)


11 POSITIONS
CHIEF FINANCIAL OFFICER
UNIT: SUPPLY CHAIN AND ASSETS MANAGEMENT
Purpose: To manage supply chain activities
Functions:
1. The Managing of Acquisition and Demand services
2. The Managing of Logistics
3. The Managing of Disposal
4. The Managing of Assets
5. The Managing of supply chain performance and contracts
Posts:
1 x Senior Manager: SCM (SL 13)
SUB-UNIT: Demand and Acquisition Management
Purpose: To manage demand and acquisition in accordance with PPAA
Functions:
1. The implementing of preferential procurement and strategy
2. The administering of the bids process
3. The determining of needs
4. The maintaining of the service providers' database
5. The rendering of secretarial service to Bid Committees (Evaluation, Specification and adjudication
Posts:
1 x Manager (SL 11)
3 x State Accountant/SCM Practitioner (SL 7)
SUB-UNIT: LOGISTICS AND CONTRACT MANAGEMENT
Purpose: To manage logistics and contracts in accordance with prescripts
Functions:
1. The administration of utilisation of vehicles
2. The administration of travelling on official trips
3. The administration of stores
4. The administration of contracts with service providers
Posts:
1 x Manager (SL 11)
2 x Admin Officers (SL 7)
SUB-UNIT: ASSET AND DISPOSAL
Purpose: To manage assets and Disposal
Functions:
1. The maintaining of the assets register
2. The implementation of asset control utilisation systems
3. The verification of asset purchases
Posts:
1 x Manager (SL 11)
2 x Provisioning Administration Officers (SL 7)

