CYBERSECURITY ASSESSMENT REPORT
KENYA
6. KENYA

Regional Economic Community: East African Community (EAC)
Population: 52,214,791
Internet Penetration: 46,870,422 users i.e. 89.9% of the population
AUCC Ratification Status: N/A

6.1. OVERVIEW

DATA PROTECTION: Kenya has a data protection law (the Data Protection Act, 2019). Kenya has a Policy and Regulatory Framework for Privacy and Data Protection, as well as various other ICT Policies. The Office of the Kenyan Data Commission has been established.

ELECTRONIC TRANSACTIONS: Kenya has a law governing electronic data (The Kenya Information and Communications Act, 2015 – as amended), Electronic Transactions Regulations, 2016 and a draft Information and Communications (Electronic Transactions) Bill, 2018. Kenya has a Whitepaper on Facilitation And Adoption of E-Commerce Via The Postal/Courier Networks and a National ICT Policy and Masterplan. The Communications Authority of Kenya is empowered to authorise an entity to provide electronic certification services in Kenya. Kenya also has an ICT Authority and a Root Certification Authority.

CYBERCRIME AND CYBERSECURITY: Kenya has a cybercrimes law (The Computer Misuse and Cybercrimes Act of 2018), as well as a Draft Critical Infrastructure Bill, 2015. Kenya has a National Cyber Security Strategy (2014) and a Critical Infrastructure Information Policy, 2016 in addition to other policies. Kenya has a CERT (KE-CIRT/CC), a National Computer and Cybercrimes Co-Ordination Committee and a ICT Authority. A Critical Infrastructure Protection Committee and a Critical Infrastructure Protection Unit will be established under the Draft Critical Infrastructure Bill.

6.2. DATA PROTECTION

6.2.1. Overview of Data Protection Legislation

At a Constitutional level, Article 31 of the Kenyan Constitution specifically protects the right to privacy. Thereunder, all persons have the right to privacy, including the rights not to have information relating to their family or private affairs unnecessarily required or revealed (Section 31(c)); or the privacy of their communications infringed (Section 31(d)).

Previously (up until November 2019), personal data protection in Kenya was not governed by a dedicated data protection law (despite two Data Protection Bills having been submitted to Kenya’s Senate, and Parliament, respectively). Instead, the confidentiality of data was catered for under a patchwork of sectoral laws. For example (KICTAnet, 2019):

- Personal financial information is protected through confidentiality requirements under the Kenya Banking Act, Credit Reference Bureau Regulations and Capital Markets Act;
- The Kenya Access to Information Act and the Public Archives and Documentation Service Act also have internal protections for the safeguarding of personal information; and
- The Kenya Information and Communications Act (KICA); the Kenya Information and Communications (Amendment) Bill, 2019; Private Security Regulation Act; and the Elections (Technology) Regulations, 2017 also cater for protection of personal data in certain instances.

The Data Protection Act, 2019

It is positive to note that on 8 November 2019 the Kenyan Data Protection Act, 2019 was signed into law (“the DPA”). The DPA codifies the right to privacy enshrined under Article 31 of the Kenyan Constitution.

The Office of the Kenyan Data Commission is established under Section 5 of the DPA, whereas its functions and powers are set out under Sections 7 and 8. Interestingly, unless an exception applies under the DPA, all Data Controllers and Data Processors are to be registered with the Kenyan Data Commissioner – as per Section 21 of the DPA.

Obligations on Data Controllers are listed under Part IV of the DPA and include:

- a duty to notify under (Section 29);
- mandatory data protection impact assessments under certain circumstances (Section 31); and
- the implementation of appropriate technical and organisational measures which are designed to implement the data protection principles effectively, and to integrate necessary safeguards for that purpose into the processing.
The DPA does not, however, contain a direct confidentiality obligation for Data Controllers and Data Processors. Instead, confidentiality and security obligations are contained indirectly under the duty to notify where data controllers are required to provide data subjects with “a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data”. Further, Section 25(a) of the Bill requires every data controller and data processor to “process personal data in accordance of the right of privacy of the data subject”.

Data retention requirements are provided for under Section 39.

