Republic of Kenya

Ministry of Information, Communications and Technology

REQUEST FOR COMMENTS ON THE PROPOSED PRIVACY AND DATA PROTECTION POLICY AND BILL ,2018

Recent developments in the ICT sector both locally and internationally have led to the recognition of Privacy as a fundamental human right, making protection of Personal Data a key pillar for human dignity. Further to this, in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a Data Protection framework is critical for Kenya.

The Cabinet Secretary, Ministry of Information, Communications and Technology through Gazette Notice Number 4367 of 11th May 2018 constituted a Taskforce to develop the Policy and Regulatory Framework for Privacy and Data Protection in Kenya. The proposed Policy and Bill will give effect to Article 31 of the Constitution of Kenya, by defining the requirements for the protection of Personal Data.

The Taskforce, in line with the Constitutional requirement to subject proposed Regulatory Framework for public consultation, hereby invites the public to give comments on the proposed Policy and Bill on or before 19th September 2018.

Comments may be submitted through the following email addresses pdp@information.go.ke or pdp@ca.go.ke or through the addresses below:

Mr. Jerome Ochieng
Principal Secretary, ICT &Innovation
Ministry of Information Technology and Communication,
Teleposta Towers
P.O. Box 30025-00100
NAIROBI

Chairperson
Taskforce on Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya.
Communication Authority of Kenya
P.O. Box 14448 00800
NAIROBI

Privacy and Data Protection Policy 2018- Kenya

OUTLINE

1. INTRODUCTION

In the recent years, information has increasingly become a critical resource that has to be managed carefully. Generally, much of today's information consists of personal data relating to individuals. Kenya like other countries has been experiencing technological growth that has impacted the way personal data is generated, processed, stored and distributed. Kenya acknowledges the importance of accessing information and safeguarding it as articulated in the National ICT Policy. As a result, the transformative developments in computing are presenting major concerns for privacy in the way information is processed.

On daily basis, vast amounts of personal data are collected, transmitted and stored globally by ever growing computing and communication technologies. Personal data is a critical resource that drives economic growth and development in this century as oil was in the past. As a result personal data protection is increasingly becoming a critical area that requires to be managed carefully.

Both the public and private sectors collect, use and transfer Personal Data at an unprecedented scale and for multiple purposes. This Personal Data can be put to beneficial use, however, the unregulated and arbitrary use of Personal Data, has raised concerns regarding the privacy and control over such data by the data subject.

The Government of Kenya values the Privacy and the Protection of Personal Data. All the actors involved in the management of Personal Data are expected to respect the requirements of safeguarding Personal Data. Through the Constitution, the Government of Kenya is committed to protecting the privacy of individuals. The Government recognizes that this protection is an essential element in maintaining public trust in entities managing Personal Data and essential for the social-economic development of Kenya in the fourth revolution.

The Constitution of Kenya 2010, under Article 31 recognizes the right to privacy. Consequently, as an effort to further guarantee the same this Policy seeks to outline the legal framework for the enforcing the right to privacy and in particular protection of Personal Data. The Universal

Declaration of Human Rights 1948 and the International Covenant on Civil and Political Rights 1976[1] supports the passage of domestic legislation, on the principles concerning the protection of privacy and individual liberties as set forth in the Declaration and Covenant. Kenya has signed and ratified the Declaration and the Covenant and thus has a moral, ethical and legal duty to ensure that the domestic laws are consistent with the two instruments. In addition, Kenya is party to other conventions that have recognized the right to freedom of expression, including The African Charter on Human and Peoples Rights (ACHPR) and African Union Convention on Cyber Security and Personal Data Protection (2014).

Recent development in jurisprudence internationally has strengthened the recognition of Privacy as a fundamental human right, thereby, making the protection of Personal Data a key pillar in the respect for human dignity. In this light, and in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a Data Protection policy is critical for Kenya. The aim of the policy is to protect personal data in order to guard against misuse and to eliminate the unwarranted invasion of privacy. The fundamental principles of the policy have been largely informed by global practices and the need to bridge the gaps that exist in contextualizing privacy and data protection in technological environment in Kenya.

2. PURPOSE OF THE POLICY

2.1. The purpose of this policy is to lay foundation to enforce Article 31 of the Constitution of Kenya, by developing privacy and data protection laws.

2.2. This policy informs on the management of Personal Data in the information life cycle and the commitment of the Kenya Government to protect the Personal Data including the Personal Sensitive Data.

2.3. The objectives of this policy are:

[1] Article 17.of the International Convention on Civil and Political Rights 1996 provides that No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2.3.1. To inform the development of Privacy and Data Protection laws and facilitate statutory and regulatory compliance, and enhance effective application of the proposed laws in Kenya;

2.3.2. To comply with the international good practice and ensure consistency in practices and procedures in developing and administering the Privacy and Data Protection laws;

2.3.3. To ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in programs and activities involving the collection, retention, use, disclosure and disposal of Personal Data;

2.3.4. To establish the required institutional framework for privacy and data protection; and

2.3.5. To protect children and vulnerable groups

2.4. The expected results of this policy are to develop a legal framework to govern the protection of personal data. This policy will establish an independent oversight authority that will ensure compliance of the policy and sound management practices to safeguard the rights of the data subjects, including children and the vulnerable groups (People with incapacity).

3. DEFINITIONS

3.1 The main terms used in this Policy are defined in Appendix A of this Policy.

4. SCOPE

4.1. This policy sets out the requirements for the protection of Personal Data in manual, electronic or any other form.

4.2. This policy shall be the overarching guiding policy in relation to matters of Privacy and Data Protection.

4.3. The policy applies to all entities in Kenya that undertake processing of data belonging to natural persons.

4.4. This policy applies to any Personal Data which is processed or controlled by a data controller in Kenya or outside Kenya that processes personal data using a data processor inside Kenya.

4.6. The policy applies to all data subjects, whether resident in Kenya or not, whose data is or has been collected or processed by a data controller in Kenya.

5. PRINCIPLES FOR DATA PROTECTION

This section of the policy defines the guiding principles for the processing of personal data. To comply with the policy, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. The principles applied in the Policy are based on the global best practices in data protection.

5.1 Fairness and lawfulness and Transparency

5.1.1. Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

5.1.2 The processing of Personal Data must happen in a lawful way and have a legal or legitimate basis.

5.1.3 Personal data will be considered to have been obtained fairly if the data subject is informed of the name of the data controller and the purpose(s) for processing the personal data or any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair.

5.1.4 Data controller/ processor should be transparent regarding the processing of personal data and inform the data subject in an open and transparent manner. Personal data should only be processed if and only if there is a legitimate purpose for the processing of that personal data. A Data controller/ processor

should practice transparency so that the data subjects will be sufficiently informed regarding the processing of their personal data. When processing personal data, the individual rights of data subject must be protected.

5.2 Purpose Limitation

5.2.1 Personal Data shall be collected for specified, explicit, and legitimate purpose and not further processed in a manner that is incompatible with those purposes.