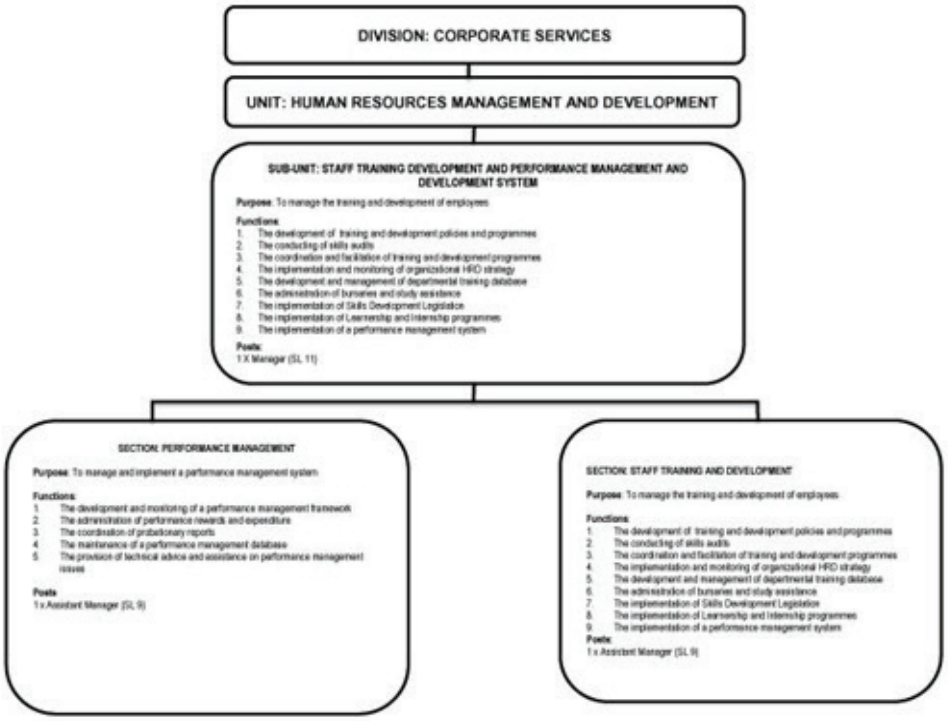

2 POSITIONS
CHIEF EXECUTIVE OFFICER
DIVISION: CORPORATE SERVICES
Purpose: To ensure the provision of corporate services and administrative support
Functions:
1. Ensuring the managing of the provision of Human Resources Management and Development Services
2. Ensuring the managing of the provision of administrative support services
3. Ensuring the managing of the provision of the information technology services
4. Ensuring the managing of the provision of support in utilization of information and information technology
Posts:
1 x Executive Officer (SL 15)
1 x Personal Assistant (SL 7)
UNIT: HUMAN RESOURCES MANAGEMENT AND DEVELOPMENT
Purpose: To manage the rendering of Human Resources management services and development
Functions:
1. The developing and implementing of a Human Resources strategy and plan
2. The rendering of efficient human resource administration services
3. The management of sound employee relations, health, wellness and safety
4. The promotion of optimal human resource development
Refer to pages 11-15 for details
UNIT: ADMINISTRATIVE SUPPORT SERVICES
Purpose: To manage the rendering of administrative support services
Functions:
1. Rendering of facilities and office accommodation services
2. Rendering of transport services
3. Rendering of telephone services
4. Rendering of messenger services
5. Administering of Registry and archive services
6. Rendering of cleaning, food and refreshment services
Refer to page 16 for details
SUBDIVISION: INFORMATION AND COMMUNICATION TECHNOLOGY
Purpose: To manage the provision of information and communication technology services
Functions:
1. The managing of the information and communication technology infrastructure of the organisation
2. The developing and implementing of the Information and Communication Technology Strategies and plans in accordance with the DPSA's CGICT and COBIT frameworks
3. The managing of the development of policies, procedures, standards and systems for information technology, information and knowledge management
4. Developing and implementing information risk management, security and support protocols
5. The managing of contracts and agreements with suppliers of information management and technology goods and services
Refer to page 17


2 POSITIONS
DIVISION: CORPORATE SERVICES
UNIT: HUMAN RESOURCES MANAGEMENT AND DEVELOPMENT
Purpose: To manage the rendering of Human Resources management services and development
Functions:
1. The developing and implementing of a Human Resources strategy and plan
2. The rendering of efficient human resource administration services
3. The management of sound employee relations, health, wellness and safety
4. The promotion of optimal human resource development
Posts:
1 x Senior Manager (SL 13)
1xSecretary (SL 5)
SUB-UNIT: HUMAN RESOURCE STRATEGY, PLANNING, ORGANISATIONAL DEVELOPMENT AND DESIGN
Purpose: To develop human resource strategies, plans and organizational design and development services
Functions
1. The development of human resource strategies
2. The provision of human resources information and knowledge resources services
3. The monitoring and evaluating of the HR strategies
4. The managing and allocation of posts
5. The provision of organisational development and design and job evaluation services
(Refer to page 12 for detailed structure)
SUB-UNIT: HUMAN RESOURCE ADMINISTRATION, UTILISATION AND HEALTH AND WELLNESS
Purpose: To render efficient human resource administration and utilization services
Functions
1. The performance of recruitment, selection, appointment and other life cycle events of employees
2. The rendering of compensation and the conditions of service
3. The provision of human resource service records
4. The providing of the quality of work life processes
5. The managing of the implementation of occupational health and safety programmes
(Refer to page 12 for detailed structure)
SUB-UNIT: EMPLOYEE RELATIONS,
Purpose: To provide sound employee relations, health and wellness and occupational health and safety
Functions:
1. The providing of labour relations services
2. The providing of collective bargaining process services
3.
(Refer to page 12 for detailed structure)
SUB-UNIT: STAFF TRAINING DEVELOPMENT AND PERFORMANCE MANAGEMENT AND DEVELOPMENT SYSTEM
Purpose: To manage the training and development of employees
Functions
1. The development of training and development policies and programmes
2. The conducting of skills audits
3. The coordination and facilitation of training and development programmes
4. The implementation and monitoring of organizational HRD strategy
5. The development and management of departmental training database
6. The administration of bursaries and study assistance
7. The implementation of Skills Development Legislation
8. The implementation of Learnership and Internship programmes
9. The implementation of a performance management system
(Refer to page 12 for detailed structure)
SUB-UNIT: SECTOR TRAINING
Purpose: To manage the training and development of public education and training officers
Functions
1. The development of the training programmes
2. The implementation of public education and training programmes
3. The coordination and facilitation of training and development of programmes
4. The monitoring of the effectiveness of training and reporting
(Refer to page 12 for detailed structure)
11