The basic principles governing the processing of personal data are listed under Section 25 and require that personal data be:

- (a) processed in accordance with the right to privacy of the data subject;
- (b) processed lawfully, fairly and in a transparent manner;
- (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) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

The general principles and obligations for processing personal data are contained within Chapter IV of the DPA. Thereunder, data collection requirements, notification duties, lawful bases for the processing of personal data, and conditions for consent and regulated amongst other things.

The appointment of a data protection officer is envisaged under the DPA; however, it is voluntary and not mandatory.

Data Subject rights provided for under the DPA include:

- The right to be informed - Section 26(a);
- The right of access - Section 26(b);
- The right to object - Section 26(c);
- The right to correction of false or ‘misleading’ data - Section 26 (d);
- The right to deletion of false or ‘misleading’ data - Section 26 (3);
- The right to request the restriction on the processing of data – Section 34;
- The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject – Section 35; and
- The right to data portability (sustainability of data) – Section 38.

Worryingly, the right to correction and deletion of data is limited to ‘misleading’ data. This may be argued to confer an unreasonable onus on Data Subject’s to prove that data is ‘misleading’.

The processing of special/sensitive personal data is regulated under Chapter V (Sections 44-47). Thereunder, a general prohibition on the processing of sensitive personal data exists. However, the prohibition ceases to exist where any of the grounds for lawful processing under Section 25 of the DPA are present, or where permitted grounds for the processing of sensitive personal data exist under Section 45.

Furthermore, Section 33 of the DPA regulates the processing of personal data belonging to children, requiring that:

- consent is given by the child’s parent or guardian – Section 33(1)(a);
- the processing is in such a manner that protects and advances the rights and best interests of the child – Section 33(1)(b); and
- appropriate mechanisms for age verification and consent in order to process personal data of a child be incorporated – Section 33(2)-(3).

Finally, exemptions for the processing of personal data are contained under Part VII (Sections 51-55):

- General exemptions are provided for under Section 51;
- Journalism literature and art under Section 52;
- Research, history and statistics under Section 53;
- Exemptions by the Data Commissioner under Section 54; and
- Data-sharing code under Section 55.

**International Conventions**

Kenya has signed/ratified the following internal legal instruments:

- the Universal Declaration of Human Rights (UDHR) (signed); and
- the International Covenant on Civil and Political Rights (ICCPR) (ratified).
6.2.2. Data Protection Policy Developments

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 will give effect to Article 31 of the Constitution of Kenya, by presenting legislative proposals and recommendations for stakeholder consultation with the object of developing the draft policy and legislation for privacy and data protection. (Privacy International, 2019). The primary objectives of the policy are to:

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

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

- 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;

- establish the required institutional framework for privacy and data protection; and

- protect children and vulnerable groups.

Other notable policy instruments relating to data protection and privacy are:

- ICT Authority Strategic Plan (2013-2018) – Roadmap for the transformation of Government ICT services;

- National ICT Masterplan (2014-2017) – Blueprint towards transforming Kenya into a digital economy and regional ICT hub; and

- The National ICT Policy.

6.2.3. Data Protection Institutional Measures

The following institutions are relevant to Data Protection in Kenya:

- The Kenyan Data Protection Commissioner: The Commissioner will be responsible for enforcing the provisions of Kenya’s future data protection law.

- The Data Protection Taskforce: The Taskforce was appointed by the Cabinet Secretary to formulate the Kenyan Privacy and Data Protection Policy.

6.3. CYBERCRIME AND CYBERSECURITY

6.3.1. Overview of Cybercrime and Cybersecurity Legislation

Cyber security and crimes associated therewith in Kenya are primarily governed by the following laws/legal instruments:

- The Computer Misuse and Cybercrimes Act of 2018 (the “Cybercrimes Act”);

- The Draft Information Communications (Cyber-security) Regulations 2016 (“the Cybersecurity Regulations”);

- The Draft Critical Infrastructure Bill, 2015 (the “CIB”)

- The Kenya Information Communication Act, 2012 (the “KICA”) and the Regulations thereto; and

- The Kenyan Penal Code.

The KICA Act

The KICA and its regulations had criminalised several cybercrimes. Its provisions have been now been superseded by the Cybercrimes Act.