5.2.2 Personal data must be processed only for the purpose that was defined before the data was collected.

5.2.3 Further processing for archiving purposes in the public interest, scientific interest or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose. Subsequent changes to the purpose are only possible to a limited extent and require legitimate basis.

5.3 Data Minimization

5.3.1. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed.

5.3.2. Before processing personal data, a data controller must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which the data was required.

5.3.3. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law.

5.3.4. Privacy and security should be built and integrated in from the onset in all data management systems that collect and process personal data. Such systems should have privacy incorporated by design or default.

5.4 Storage Limitation

5.4.1 Personal data shall not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed.

5.4.2 There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the archive has evaluated the data to determine whether it must be retained for historical purposes subject to adequate protection against access or use for unauthorized purpose.

5.5 Accuracy

5.5.1 Personal data on file must be correct, complete, and be kept up to date.

5.5.2 Suitable steps must be taken by a data controller to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

5.6 Confidentiality and Integrity

5.6.1 Personal data must be processed securely to retain confidentiality and integrity in consistency, accuracy, and trustworthiness over its entire life cycle.

5.6.2 Steps must be taken to ensure that data cannot be altered by unauthorized entities or people.

5.6.3 Security of personal data shall be preserved by establishing suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

5.7 Accountability

5.7.1All Data Controllers/Processors shall be responsible for personal data protection, and be able to demonstrate compliance to the principles on Data Protection.

6. DATA SUBJECT RIGHTS

6.1. There may be limitations on data rights of data subject when required by the law or when there are competing rights and therefore would require an assessment based on the facts and circumstances. A data subject (an individual to whom personal data relates) has the following rights**:**

6.1.1. Right to access to personal information;

6.1.2. Right to information as to whether personal data is being processed;

6.1.3. The right to rectification if the information held is inaccurate or incomplete or requires to be updated;

6.1.4. The right to restrict processing of their personal data;

6.1.5. The right to object decisions solely based on automated processing circumstances such as automated processing, publication/ processing of sensitive personal data profiling which produces legal effects or significantly affects data subject;

6.1.6. The right to complain (as would be appropriate to the controller, processor or regulator).

6.1.7. The right to object the processing of their data for direct-marketing purposes;

6.1.8. The right to data portability;

6.1.9. The right to be forgotten/ the right to erasure will require mechanisms to be put in place to ensure this right;

6.1.10. Right to appropriate security safeguards where personal data is being archived for various purposes;

6.1.11. The right to appropriate security safeguards in cross border transfer of personal data; and

6.1.12. The right of the data subject can withdraw their consent at any time without detriment to their interests

7. LEGAL GROUNDS FOR PROCESSING

7.1 Data protection policy strives to ensure that collecting, processing, transmitting, using, storing and disposal of personal data is permitted only under lawful and legitimate basis.

7.2 Consent

7.2.1. Data Controller/Data Processor will obtain consent from Data Subject on the processing of Personal Data including sensitive personal data.

7.2.2. Data subject should clearly understand why his/her information is needed, who it will be shared with, and the possible consequences of them agreeing or refusing the proposed use of the data.

7.2.3. The processing of personal data for a child shall be done only with the consent of the child's parent or guardian.

7.3 Exceptions

7.3.1. The policy acknowledges that there will be exceptional circumstances where personal data can be processed without the data subjects consent. There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances.

7.4 Third party data processing

7.4.1. Personal data shall not be disclosed or processed by a third party except when required by law or the third party Data Processing Agreement has been approved and signed by the Data Controller and the Data Processor (i.e. the third party) and the Data subject is aware of this arrangement.

7.5 Cross Border Transfer

7.5.1. This policy may allow personal data to be transferred to other countries or entities if such countries or entities have met the adequate safeguards spelt out in this policy for maintaining the required protection for the privacy rights of the data subjects in relation to their personal data.

7.6 Big Data and Analytics

7.6.1 The use of big data and analytics is permitted subject to the processes involved in complying with the requirements of the Data Protection Laws.

8. OBLIGATIONS FOR DATA PROCESSING

8.1 Entities handling personal data must comply with the data protection principles articulated in section 5. This section of the policy defines the key requirements of data controller and data processor.

8.2. A data controller's obligations

8.2.1. Inform the data subject about the data processing activities and the rights of data subject under the law;

8.2.2. Specify the purposes for which data is to be used;

8.2.3. Should only collect and use personal data in accordance with lawful conditions;

8.2.4. Should keep updated Records of Processing activities, making them available to the Office of the Data Protection Regulator and to the data subject on request;

8.2.5. Rely on consent as a condition for processing personal data only where: The data controller first obtain the data subject's specific, informed and freely given consent;

8.2.6. Notify the regulator of any data breach;

8.2.7. Register with the data protection regulator;

8.2.8. Designate a Data Protection Officer to handle all matters of data protection;

8.2.9. Conduct data protection impact assessment;

8.2.10. Develop internal data protection policies and procedures;

8.1.11. Provide privacy notices/notifications to data subject before personal data is collected or used; and

8.1.12. The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process that data except on instructions from the controller, unless required to do so by law.

8.2 Joint Data Controllers

8.2.1. Two or more controllers may jointly determine the purposes and means of processing personal data.

8.2.2. Joint controllers shall in a transparent manner determine the respective responsibilities for compliance and exercise the rights of the data subject.

8.2.3. The arrangement of joint data controllers shall duly reflect the respective roles and relationships of the joint controllers Vis-a Vis the data subject. The essence of the arrangement shall be made available to the data subject.

8.3 Data protection by design and default

8.3.1. Privacy should be built in from the outset in all data management systems including critical systems.

8.3.2. Data Controller should conduct privacy and information audit and risk assessment at each stage of every project or initiative involving collection, processing, transmitting, storage, use and disposal of personal data and in managing upgrades or enhancements to systems and processes used to handle personal data.

8.3.3. The Data Controller/Data Controller should apply appropriate personal data security controls such as encryption, anonymization and Pseudonymisation of personal data.

8.4 Data Controller/Data Processor must protect personal data

8.4.1. Data Controller/ Data Processor is required take appropriate technical, organizational and other measures to prevent unauthorized or unlawful processing or accidental loss or

destruction of, or damage to, as well as unauthorised access, disclosure, copying, use, or modification of personal information.

8.5 Data controller must manage any personal data breaches promptly and appropriately:

8.5.1. All data breaches are to be reported to the Data Protection Regulator. The reporting must be done expeditiously.

8.5.2 The frequency and severity of the breach will determine the next level of intervention.

8.6 Data controller shall uphold rights of data subject:

8.6.1. Data controller is required to provide a copy of the information comprising personal data of a data subject at minimal cost and within a reasonable time of his/her request.

8.6.2. The Data Controller may disapprove a request for personal data, but must provide reasons for denying the request.

8.6.3. When Data subject successfully demonstrates the inaccuracy or incompleteness of data, Data Controller will amend the data as required within a reasonable time.

