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.