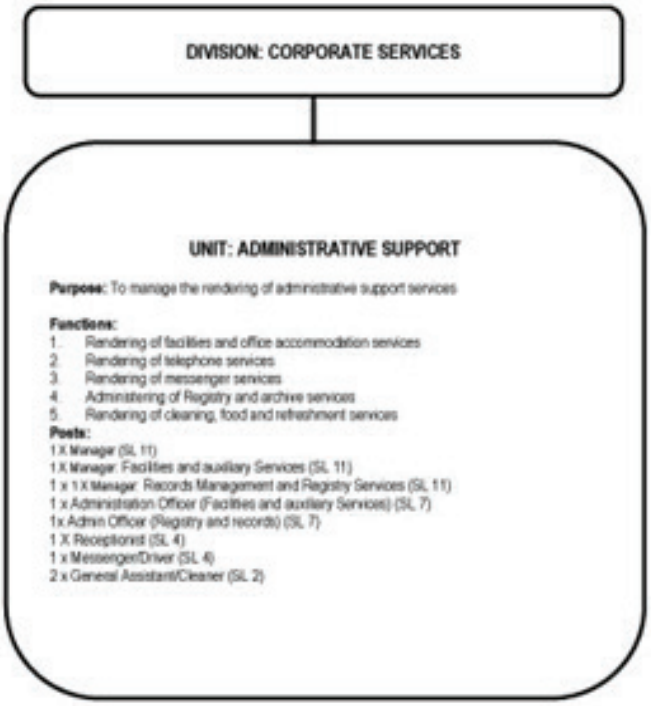

8 POSITIONS
DIVISION: CORPORATE SERVICES
UNIT: HUMAN RESOURCES MANAGEMENT AND DEVELOPMENT
SUB-UNIT: HUMAN RESOURCE STRATEGY, PLANNING, ORGANISATIONAL DEVELOPMENT AND DESIGN
SUB-UNIT: HUMAN RESOURCE ADMINISTRATION AND UTILISATION
1 X Manager SL 11
SECTION: HUMAN RESOURCE PLANNING AND MONITORING AND EVALUATION
Purpose: To render human resource policy and planning as well as monitoring and evaluation
Functions:
1. The assessment of human resource demand, supply and financial constraints
2. The development of an HR plan
3. The development, implementation and maintenance of a monitoring and evaluation system
4. The monitoring and evaluation of service delivery performance
5. The analysis and monitoring of strategic information
6. The monitoring of the implementation of organisational HR strategies and policies (EE, Remuneration, Recruitment
Posts
1 X Manager (SL 11)
1 x Assistant Manager HRP (SL 9)
1 x Assistant Manager: Organisational Development Officer (SL 9)
SECTION: RECRUITMENT, SERVICE CONDITIONS AND REMUNERATION
Purpose: To provide human resource staffing, conditions of service and remuneration services
Functions
1. The recruitment of human resources
2. The selection of human resources
3. The appointment of selected staff
4. The provision of employee cycle management
5. The capturing and processing of employee benefits
6. The administration of remuneration matters
7. The management of the HR registry
Posts
1 x Assistant Manager (SL 9)
2 x HR Practitioner (SL 7)
SECTION: OCCUPATIONAL HEALTH, SAFETY AND EMPLOYEE HEALTH AND WELLNESS
Purpose: To manage personnel records
Functions:
1. The administration of compensation for injury on duty
2. The design, implementation and monitoring of employee assistance and wellness programmes
3. The promotion of good health and safety within the organization
4. The design and implementation of programmes to address environment risks
5. The managing of occupational hygiene within the Regulator
6. The overseeing of health and productivity in the Regulator
Posts:
1 x Assistant Manager (SL 9)