8.7 Challenge to Compliance

8.7.1. Data Controller is required to put mechanisms and processes in place to receive and address complaints or inquiries about its policies and procedures relating to the handling of data including personal data.

9. INSTITUTIONAL FRAMEWORK

The policy is under the responsibility and accountability of the Cabinet Secretary in charge of matters Information, Communications and Technology. The compliance to this policy shall be ensured by the Office of Data Protection Regulator. This policy provides mechanism on redress for administration, processing and appeals.

9.1. Office of the Data Protection Regulator

The Office of Data Protection Regulator is an Independent Public Office responsible for upholding the Bill of Rights and enforcing the application of Article 31 of the Constitution on the protection of Right to Privacy. The Office of Data Protection Regulator will be charged with the responsibility of;

- Enforcing data protection procedures;
- Receiving complaint on personal data breaches;
- Central registration of data controllers;
- Monitor and enforce the application of the laws and the regulations;
- Advise and promote awareness on data protection;
- Administrate data breaches and other infringements;
- Facilitate in investigation data breaches and other infringements;
- Define conditions for imposing administrative fines;
- Cooperate with other Supervisory Authorities and other relevant bodies in data protection; and
- Set and promote self-regulatory mechanisms

10. CONSEQUENCES OF NON COMPLIANCE

10.1. It is the responsibility of all entities that process personal data to adhere to this Data Protection Policy. Misuse of personal data, through loss, disclosure, or failure to comply with the data protection principles and the rights of data subjects, shall result in significant legal, and financial damages. This may include penalties specified in the Law.

11. MONITORING AND EVALUATION

11.1. The Office of the Data Protection Regulator will set up framework to detect and deter data breaches;

11.2. Data controller will designate a Data Protection Officer to monitor new and on-going data protection risks and update the relevant risk register of Data Controller;

11.3. Data Protection Officer will liaise with the Office of the Data Protection Regulator to ensure that all the risks related to data protection are captured in a register and addressed appropriately;

11.4. Data Protection Officer will make regular compliance reports to the Office of the Data Protection Regulator on data protection;

11.5. A data controller is required to develop internal data protection and audit policies, guidelines and procedures to manage privacy and data protection risks and compliance with relevant controls as required in this Policy. The internal policies should align with this policy and any other Government policy or any national legislation on Privacy and Data Protection; and

11.6. The Office of the Data Protection Regulator shall prepare and present annual data protection report to the National Assembly.

12. IMPLEMENTATION

12.1. The implementation of this Policy and Law will be gradual and in phases, and will start by having the policy approved. The Privacy and Data Protection Bill will be approved to become law. The other critical development of this Policy will involve establishment of the Office of Data Protection Regulator.

12.2. The funding of the Office will be drawn from the National Treasury.

13. REVIEW

13.1 This policy shall be reviewed every five (5) years, or more frequently if appropriate, to be consistent with future developments, industry trends and/or any changes in legal or regulatory requirements.

14. RELATED POLICIES

14.1 Data Protection Policy has referenced the following policy:

- National ICT Policy

Appendix A: Definitions of key terms

This part of the policy defines key terms

Anonymisation: Irreversible removal of personal identifiers from information so that the data subject is no longer identifiable.

Collection: The act of gathering, acquiring, or obtaining Personal Data from any source, including third parties and whether directly or indirectly by any means.

Consent: Any freely given specific and informed indication of the wishes of the data subject by which they signify their agreement to personal data relating to them being processed.

Control: An agency, natural or legal person, public authority, organisation or any other body which alone or jointly with others has the power to determine the purposes and means of the processing of data, and the manner in which the data is processed.

Critical system: Any system whose 'failure' could threaten human life, the system's environment or the existence of the organisation which operates the system. Such systems include but not limited to electric grid, manufacturing system, transportation system, financial institutions, water treatment facilities and water supply systems.

Data: **A**ll data including personal data in electronic or manual form.

Data controller: A person who either alone or jointly with other persons or in common with other persons or as a legal duty determines the purpose for and the manner in which data is processed or is to be processed.

Data Processor: In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data Subject: A Natural person whose personal data is held by the data controller.

Disclosure: Making data available to others outside the Agencies

Encryption: The process of converting information or data into code, to prevent unauthorised access

Investigation — means an investigation relating to:
(a) A breach of this policy;
(b) A contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or
(c) A circumstance or conduct that may result in a remedy or relief being available under any law;

National Interest — includes national security, defense, public security, the conduct of international affairs and the financial and economic interest of Kenya;

Notification: Notifying the Data Protection Regulator/Data Subject about the data breach.

Office of the Data Protection Regulator / Supervisory authority: An independent public authority established by state to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance.

Personal data: Any information relating to an identified or identifiable natural person (Data Subject) an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, passport number, birth certificate or to one or more specific factors like physical or physiological.

Processing: Any operation performed on personal data, such as collecting, creating, recording, structuring, organising, storing, retrieving, accessing, using, seeing, sharing, communicating,

disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data
Restriction of processing: The marking of stored personal data with the aim of limiting their processing in the future.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymised data is therefore re-identifiable and falls within the definition of personal data

Sensitive personal data means personal data as to:

(a) The racial, ethnic or social origin,
(b) The political opinions or the religious or conscience belief, culture dress language or birth) of the data subject.
(c) Gender
(d) Whether the data subject is a member of a trade-union.
(e) disability
(f) Sexual life or orientation
(g) Pregnancy
(h) Colour
(i) Age
(j) Marital status
(k) Health Status
(l) the commission or alleged commission of any offence by the data subject, or
(m) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
(n) Biometrics (where needed for identification)

Third Party-Third party, in relation to personal data, means any person/entity other than the data subject, the data controller, or data processor or other person authorized to process data for the data controller or processor

Vulnerable Group/ people with incapacity – Any member of the society who is at a risk of being discriminated because of their physical, mental, physiological and social conditions. Such members usually have difficulties giving free and informed consent.

THE DATA PROTECTION BILL, 2018

ARRANGEMENT OF CLAUSES

Clause

PART I—PRELIMINARY

PART II— OFFICE OF THE DATA PROTECTION COMMISSIONER

PART III—REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

PART IV— PRINCIPLES AND OBLIGATIONS OF PEROSNAL DATA PROTECTION

PART IX — FINANCIAL PROVISIONS

PART X — OFFENCES AND MISCELLANEOUS PROVISIONS

THE DATA PROTECTION BILL, 2018

A Bill for

AN ACT of Parliament to give effect to Article 31(c) and (d) of the Constitution; to establish the Office of the Data Protection Commissioner; to regulate the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes—

ENACTED by Parliament of Kenya, as follows—

PART I – PRELIMINARY

Short title.

1. This Act may be cited as the Data Protection Act, 2018.

Interpretation.

