Computer Misuse and Cybercrimes Act

Kenya

Data Governance

Definitions of Data:

Data 'means representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.'

Main Focus of Document:

Provides for computer misuse and cybercrimes to be a statutory offence.

Target Beneficiaries or Sectors:

n/a

Key Elements:

Provides criminal sanctions for the misuse of computer systems or data and abuse of electronic means of completing transactions and to facilitate the investigation and prosecution of cybercrimes.

Key details include: 3. The objects of this Act are to: (a) protect the confidentiality, integrity and availability of computer systems, programs and data; (b) prevent the unlawful use of computer systems; (c) facilitate the prevention, detection, investigation, prosecution and punishment of cybercrimes; (d) protect the rights to privacy, freedom of expression and access to information as guaranteed under the Constitution; and (e) facilitate international co-operation on matters covered under this Act.

4. Establishment of the National Computer and Cybercrimes Co-ordination Committee.

5. (1) A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both. (2) Access by a person to a computer system is unauthorised if— (a) that person is not entitled to control access of the kind in question to the program or data; or (b) that person does not have consent from any person who is entitled to access the computer system through any function to the program or data. (3) For the purposes of this section, it is immaterial that the unauthorised access is not directed at— (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer system.

6. (1) A person who commits an offence under section 14 with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person, commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding ten years, or to both.

7. (1) A person who intentionally and without authorisation does any act which causes an unauthorised interference, to a computer system, program or data, commits an offence and is liable on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

8. (1) A person who intentionally and without authorisation does any act which intercepts or causes to be intercepted, directly or indirectly and causes the transmission of data to or from a computer system over a telecommunication system commits an offence and is liable, on conviction, to a fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

9. (1) A person who intentionally inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible commits an offence and is liable, on conviction, to fine not exceeding ten million shillings or to imprisonment for a term not exceeding five years, or to both.

Consent Data Data privacy Data transfer or transmission

Policy/regulation mirrored:

Cybercrime Acts/Bills

Countries:

Jamaica