The Cybercrimes Act

The Cybercrimes Act was introduced as the primary legislation establishing a statutory cyber authority and criminalising cyber offences. The Act repealed various provisions from the KICA. Before detailing its provisions below, it is imperative to note that on 29 May 2018, the High Court of Kenya issued a conservatory order suspending the entry into force of 26 sections of the Cybercrimes Act – these are Sections: 5, 16, 17, 22, 23, 24, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 46, 49, 50, 51, 52 & 53. The judgment on the constitutionality of the Computer Misuse and Cybercrimes Act 2018 was initially set to be heard on 30th January 2020 (Itimu, 2019). However, judgment in the matter was postponed for a second time to 20 February 2020. On 20 February 2020, Judge James Makau of the Kenyan High Court declared the Cybercrimes Act constitutional in its entirety (Shiwalo and Vilita, 2020).

Part II of the Cybercrimes Act establishes the National Computer And Cybercrimes Co-Ordination Committee (the “NCACCC”) whose functions include designating certain systems as ‘critical infrastructure’ (Section 9) under certain circumstances - listed in Section 9(2). The NCACCC is also responsible for regulating the minimum physical and technical security measures that must be implemented to protect critical information infrastructure. The NCACCC has statutory authority and legal capacity to conduct investigations and enforce the provisions of the Cybercrimes Act – in terms of Part IV of the Cybercrimes Act.
Part III of the Cybercrimes Act sets out a vast range of cyber offences between Sections 14-46 (32 cyber offences in total). The range of offences adapts certain sanctions and offences to Information and Communication Technologies—these include:

- The fraudulent use of electronic data (Section 37) which is widespread enough to include the causing of damage to intellectual property in an electronic form;
- Issuance of false e-instructions (Section 39);
- Employee responsibilities to relinquish access codes (Section 41); and
- Cybersquatting (Section 27) and Cyber Harassment (Section 28).

Lastly, Part V of the Cybercrimes Act lays the ground for international cooperation in tackling cyber-crimes. And it sets up a crime reporting database. Any person who has information about a threat, attempt or actual cyber-attack is now legally obliged to share this with the database within 24 hours of the incident. If they don’t, they’re liable for a fine or could be jailed for up to two years.

The Cybercrimes Act has been criticised for having the potential to prejudice citizens and curb freedom of expression due to poorly defined offences such as that of ‘fake publications’.

**The Cybersecurity Regulations**

The Cybersecurity Regulations provides for various cyber offences and cyber penalties. However, in light of the Cybercrimes Act, the 2016 Cybersecurity Regulations have been superseded.

**The CIB**

On 27th March 2015, the then Cabinet Secretary in the Ministry of Information and Communications Dr Fred Matiang’i appointed a task force to formulate the Critical Infrastructure Policy, 2016 and the CIB. The CIB is a dedicated Bill providing for the protection of critical infrastructure in Kenya.

### 6.3.2. Cybercrime and Cybersecurity Policy Developments

The primary policy developments relating to cybersecurity and cybercrime in Kenya are:

- The Critical Infrastructure Information Policy, 2016; and
- Vision 2030;

The National Cyber Security Strategy (2014) is in direct support of the national priorities and ICT goals defined in Vision 2030—one of which is to enhance cybersecurity to reduce the risk of cyber-attacks and create a more secure network. The Strategy also defines Kenya’s cybersecurity vision, key objectives, and ongoing commitment to support national priorities by encouraging ICT growth and aggressively protecting critical information infrastructures.

The task force established by the erstwhile Cabinet Secretary in the Ministry of Information and Communications, Dr Fred Matiang’i, have begun a draft Policy Framework for the Protection of Critical Infrastructure.

According to Fred Matiang’i, Ministry of Internal Security, “efforts are underway to harmonize the state’s Policy and Legal Framework on Cybersecurity with global instruments. In addition, the ICT Policy, National Cybersecurity Strategy, and other legislative platforms are under keen review to match their global counterparts in terms of best practices and standards. This statement can be referenced by an earlier suggestion by the ICT Ministry that tasked legislators to include GDPR-like clauses in the Data Protection Bill that is still under deliberations in Parliament” (Abuya, 2019).