2. In this Act –

"anonymisation" means the irreversible removal of personal identifiers from personal data so that the data subject is no longer identifiable;

''biometrics'' means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, deoxyribonucleic acid analysis, retinal scanning and voice recognition;

"Cabinet Secretary" means the Cabinet Secretary responsible for matters of information, communication and technology;

"consent" means any voluntary, specific and informed expression of will of a data subject to process personal data;

"Cross-border processing" means —

(a) processing of personal data by a data controller or data processor who is outside Kenya; or

(b) processing of personal data while outside Kenya but which substantially affects or is likely to substantially affect the data subject in Kenya;

"Data Commissioner" means the Data Protection Commissioner appointed under section 9;

"data controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data;

"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"Data Subject" means an identified or identifiable natural person who is the subject of personal data;

"filing system" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"health data" means data related to the state of physical or mental health of the Data Subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data whch associates the Data Subject to the provision of specific health services;

"Identifiable natural person" means a person who can be identified directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity;

"personal data" means any information relating to an identified or identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"Office" means the office of the Data Protection Commissioner;

"processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as –

(a) collection, recording, organisation, structuring;
(b) storage, adaptation or alteration;

(c) retrieval, consultation, use;
(d) disclosure by transmission, dissemination, or otherwise making available; or
(e) alignment or combination, restriction, erasure or destruction;

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

"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"Register" means the register as established and maintained by the Data Commissioner under section 19;

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"Sensitive personal data" means data revealing the natural person's race, health status, ethnic social origin, political opinion, belief, personal preferences, location, genetic data, biometrics, sex life or sexual orientation, personal financial expenditures, of the data subject;

"third Party" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the direct authority of the data controller or data processor, are authorised to process personal data; .

Object and purpose.

3. The object and purpose of this Act is to—

(a) give effect to the provisions of Article 31 (c) and (d) Constitution;
(b) regulate the processing of personal data;
(c) ensure handling of personal data of a data subject is guided by the principles of: lawful processing; minimisation of

collection; restriction to further processing; data quality; and security safeguards;

(d) establish the legal and institutional mechanism to protect personal data; and

(e) provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

Application

4. (1) This Act applies to the processing of personal data —

(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means: provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;

(b) to a data controller or data processor who –

(i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

(ii) not established or ordinarily resident in Kenya, but uses equipment in the Kenya for processing personal data, other than for the purpose of transit through the country;

(2) This Act shall not apply to –

(a) the exchange of information between government departments and public sector agencies where such exchange is required on a need-to-know basis;

(b) the processing of personal data by an individual in the course of a purely personal or household activity; or

(c) Processing of personal data exempted under section Part VII.

PART II – OFFICE OF DATA PROTECTION COMMISSIONER

Establishment of the Office

5. (1) There is established the Office of the Data Protection Commissioner which shall be a body corporate with perpetual succession and a common seal and, in its corporate name, be capable of—

(a) suing and being sued;

(b) taking, purchasing or otherwise acquiring, holding, charging or disposing of movable and immovable property;

(c) entering into contracts; and

(d) doing such other legal acts necessary for the proper performance of the functions of the Office.

(2) The Office of Data Protection Commissioner is established and designated as a State Office and shall be deemed as such in accordance with Article 260 (q) of the Constitution.

(3) The Office shall comprise the Data Protection Commissioner as its statutory head and accounting officer, and other staff appointed by the Data Commissioner

(4) The Office shall ensure reasonable access to its services in all parts of the Republic

(5) The Data Commissioner may establish such Directorates as may be necessary for the better carrying of the functions of the Office.

Appointment of the Data Commissioner

6. (1) The Data Commissioner shall be appointed by the Cabinet Secretary on a competitive basis and on such terms and conditions as may be specified in the instrument of appointment.

(2) To be qualified to be the Data Commissioner, a person shall –

(a) have extensive knowledge of data privacy or at least ten year experience in fields of data science, law, information technology or any other relevant qualifications and experience related to the functions of the Office; and

(b) meets the requirements of Chapter 6 of the Constitution; or

(3)The Data Commissioner holds office for a term of six years and shall not be eligible for a re-appointment.

Functions of the Data Protection Commissioner.

7. (1) The functions of the Data Commissioner shall be to—

(a) oversee the implementation of and be responsible for the enforcement of this Act;

(b) establish and maintain a Register of data controllers and data processors;

(c) exercise control on all data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(d) promote self-regulation among data controllers and data processors;
(e) receive and investigate any complaint by any person on infringements of the rights under this Act;
(f) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;
(g) carry out inspections of public and private entities with a view to evaluating the processing of personal data;
(h) ensure country's compliance on data protection obligations under international conventions;
(i) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;
(j) perform such other functions as may be prescribed by any other law or as considered necessary for the promotion of object of this Act.

(2) In the exercise of his functions under this Act, the Data Commissioner shall act independently and shall not be subject to the direction or control of any other person or authority.

Powers of the Data Commissioner

8. (1) The Data Commissioner shall have all the powers necessary for the performance of the functions under this Act.

(2) Without prejudice to the generality of subsection (1), the Data Commissioner shall have power to—

(a) conduct investigations on own initiative, or on the basis of a complaint made by a third party;
(b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate;
(c) facilitate conciliation, mediation and negotiation on disputes arising from this Act;
(d) issue summons to a witness for the purposes of investigation;
(e) request any person that is subject to this Act to provide explanations, information and assistance in person and in writing;

(f) undertake any activity necessary for the fulfilment of any of the functions of the Office; and

(g) perform any function and exercise any powers prescribed by any other legislation, in addition to the functions and powers conferred by the Constitution

(3) The Data Commissioner may enter into association with other bodies or organisations within and outside Kenya as appropriate in furtherance of the object of this Act.

Delegation Data Commissioner

9. (1) The Data Commissioner may, subject to such conditions as the Data Commissioner may impose, delegate any power conferred under this Act or any other written law to—

(a) an employee of the Office;

(b) A regulator or professional body, or any other public body established through an Act of parliament; or

(c) A recognised self-regulatory organisation.

Vacancy in the Office of the Data Commissioner.

10. The Office of the Data Commissioner shall become vacant, if the Data Commissioner—

(a) dies;

(b) by notice in writing addressed to the Cabinet Secretary resigns from office;

(c) is convicted of an offence and sentenced to imprisonment for a term exceeding six months without the option of a fine;

(d) is removed from Office in accordance with the provisions of section 11.

Removal of the Data Commissioner

11. (1) The Data Commissioner may be removed from Office on grounds of—

(a) non-compliance with Chapter Six of the Constitution;

(b) inability to perform the functions of the Office arising from mental or physical incapacity;

(c) gross misconduct or misbehaviour;

(d) incompetence; or

(e) bankruptcy.

(2) Prior to removal under subsection (1), the Data Protection Commissioner shall be–

(a) informed, in writing, of the reasons for the intended removal; and

(b) offered an opportunity to put in a defence against any such allegations.

Staff of the Office

12. The Data Commissioner may appoint such staff as may be necessary for the proper discharge of the functions under this Act or any other law, on terms as the Data Commissioner, in consultation with the Salaries and Remuneration Commission, may determine.

Duty of confidentiality.

