PROTECTION OF PERSONAL INFORMATION IN THE DIGITAL ERA

1. Introduction

In the digital age, protecting personal information has become increasingly vital. Technological advancements in communication, commerce, and service delivery have led to the widespread collection, storage, and processing of personal data. Consequently, reliance on digital platforms has created significant privacy risks, necessitating a robust legal framework for data protection.

2. What is personal data?

Personal data refers to any information relating to an identified or identifiable natural person. Simply put, it is any information used to identify an individual. Data protection laws further distinguish sensitive personal data to be that which reveals an individual's race, health status, ethnic origin, beliefs, genetic data, biometric data, property details, marital status, and family information (e.g. names of children, parents, or spouse(s)), as well as sex or sexual orientation.

Kenya has taken significant steps to protect personal information by establishing laws, regulations, and institutions governing data protection.

3. Legal framework for protection of personal data

Article 31 of the Constitution of Kenya guarantees the right to privacy. This includes the right not to have information relating to one's family or private affairs unnecessarily required or revealed, and the right to privacy in communications. However, this right is not absolute and may be lawfully limited under reasonable and justifiable circumstances in an open and democratic society.

The Data Protection Act of 2019 was enacted to regulate the collection, processing, storage, and use of personal data. Aligned with international best practices, including the European Union's General Data Protection Regulation (GDPR), the Act aims to enhance transparency, accountability, and the rights of data subjects (identified or identifiable natural persons). It also establishes the Office of the Data Protection Commissioner (ODPC) to oversee data protection compliance in Kenya.

The Data Protection Commissioner ensures compliance with international standards, facilitates cooperation on cross-border data transfers, and enforces data protection laws. The Commissioner has the authority to issue directives, conduct audits, investigate complaints, and impose sanctions on non-compliant organisations.

4. Rights of individuals under the data protection laws

Individuals have several key rights under Kenya's data protection laws:

- *Right to information* – Individuals must be informed about how their personal data is being used, promoting transparency between them and data controllers.
- *Right to access* – Individuals can request access to their personal data held by controllers to understand how it is being utilised.
- *Right to rectification* – Individuals can correct false or misleading personal data.

- *Right to erasure ("Right to be forgotten")* – Individuals can request the deletion of personal data that is no longer necessary for its original purpose or if they withdraw consent.
- *Right to object* – Individuals can object to the processing of their personal data in certain circumstances.
- *Right to data portability* – Individuals can transfer their personal data between different platforms.

5. Role of Data Controllers in data protection and privacy

A data controller is an individual or entity that determines how personal data is collected, processed, stored, and used. The Data Protection Act imposes several key responsibilities on data controllers to safeguard privacy.

- *Data collection:* Data controllers must collect personal data directly from individuals unless exceptions apply, such as when data is publicly available or acquired through consent.
- *Consent:* Personal data collection must be based on freely given, informed, and revocable consent.
- *Notification:* Individuals must be informed about their data subject rights, the purpose of data collection, any third parties involved, and potential consequences of withholding data.
- *Security measures:* Data controllers must implement safeguards to prevent unauthorized access, alteration, or destruction of personal data.

6. Consequences of breaching data privacy laws

The Data Protection Act provides penalties and sanctions for non-compliance, including: -

- *Fines:* Up to Kshs. 3,000,000/= for violations of data protection laws.
- *Operational sanctions:* Suspension of operations or forfeiture of equipment used in data breaches.
- *Legal action:* Victims of data breaches can take legal action against violators to seek damages.

To wrap it up, the protection of personal data is a crucial aspect of privacy rights in the digital era. Kenya's legal framework establishes key safeguards to ensure transparency, accountability, and security in handling personal information. Strengthening enforcement mechanisms and increasing public awareness will further enhance data privacy and protection in Kenya.