3 POSITIONS
DIVISION: CORPORATE SERVICES
UNIT: HUMAN RESOURCES MANAGEMENT AND DEVELOPMENT
SUB-UNIT: EMPLOYEE RELATIONS
Purpose: To provide sound employee relations, health and wellness and occupational health and safety
Functions:
1. The providing of labour relations services
2. The providing of collective bargaining process services
Posts
1 x Manager (SL 11)
SECTION: LABOUR RELATIONS
Purpose: To manage labour relations matters
Functions
1. The development and implementation of labour relations policies, codes and practices
2. The handling of grievances, disputes and disciplinary matters
3. The provision of labour relations support to the organisation on labour relations issues
4. The facilitation of capacity building programmes in the labour relations field
5.
Posts:
1 x Assistant Manager (SL 9)
SECTION: COLLECTIVE BARGAINING
Purpose: To manage collective bargaining
Functions
1. The negotiating and management of agreements in the Bargaining Chamber
2. The communicating of resolutions and decisions to employees
3. The coordinating of the employee caucus processes
Posts:
1 x Assistant Manager (SL 9)

2 POSITIONS

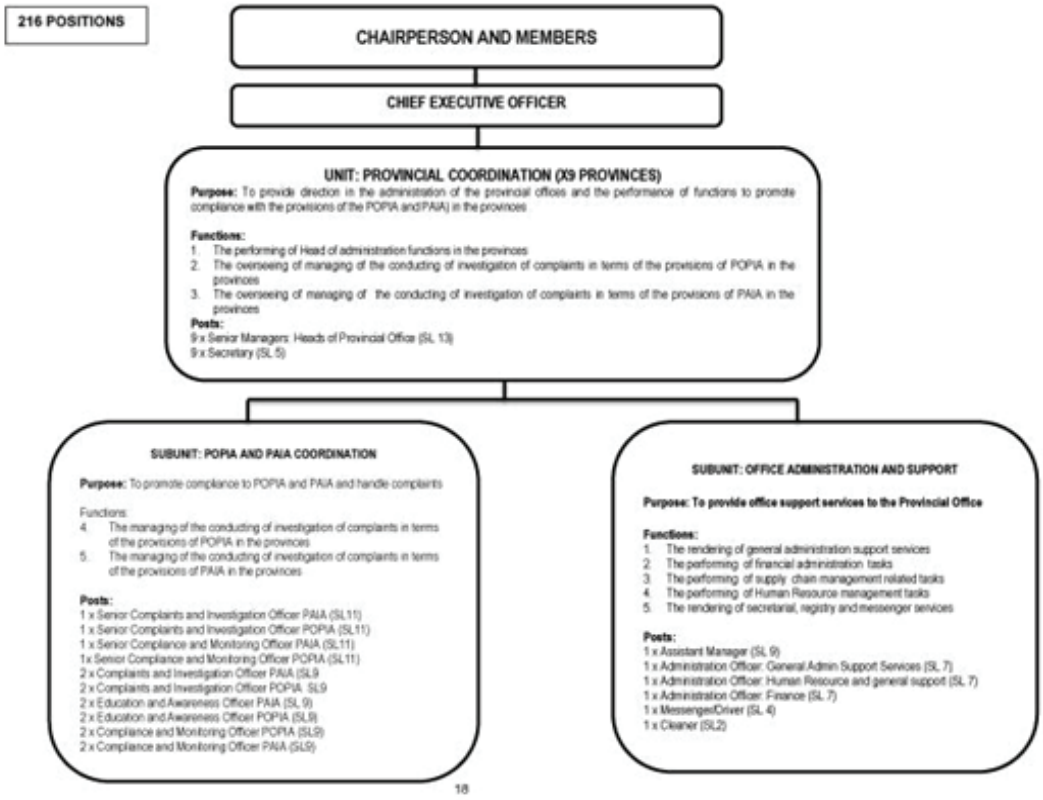


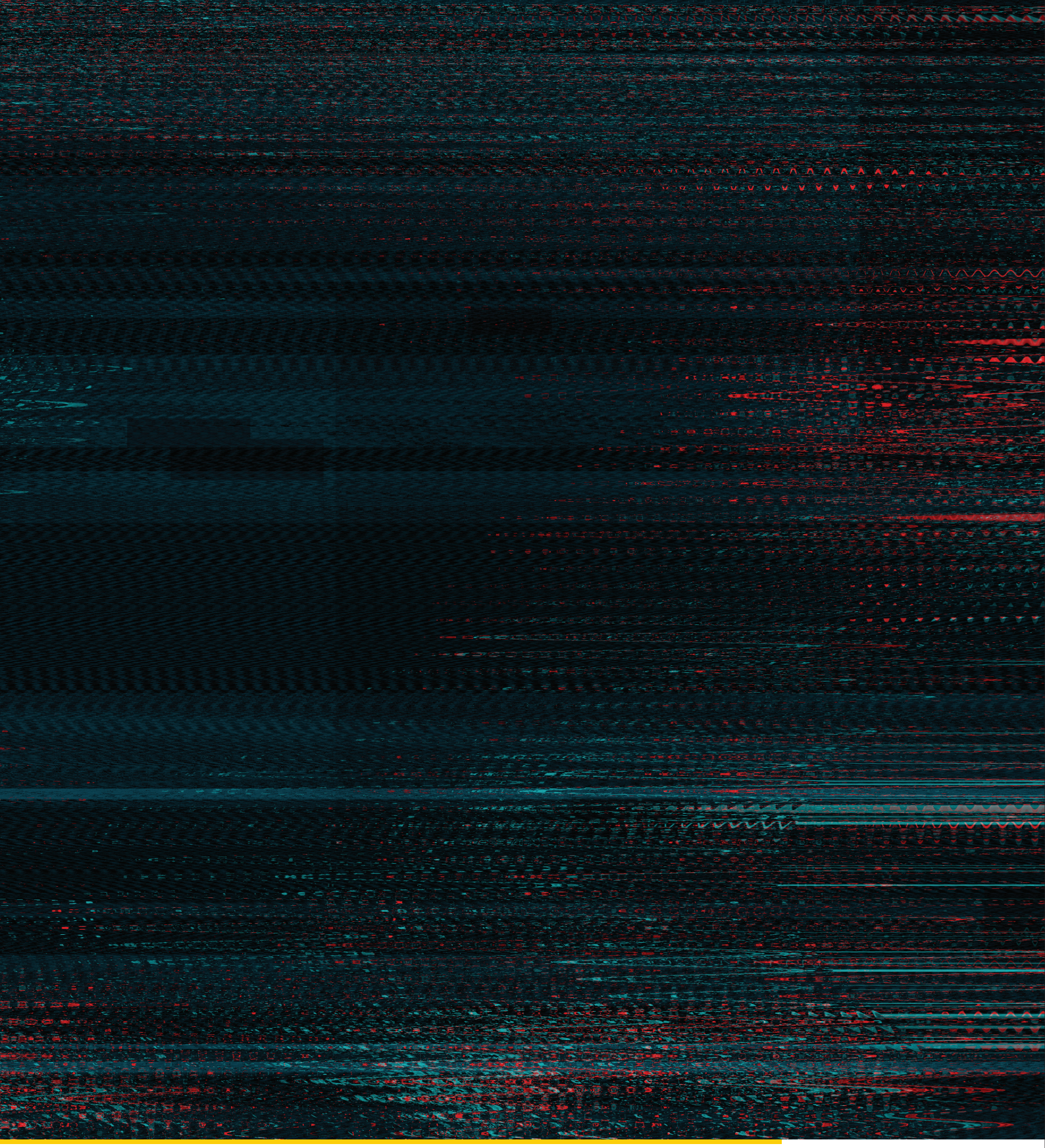
3 POSITIONS


DIVISION: CORPORATE SERVICES
UNIT: ADMINISTRATIVE SUPPORT
Purpose: To manage the rendering of administrative support services
Functions:
1. Rendering of facilities and office accommodation services
2. Rendering of telephone services
3. Rendering of messenger services
4. Administering of Registry and archive services
5. Rendering of cleaning, food and refreshment services
Posts:
1 X Manager (SL 11)
1 X Manager: Facilities and auxiliary Services (SL 11)
1 x 1 X Manager: Records Management and Registry Services (SL 11)
1 x Administration Officer (Facilities and auxiliary Services) (SL 7)
1x Admin Officer (Registry and records) (SL 7)
1 X Receptionist (SL 4)
1 x Messenger/Driver (SL 4)
2 x General Assistant/Cleaner (SL 2)