13. (1)The Data Commissioners and the authorised officers of the Office shall take the oath set out in the Schedule on their appointment.

(2) The Data Commissioner, or any staff of the Office, shall not, unless with lawful authority, disclose any information obtained for the purposes of this Act.

Protection from personal liability.

14. The Data Commissioner or any employee or agent of the Office, shall not be held personally liable for having performed their function in accordance with this Act.

PART III— REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Registration of data controllers and data processors.

15. Subject to exemptions provided under this Act, no person shall act as a data controller or data processor unless registered with the Data Commissioner

Application for registration.

16. (1) Every person who intends to act as a data controller or data processor shall apply to the Data Commissioner in prescribed form.

(2) An application under subsection (1) shall provide the following particulars –

(a) a description of the personal data to be processed by the data controller or data processor, and of the category of data subjects, to which the personal data relates;

(b) a statement as to whether the data controller or data processor is likely to hold any categories of sensitive personal data;

(c) a description of the purpose for which the personal data is to be processed;

(d) a description of any recipient to whom the data controller or data processor intends or may intend to disclose the personal data;

(e) the name, or a description of, any country to which the proposed data controller intends or may wish, directly or indirectly, to transfer the personal data;
(f) statement as to a representative for the purposes of this Act and details of such representative;
(g) a general description of the risks, safeguards, security measures and mechanisms to ensure the protection of personal data; and
(h) any other details as may be prescribed by the Data Commissioner.

(3) A data controller or data processor who knowingly supplies any false or misleading detail under subsection (1) commits an offence.

(4) The Data Commissioner shall issue a certificate of registration to an applicant who satisfies the criteria to be registered as a data controller or data processor.

(5) Where there is a change in any particular outlined under subsection (2), the data controller or data processor shall notify the Data Commissioner of such change in prescribed period.

(6) On receipt of a notification under subsection (5), the Data Commissioner shall amend the respective entry in the Register.

(7) A data controller or data processor who fails to comply with the provisions of subsection (5) commits an offence.

Duration of the registration certificate.

17. A registration certificate issued under section 16 shall be valid for a period of three years and the holder may apply for the renewal within a prescribed period.

Register of data controllers and data processors.

18. (1) The Data Commissioner shall keep and maintain a Register of the registered data controllers and data processors.

(2) The Data Commissioner may, at the request of a data controller or data processor, remove any entry in the Register which has ceased to be applicable.

(3) The Register shall be a public document and available for inspection by any person.

(4) A person may request the Data Commissioner for a certified copy of any entry in the Register.

Cancellation or variation of the certificate

19. The Data Commissioner may, upon issuance of a notice to show cause, cancel or vary terms and conditions of the certificate of registration where—

(a) any information given to by the applicant is false or misleading; or
(b) the holder of the registration certificate, without lawful excuse fails to comply with any —
(i) requirement of this Act; or
(ii) term or condition specified.

Compliance and audit

20. The Data Commissioner may carry out periodical audits of the systems held by the data controllers or data processors to ensure compliance with this Act.

Designation of the Data Protection Officer.

21. (1) A data controller or data processor may designate or appoint a data protection officer on such terms and conditions as the data controller or data processor may determine, where—
(a) the processing is carried out by a public body or private body, except for courts acting in their judicial capacity;

(b) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the data controller or the data processor consist of processing on a large scale of sensitive categories of personal data.

(2) A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.

(3) A group of entities may appoint a single data protection officer provided that such officer is easily accessible by each entity.

(4) Where a data controller or a data processor is a public body, a single data protection officer may be designated for several such public bodies, taking into account their organisational structures.

(5) A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

(6) A data controller or data processor shall publish the contact details of the data protection officer and communicate them to the Data Commissioner.

(7) The responsibility of a data protection officer shall be to —
(a) advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law;
(b) ensure on behalf of the data controller or data processor that this Act is complied with;
(c) facilitate capacity building of staff involved in data processing operations;
(d) provide advice on data protection impact assessment; and
(e) Cooperate with the Data Commissioner and any other authority on matters relating to data protection.

PART IV–PRINCIPLES AND OBLIGATIONS OF PERSONAL DATA PROTECTION

Principles of data protection

22. (1) Every data controller or data processor shall ensure that personal data is–
(a) Processed in accordance of the right of privacy of the data subject;
(b) processed lawfully, fairly and in a transparent manner in relation to any data subject
(c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
(d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
(e) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data are erased or rectified without delay;
(f) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected;
(g) only released to a third party only with the consent of the data subject; and
(h) not transferred outside Kenya, unless there is adequate proof of adequate data protection laws by the recipient country.

Rights of a Data Subject.

23. (1) A data subject has a right to —
(a) be informed of the use to which their personal data is to be put;
(b) access their personal data in custody of data controller or data processor;

(c) object to the collection or processing of all or part of their personal data;
(d) correction of false or misleading data; and
(e) deletion of false or misleading data about them.

Exercise of rights of data subjects

24. A right conferred on a data subject may be exercised –
(a) where the data subject is a minor, by a person who has parental authority or by a guardian;
(b) where the data subject is physically or mentally unfit, by a person a duly authorised guardian or administrator; or
(c) in any other case, by a person duly authorised by the data subject.

Collection of personal data.

25. (1) A data controller or data processor shall collect personal data directly from the data subject.

(2) Despite subsection (1), personal data may be collected indirectly where—
(a) the data is contained in a public record;
(b) the data subject has deliberately made the data public;
(c) the data subject has consented to the collection from another source
(d) the data subject has an incapacity, the guardian appointed has consented to the collection from another source;
(e) the collection from another source would not prejudice the interests of the data subject;
(f) collection of data from another source is necessary-
(i) for the prevention, detection, investigation, prosecution and punishment of crime;
(ii) for the enforcement of a law which imposes a pecuniary penalty;
(iii) for the protection of the interests of the data subject or another person;
(iv) to comply with an obligation imposed by law; or
(v) in the interest of national security; or
(g) compliance is not reasonably practical.

(3) A data controller or data processor shall collect, store or use personal data for a purpose which is lawful, specific and explicitly defined.

Duty to notify.

26. (1) A data controller or data processor shall, before collecting personal data, in so far as practicable, inform the data subject—

(a) rights of data subject specified under Section 23;
(b) the fact that personal data is being collected;
(c) purpose for which the personal data is being collected;
(d) the intended recipient of the data;
(e) contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;
(f) whether the data is being collected pursuant to any law and whether such collection is voluntary or mandatory; and
(g) consequences if any, where the data subject fails to provide all or any part of the requested data

Lawful Processing of personal data.

27. (1) A data controller or data processor shall not process personal data, unless –

(a) the data subject consents to the processing for one or more specified purposes;
(b) the processing is necessary –
(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
(ii) for compliance with any legal obligation to which the controller is subject;
(iii) in order to protect the vital interests of the data subject or another person;
(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(v) the performance of any task carried out by a public authority;
(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;
(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
(viii) for the purpose of historical, statistical or scientific research.