### 6.3.3. Cybercrime and Cybersecurity Institutional Measures

The focal cybersecurity and cybercrime institutional measures in Kenya are:

- The National Computer and Cybercrimes Co-Ordination Committee (described above);
- The Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC): coordinates computer-related incidences in the country;
- The Kenyan ICT Authority (ICTA); and
- If passed as law, the CIB will create the Critical Infrastructure Protection Committee and a Critical Infrastructure Protection Unit.

### 6.4. ELECTRONIC COMMERCE

#### 6.4.1. Overview of Electronic Commerce Legislation

Electronic communications and transactions (in the context of electronic commerce) in Kenya are primarily governed by:

- The Kenya Information and Communications Act, 2015 (“KICA”);
- The Draft Information and Communications (Electronic Transactions) Regulations 2016 (the “ET Regulations”); and
- The DPA (described under Data Protection above).
KICA

At the outset, it is interesting to highlight that the term 'electronic transaction' is not defined under the KICA. However, the terms “data”, “electronic” and “electronic form” are defined which may be coupled to cater for electronic transactions.

Part II of the KICA establishes the Communications Authority of Kenya (the “CA”). Part VI-A of the KICA contains provisions relating to electronic transactions. Thereunder, the CA has statutory functions to guarantee the security of electronic transactions which include:

- “facilitate electronic transactions... by ensuring the use of reliable electronic records” - Section 83C(1)(a);
- “facilitate electronic commerce and eliminate barriers to electronic commerce such as those resulting from uncertainties over writing and signature requirements” - Section 83C(1)(b); and
- “[fostering] the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium” - Section 83C(1)(d).

Electronic Contracts: Section 83J of KICA states that an offer and acceptance may be expressed by means of electronic messages. Thus, where electronic messages are used in the formation of a contract, the contract shall not be denied validity or enforceability solely on the ground that an electronic message was used.

Importantly, Section 83B states that the creation or execution of a will; negotiable instruments; and documents of title may not be concluded electronically.

Electronic Certificates and Signatures: Section 83E of the KICA empowers the CA to authorise an entity to provide electronic certification services. On this note, electronic writing is given legal recognition under Section 83G of the KICA. Electronic signatures are given legal recognition under Section 83P and electronic messages and the parties to these messages are given legal recognition under Section 83K.

Electronic Advertising: Electronic advertising is partially catered for under the KICA. Thereunder, responsibilities on ‘broadcasters’ (TV/Radio providers) include “[ensuring] that advertisements, either in terms of content, tone or treatment, are not deceptive or are not repugnant to good taste”.

The ET Regulations

Contractual liability for providers who provide goods/services by electronic means is established under the ET Regulations. Unfortunately, a copy of these Regulations is not available in the public domain at the time of writing.

The DPA

Direct marketing is not regulated under the KICA. Instead, the DPA regulates direct marketing under Section 37.

6.4.2. Electronic Commerce Policy Developments

The following policies and strategies apply to electronic commerce and electronic transactions in Kenya.

- ICT Authority Strategic Plan (2013-2018) – Roadmap for the transformation of Government ICT services;
- National ICT Masterplan (2014-2017) – Blueprint towards transforming Kenya into a digital economy and regional ICT hub; and
- The National ICT Policy.

The Whitepaper On Facilitation And Adoption Of E-Commerce Via The Postal/Courier Networks was developed by the Kenyan CA in 2015. The Whitepaper was developed "developed with a view to developing an appropriate framework that will promote the adoption of e-commerce via the post" (Communication Authority, 2015). The Whitepaper canvassed the concept of e-commerce, looked at various case studies, identified lessons learnt and inhibiting growth factors in Kenya, and provided intervention measures to promote the adoption of e-commerce in Kenya.

The Digital Economy Blueprint: seeks to provide a conceptual framework adopted by Kenya in its quest towards the realisation of a successful and sustainable digital economy. The Blueprint acknowledges e-commerce as a rationale for digital business and considers actions to be taken to grow and streamline the adoption of e-commerce in Kenya.
6.4.3. Electronic Commerce Institutional Measures

The following institutions play a fundamental role in Kenya’s e-commerce:

- The Ministry of ICT (MoICT): which is responsible for formulating, administering, managing and developing information, communications and broadcasting policies in Kenya;

- The National Communications Secretariat (NCS): which advises the MoICT on ICT policy;

- The Directorate of e-Government (DeG);

- The Parliamentary Committee on Communications Information and Innovation;

- The Communications Authority of Kenya; and

- The Root Certification Authority (RCA);

- The Government Certification Authority (GCA); and

- The ICT Authority (ICTA): responsible for the management of the mainstream government ICT services, and which operates the GCA.
6.5. COMPARISON WITH THE AUCC PROVISIONS ON LAWS, POLICIES AND INSTITUTIONS FOR DATA PROTECTION, CYBERCRIME AND ELECTRONIC TRANSACTIONS.