5 POSITIONS


DIVISION: CORPORATE SERVICES
SUBDIVISION: INFORMATION A ND COMMUNICATION TECHNOLOGY
Purpose: To manage the provision of information and communication technology (ICT) services
Functions:
1. The managing of the developing of the ICT Policy, Strategy and Guidelines in line with King IV, OPSA's CGICT and COBIT
2. information and communication technology infrastructure of the Regulator
3. The managing of the developing of policies, procedures, standards and systems for information technology, information and knowledge management
4. Developing and implementing information risk management, security and support protocols
5. The managing of contracts and agreements with suppliers of information management and technology goods and services
Posts:
1x Chief Information Officer (SL14)
1 x Secretary (SL 5)
UNIT: ICT INFRASTRUCTURE, INFORMATION AND KNOWLEDGE MANAGEMENT
Purpose: To manage the provision of ICT Governance services
Functions:
1. Ensuring the rendering of ICT infrastructure and maintenance services
2. Ensuring the rendering of ICT architecture and project management services
3. Ensuring the management of the ICT contracts and agreements with suppliers
4. Ensuring the rendering of risk management, security and support protocols
5. Ensuring the rendering information and knowledge management services
Posts:
1 x Senior Manager: ICT Infrastructure Services (SL 13)
1 x ICT Specialist (SL 11)
1x ICT Technician (SL 9)


216 POSITIONS
CHAIRPERSON AND MEMBERS
CHIEF EXECUTIVE OFFICER
UNIT: PROVINCIAL COORDINATION (X9 PROVINCES)
Purpose: To provide direction in the administration of the provincial offices and the performance of functions to promote compliance with the provisions of the POPIA and PAIA) in the provinces
Functions:
1. The performing of Head of administration functions in the provinces
2. The overseeing of managing of the conducting of investigation of complaints in terms of the provisions of POPIA in the provinces
3. The overseeing of managing of the conducting of investigation of complaints in terms of the provisions of PAIA in the provinces
Posts:
9 x Senior Managers: Heads of Provincial Office (SL 13)
9 x Secretary (SL 5)
SUBUNIT: POPIA AND PAIA COORDINATION
Purpose: To promote compliance to POPIA and PAIA and handle complaints
Functions:
4. The managing of the conducting of investigation of complaints in terms of the provisions of POPIA in the provinces
5. The managing of the conducting of investigation of complaints in terms of the provisions of PAIA in the provinces
Posts:
1 x Senior Complaints and Investigation Officer PAIA (SL11)
1 x Senior Complaints and Investigation Officer POPIA (SL11)
1 x Senior Compliance and Monitoring Officer PAIA (SL11)
1x Senior Compliance and Monitoring Officer POPIA (SL11)
2 x Complaints and Investigation Officer PAIA (SL9
2 x Complaints and Investigation Officer POPIA SL9
2 x Education and Awareness Officer PAIA (SL 9)
2 x Education and Awareness Officer POPIA (SL9)
2 x Compliance and Monitoring Officer POPIA (SL9)
2 x Compliance and Monitoring Officer PAIA (SL9)
SUBUNIT: OFFICE ADMINISTRATION AND SUPPORT
Purpose: To provide office support services to the Provincial Office
Functions:
1. The rendering of general administration support services
2. The performing of financial administration tasks
3. The performing of supply chain management related tasks
4. The performing of Human Resource management tasks
5. The rendering of secretarial, registry and messenger services
Posts:
1 x Assistant Manager (SL 9)
1 x Administration Officer: General Admin Support Services (SL 7)
1 x Administration Officer: Human Resource and general support (SL 7)
1 x Administration Officer: Finance (SL 7)
1 x Messenger/Driver (SL 4)
1 x Cleaner (SL2)
18



KENYA AMNESTY INTERNATIONAL