(2) Further processing of personal data shall be in accordance with the purpose of collection.

(3) Where processing operation is likely to result in a high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context and purposes, a data controller or data processor shall, prior to the processing, carry out an impact assessment of the envisaged processing operations on the protection of personal data.

(4) A data controller who contravenes the provisions of section (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five million to imprisonment for a term not exceeding five years.

Conditions for consent.

28. (1)A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of his personal data for a specified purpose.

(2) Unless as provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Processing of personal data relating to a child.

29. (1) Every data controller or data processor shall process personal data of children in a manner that protects and advances the rights and best interests of the child.

(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and parental consent in order to process personal data of children, such mechanisms determined on the basis of—

(a) volume of personal data processed;

(b) proportion of such personal data likely to be that of children;

(c) possibility of harm to children arising out of processing of personal data; and

(d) such other factors as may be specified by the Authority.

(3) The Data Commissioner may appoint as guardian of the child a data controller or processor who—

(a) operate commercial websites or online services directed at children; or

(b) process large volumes of personal data of children.

(4) A guardian appointed under subsection (3) shall be barred from profiling, tracking, or behavioural monitoring of, or targeted advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

(5) Where a guardian appointed under subsection (3)exclusively provides counseling or child protection services to a child, such guardian data may not be required to obtain parental consent as set out under sub-section (2).

Restrictions on processing

30. (1) A data controller or data processor may, at the request of a data subject, restrict the processing of personal data where—

(a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

(b) personal data is no longer required for the purpose of the processing, but the data subject requires the personal data for the establishment, exercise or defence of a legal claim;

(c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

(d) data subject has objected to the processing, pending verification as to whether the legitimate grounds of the data controller or data processor overrides those of the data subject.

(2) Where processing of personal data is restricted under this section –

(a) the personal data shall, unless the data is being stored, only be processed with the data subject's consent or for the establishment, exercise or defence of a legal claim, the protection of the rights of another person or for reasons of public interest; and

(b) the data controller shall inform the data subject before withdrawing the restriction on processing of the personal data.

(3) The data controller or data processor shall implement mechanisms to ensure that time limits established for the rectification, erasure or restriction of processing of personal data, or for a periodic review of the need for the storage of the personal data, is observed.

Automated individual decision making

31. (1) Every data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject.

(2) Subsection (1) shall not apply where the decision is –

(a) necessary for entering into, or performing, a contract between the data subject and a data controller;

(b) authorised by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

(c) based on the data subject's explicit consent.

(3) Any automated processing of personal data intended to evaluate certain personal aspects relating to an individual shall not be based on senstive categories of personal data.

Objecting to processing

32. (1) A data subject has a right to object to the processing of their personal data, unless the data controller or data processor demonstrates compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.

Processing for direct marketing.

33. (1) A data controller or data processor shall not provide, use, obtain, procure personal data of data subject for the purpose of direct marketing without prior consent of the data subject.

(2) A data subject may object to processing of their personal data for such marketing, which includes profiling to the extent related to direct marketing.

(3) Where a data subject objects to processing for the purpose of direct marketing, the personal data shall no longer be processed for that purpose.

(4) In this section, "direct marketing" means the communication of any advertising or marketing material which is directed to any particular individual.

Right to data portability.

34. (1) A data subject has the right to receive personal data concerning them, which the data subject has provided to a data controller or data processor, in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit the data obtained under subsection (1), to another data controller or data processor without any hindrance.

(3) Where technically possible, the data subject shall have the right to have the personal data transmitted directly from one data controller or processor to another.

(4) The right under this section shall not apply in circumstances where—

(a) processing may be necessary for the performance of a task carried out in the public interest or in the exercise of an official authority; or

(b) it may adversely affect the rights and freedoms of others.

(5) A data controller or data processor shall comply with data portability requests, free of charge and within a period of one month.

(6) The period under subsection (5) may be extended for a further two months where data portability requests are complex or numerous.

Limitation to retention of personal data.

35. (1) A data controller or data processor shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed unless the retention is —

(a) required or authorised by law;

(b) reasonably necessary for a lawful purpose;

(c) authorised or consented by the data subject; or

(d) for historical, statistical or research purposes.

(2) A data controller or data processor shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under subsection (1) in a manner as may be specified at the expiry of the retention period.

Right of rectification and erasure

36. (1) A data subject may, subject to exemptions under this Act, request a data controller or data processor to—

(a) rectify personal data in its possession or under its control that is inaccurate, out-dated, incomplete or misleading; or

(b) erase or destroy personal data that the data controller or data processor is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

(2) Where the data controller has shared the personal data with a third party for processing purposes, the data controller or data processor shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the–

(a) rectification of such personal data in their possession or under their control that is inaccurate, out-dated, incomplete or misleading; or

(b) erasure or destruction of such personal data that the data controller is no longer authorised to retain, irrelevant, excessive or obtained unlawfully.

Security safeguards of personal data.

37. (1) A data controller or data processor shall take the necessary steps to secure the integrity of personal data in their possession or control through the adoption of appropriate, reasonable, technical and organizational measures to prevent—

(a) the loss of, damage to or unauthorised destruction; and

(b) unlawful access to or unauthorised processing of personal data.

(2) To give effect to subsection (1), the data controller or data processor shall take reasonable measures to—

(a) identify reasonably foreseeable internal and external risks to personal data under the persons possession or control;

(b) establish and maintain appropriate safeguards against the identified risks;

(c) the pseudonymisation and encryption of personal data;

(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) verify that the safeguards are effectively implemented; and

(f) ensure that the safeguards are continually updated in response to new risks or deficiencies.

(3) In determining the appropriate security measures referred to in subsection (2), in particular, where the processing involves the transmission of data over an information and communication network, a controller shall have regard to the –

(a) state of technological development available;

(b) cost of implementing any of the security measures;

(c) special risks that exist in the processing of the data; and

(d) nature of the data being processed.

(4) Where a data controller is using the services of a data processor –

(a) the data controller shall opt for a data processor who provides sufficient guarantees in respect of security and organisational measures for the purpose of complying with subsection (1); and

(b) the data controller and the data processor shall enter into a written contract which shall provide that the data processor shall act only on instructions received from the data controller and shall be bound by obligations of the data controller.

(5) Where a data processor processes personal data other than as instructed by the data controller, the data processor shall be deemed to be a data controller in respect of that processing.

(6) A data controller or data processor shall take all reasonable steps to ensure that any person employed by him or acting under his authority, and complies with, the relevant security measures.

Notification of breach of security on personal data.

38. (1) Where there is a breach of security of personal data or there is reasonable ground to believe personal data has been accessed or acquired by unauthorised person, the data controller or data processor , within prescribed period, shall—

(a) notify the Data Commissioner; and

(b) subject to subsection (3), communicate to the data subject, unless the identity of the data subject cannot be established.

(2) Where a data processor becomes aware of a personal data breach, the data processor shall notify the data controller within the prescribed period.

(3) The data controller may delay notification referred under subsection (1) (b), for purposes of prevention, detection or investigation of offences by the concerned public body.

(4) The notification to the data subject shall be in writing and shall be communicated in the prescribed manner.

(5) The notification and communication referred to under subsection (1) shall provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach, including —

(a) description of the nature of the data breach;
(b) description of the measures that the data controller or data processor intends to take or has taken to address the data breach;
(c) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;
(d) where applicable, the identity of the unauthorised person who may have accessed or acquired the personal data.

(6) The notification of a breach of security of personal data shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data;

PART V— GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

Processing of sensitive personal data.

39. Any category of sensitive personal data shall not be processed unless section 27 applies to the processing.

Permitted grounds for processing sensitive personal data

40. (1)Without prejudice to section 38, sensitive personal data of a data subject may be processed where—

(a) the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that—
  (i) the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes; and
  (ii) the personal data is not disclosed outside that body without the consent of the data subject;
(b) the processing relates to personal data which is manifestly made public by the data subject; or
(c) processing is necessary for –

(i) the establishment, exercise or defence of a legal claim;
(ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or
(iii) protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.

Personal data relating to health.

41. (1) Personal data relating to the health of a Data Subject may only be processed—
(a) by or under the responsibility of a professional; or
(b) by a person subject to the obligation of professional secrecy under any enactment.

(2) The health data of a Data Subject under subsection (1) can only be processed when is necessary for—
(a) the purpose of preventive or occupational medicine;
(b) assessment of the working capacity of an employee,
(c) medical diagnosis;
(d) provision of health or social care; or
(e) treatment or the management of health or pursuant to a contract with a health professional.

Offence

42. Any person who contravenes any provision in this part shall commit an offence and be liable, on conviction, to a fine not exceeding five million shillings, or to imprisonment for a period not exceeding five years.

Further categories of sensitive personal data

43. (1) The Data Commissioner may prescribe further categories of personal data which may be classified as sensitive personal data.

(2) Where categories of personal data have been specified as sensitive personal data under subsection (1), the Data Commissioner may specify any further grounds on which such specified categories may be processed, having regard to—
(a) the riskof significant harm that may be caused to a data subject by the processing of such category of personal data;
(b) the expectation of confidentiality attached to such category of personal data;
(c) whether a significantly discernible class of data subjects may suffer significant harm from the processing of such category of personal data; and

(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Data Commisioner may specify other categories of personal data, which require additional safeguards or restrictions.

PART VI —TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Rule as to data centres and servers

44. (1) Every data controller or data processor shall ensure the storage, on a server or data centre located in Kenya, of at least one serving copy of personal data to which this Act applies.

(2) The Cabinet Secretary shall prescribe, based on grounds of strategic interests of the state or on protection of revenue, categories of personal data as critical personal data that shall only be processed in a server or data centre located in Kenya.

(3) Cross-boarder processing of sensitive personal data is prohibited.

Conditions for transfer out of Kenya

45. (1) A data controller or data processor may transfer personal data to another country where—

(a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;

(b) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards;

(c) the transfer is necessary for –

(i) the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest;

(iv) for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Safeguards prior to cross boarder transfer.

46. (1)The Data Commissioner may request a person who transfers data to another country to demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests.

(2) The Data Commissioner may, in order to protect the rights and fundamental freedoms of data subjects, prohibit, suspend or subject the transfer to such conditions as may be determined.

PART VII— EXEMPTIONS

General exemptions.

47. (1) Nothing in this part shall exempt any data controller or data processor from complying with data protection principles relating lawful processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data.

(2) The processing of personal data is exempt from the provisions of this Act if—

(a) exemption is necessary for national security or public order.

(b) disclosure is required by or under any a written law or by an order of the court

(c) the prevention or detection of crime;

(d) the apprehension or prosecution of an offender; or

(e) the assessment or collection of a tax or duty or an imposition of a similar nature

(3) For purpose of subsection (2) (a) a certificate signed by the Cabinet Secretary shall be sufficient evidence of exemption from outlined provisions of this Act.

Journalism, literature and art.

48. (1) The principles of processing personal data shall not apply where—

(a) processing is undertaken by a person for the publication of a literary or artistic material;

(b) data controller reasonably believes that publication would be in the public interest; and

(c) data controller reasonably believes that, in all the circumstances, compliance with the provision is incompatible with the special purposes.

(2) Subsection (1)(b) shall only apply only where it can be demonstrated that the processing is in compliance with any self regulatory or issued code of ethics in practice and relevant to the publication in question.

Research, history and statistics

49. (1) The further processing of personal data for a research purpose in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.

(2) Personal data which is processed for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from the provisions of this Act if—

(a) data is processed in compliance with the relevant conditions; and

(b) results of the research or resulting statistics are not made available in a form which identifies the data subject or any of them.

Exemptions by the Cabinet Secretary

50. The Cabinet Secretary may prescribe other instances where compliance with certain provisions of this Act may be exempted.

PART VIII— ENFORCEMENT PROVISIONS

Complaints to Data Commissioner

51. Where a complaint is made to the Data Commissioner under this Act, the Data Commissioner shall –

(a) investigate the complaint or cause it to be investigated by an authorised officer; and

(b) where the Data Commissioner is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned, notify, in writing, the individual who made the complaint of the decision.

Investigation of complains

52. (1)The Data Commissioner may, for the purpose of the investigation of a complaint, order any person to –

(a) attend at a specified time and place for the purpose of being examined orally in relation to the complaint;
(b) produce such book, document, record or article as may be required with respect to any matter relevant to the investigation, which he is not prevented by any other enactment from disclosing; or
(c) furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(2) Where material to which an investigation relates consists of information stored in any mechanical or electronic device, the Data Protection Commissioner may require the person named to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

(3) A person who, without reasonable excuse, fails or refuses to comply with a notice, or who furnishes to the Data Commissioner any information which he knows to be false or misleading, commits an offence.

Preservation Order.

53. The Data Commissioner may apply to a court for a preservation order for the expeditious preservation of personal data; where there is reasonable ground to believe that the data is vulnerable to loss or modification.

PART IX—FINANCIAL PROVISIONS

Funds of the Office.

54. The funds and assets of the Office shall consist of—
(a) monies allocated by Parliament for purposes of the Office;
(b) any grants, gifts, donations or other endowments given to the Office; and
(c) such funds as may vest in or accrue to the Office in the performance of its functions under this Act or any other written law.

Annual estimates.

55. (1) At least three months before the commencement of each financial year, the Data Commissioner shall cause to be prepared estimates of the revenue and expenditure of the Office for that year.

(2) The annual estimates shall make provision for all the estimated expenditure of the Office for the financial year concerned and in particular shall provide for—
(a) the payment of salaries, allowances and other charges in respect of the staff of the Office;

(b) the payment of pensions, gratuities and other charges in respect of retirement benefits which are payable out of the finances of the Office;
(c) the acquisition, maintenance, repair and replacement of the equipment and other movable property of the Office; and
(d) funding of training, research and development of activities of the Office;
(e) the creation of such reserve funds to meet future or contingent liabilities or in respect of such other matters as the Data Commissioner may deem fit; and
(f) any other expenditure for the purposes of this Act.

(2) The annual estimates shall be submitted to the Cabinet Secretary for tabling in parliament

Accounts and Audit.

56. The annual accounts of the Office shall be prepared, audited and reported in accordance with the provisions of Articles 226 and 229 of the Constitution, the Public Finance Management Act 2012, or any other law relating to audit of public entities.

Annual reports.

57. (1) The Data Commissioner shall, at the end of each financial year cause an annual report to be prepared.

(2) The Data Commissioner shall submit the annual report to the Cabinet Secretary and the Parliament three months after the end of the year to which it relates and publicise it.

(3) The annual report shall contain in respect of the year to which it relates—
(a) the financial statements and description of activities of the Office;
(b) such other statistical information as the Data Commissioner may consider appropriate relating to the Data Commissioner's functions;
(c) the impact of the exercise of any of Data Commissioner's mandate or function;
(d) any impediments to the achievements of the object and purpose of this Act or any written law; and
(e) any other information relating to its functions that the Data Commissioner may consider necessary

PART X— OFFENCES AND MISCELLANEOUS PROVISIONS

Unlawful disclosure of personal data.

58. (1) A data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such data has been collected commits an offence.

(2) A data processor who, without lawful excuse, discloses personal data processed by the data processor without the prior authority of the data controller commits an offence.

(3) Subject to subsection (4), a person who –

(a) obtains access to personal data, or obtains any information constituting such data, without prior authority of the data controller or data processor by whom the data is kept; or

(b) discloses personal data to third party, shall commit an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor acting within the scope of such mandate.

(5) A person who offers to sell personal data where such personal data has been obtained in breach of subsection (1) commits an offence and is liable, on conviction, to a fine not exceeding five million or to a term of imprisonment for a period not exceeding five years or both.

(6) For the purposes of subsection (5), an advertisement indicating that personal data is or may be for sale constitutes an offer to sell the personal data.

General penalty.

59. (1) A person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall, on conviction, is liable to a fine not exceeding five million or to an imprisonment term not exceeding five years or both.

(2) In addition to any penalty referred to in subsection (1), the Court may –

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of an offence; or

(b) order or prohibit the doing of any act to stop a continuing contravention.

Codes, guidelines and certification.

60. (1) The Data Commissioner may, for the purpose of this Act—

(a) issue Guidelines or Codes of Practice for the data controllers, data processors and data protection officers; and

(b) offer data protection certification standards and data protection seals and marks in order to encourage compliance of processing operations with this Act;

(2) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.

(3) The Cabinet Secretary may prescribe regulations for to govern the certification program.

Regulations.

61. The Cabinet Secretary may make Regulations for the better carrying into effect the provisions of this Act to provide for –

(a) the requirements which are imposed on a data controller or data processor when processing personal data;

(b) the contents which a notice or registration by a data controller or data processor should contain;

(c) information to be provided to a data subject and how such information shall be provided;

(d) the levying of fees and taking of charges;

(e) issuing and approval of Codes of Practice and Guidelines; or

(f) any other matter that the Cabinet Secretary may deem fit.

Consequential amendments.

62. The laws specified under the Second Schedule are amended in a manner specified.

FIRST SCHEDULE (s.14)

I, ...……, make oath/solemnly affirm/declare that I will faithfully and honestly fulfil my duties as authorised officer/Data Protection Commissioner in conformity with the Data Protection Act, 2018 and that I shall not, without the due authority in that behalf,

disclose or make known any matter or thing which comes to my knowledge by reason of discharge of my duties.

……
Magistrate/Judge

SECOND SCHEDULE (s.62)
CONSEQUENTIAL AMENDMENTS

Written Law	***Amendment***
Registration of persons Act CAP 107 (the Act)	• The Act is amended by introducing the following new section immediately after Section 2— *"2A. The principles of personal data protection set out in the Data protection Act 2018 shall apply with necessary modifications to the processing of personal data under this Act"*
Births and Deaths Act (CAP 149) (the Act)	• Section 7 of the Act is amended by introducing the following new subsection immediately after subsection (3)— *"(3)The Register shall be maintained in accordance with the principles of data protection set out in the Data Protection Act, 2018"*
Capital Markets Act (CAP 485A) (the Act)	• Section 11 of the Act is amended in subsection 3 by inserting the following new paragraph immediately after paragraph v— *"vv. ensure processing of personal data in the operations of capital markets is in accordance with principles set out under the Data Protection Act 2018"*

Access to Information Act (Act No 31 of 2016) (The Act)	**1.** The Act is amended in section 2 by— (a) Inserting a the following new definition in appropriate chronological order *"Data Commissioner" means a Data Protection Commissioner established under the Data Protection Act, 2018"* (b)deleting the definition of the word "*Commission"* **2.** The Act is amended by deleting the word *"Commission"* wherever it appears and substituting therefor the expression *"Data Commissioner"*

KINDLY GIVE YOUR SUBMISSIONS ON LAWS LIKELY TO BE AFFECTED BY THIS DRAFT LEGISLATION

MEMORANDUM OF OBJECTS AND REASONS

The Principle object of the Bill is to govern the enforcement of Article 31 of the Constitution of Kenya on the Right to Privacy and particularly sub-article 31 (c) and (d), by setting out the requirements for the protection of Personal Data processed by both Public and Private Entities as a facet to the right to privacy.

The Bill also seeks to outline the key principle that shall govern the processing of Personal Data by both public and private entities, while outlining the rights of Data Subjects and the duties/ responsibilities of Data Controllers and Data Processors.

The Bill also provides for its jurisdictional scope and applicability scope of the right to Personal Data protection. In terms of Kenyan Data Subjects and Personal Data processed in Kenya and outside Kenya and with limitations to the right.

PART I of the Bill provides for preliminary matters

PART II of the Bill provides for the establishment of the Data Protection Regulator, its powers and functions the appointment of the Data Protection Commissioner and other staff of the regulator.

PART III of the Bill provides for the registration of both Data Controllers and Data Processors; that is the application, duration, cancellation, compliance, Audit and designation of the data protection officer.

PART IV of the Bill sets out the principles for protection of personal data, the rights of data subjects and how they shall be exercised, consent, data portability, retention and rectification of personal data and personal data breach notification.

PART V of the Bill provides for processing of sensitive personal data and archiving of personal data.

PART VI of the Bill provides for the cross-border transfer of personal data.

PART VII of the Bill provides for the exemptions to processing of personal data

PART VIII of the Bill sets out enforcement provisions of how the regulator will exercise the powers granted to it under the Bill.

PART IX of the Bill sets out the financial provisions of the Regulator, annual estimates, accounts and audits and annual reports.

PART X of the Bill sets out offences and various miscellaneous provisions on the regulation of personal data.

Dated the ……, 2018.

JOE MUCHERU,
Ministry of Information,
Communications and Technology.