<table>
<thead>
<tr>
<th>Policy and Governance Measures</th>
<th>Legislative and Regulatory Measures</th>
<th>Institutional Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cybersecurity Policy which recognises the Critical Information Infrastructure and identifies the risks to the nation and mitigation measures</strong></td>
<td><strong>Data Protection Laws and Regulations</strong>&lt;br&gt;The Data Protection Act, 2019.</td>
<td><strong>Data Protection Authority whose responsibilities in regulating data protection include authorisation of data processing, authorisation of cross border transfers of personal data</strong>&lt;br&gt;The Kenyan Data Protection Commissioner.</td>
</tr>
<tr>
<td><strong>The Critical Infrastructure Information Policy, 2016;</strong></td>
<td><strong>Electronic Commerce Laws and Regulations</strong>&lt;br&gt;Primarily governed by The Kenya Information and Communications Act, 2015; And The Data Protection Act, 2019.</td>
<td><strong>Electronic Signature Accreditation Authority that will regulate what constitutes a qualified electronic signature for the purposes of authenticating electronic records and other applications</strong>&lt;br&gt;The Communications Authority of Kenya (the “CA”).</td>
</tr>
<tr>
<td><strong>In draft is a Policy Framework for the Protection of Critical Infrastructure.</strong></td>
<td><strong>Cybercrime Laws and Regulations</strong>&lt;br&gt;Primarily governed by the Computer Misuse and Cybercrimes Act of 2018; And The Kenya Information Communication Act, 2012; The Kenyan Penal Code.</td>
<td><strong>State Department to regulate and approve electronic commerce payment methods, only approved payment methods may be validly used in the Member State territory;</strong></td>
</tr>
<tr>
<td><strong>National Cybersecurity strategy to implement the Policy</strong></td>
<td><strong>In draft is the Draft Information Communications (Electronic Transactions) Regulations 2016.</strong></td>
<td><strong>State Department to regulate vulnerability and safety guarantee assessments of ICT product vendors including ensuring mandatory disclosures of vulnerabilities and the solutions to such vendors consumers</strong></td>
</tr>
<tr>
<td><strong>The primary policy developments are National Cyber Security Strategy (2014); and Vision 2030.</strong></td>
<td><strong>If passed as law, the Draft Critical Infrastructure Bill, 2015 (the “CIB”) will create the Critical Infrastructure Protection Committee and a Critical Infrastructure Protection Unit.</strong></td>
<td><strong>Institutions with the statutory authority and legal capacity to respond to cyber security incidents, co-ordination and co-operation for (cybersecurity) restorative justice, forensic investigations, cybersecurity prosecution</strong>&lt;br&gt;The National Computer and Cybercrimes Co-Ordination Committee; and The Kenyan ICT Authority (ICTA).</td>
</tr>
<tr>
<td><strong>Public-private partnerships to engage industry, civil society, and academia in the promotion and enhancement of a cybersecurity culture</strong></td>
<td></td>
<td><strong>Institutions responsible for national and cross-border co-ordination of cybersecurity problems as well as global co-operation.</strong>&lt;br&gt;The Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC)</td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td><strong>Institutions that exchange information on cyber threats and vulnerability assessments such as the Computer Emergency Response Teams (CERTs)</strong>&lt;br&gt;The Kenya Computer Incidence Response Team and Coordination Centre (KE-CIRT/CC)</td>
</tr>
</tbody>
</table>

**Table 13: Kenya National Assessment Overview**

KENYA
Disclaimer

This report was prepared independently by EndCode.

This report is based on a variety of inputs from multiple sources including official and private data sources such as public and governmental institutions, international organisations, academic research, news articles, sector reports and interviews with various stakeholders.

Accuracy of analysis and recommendations provided are dependent on the detail and accuracy of available and declared data. The information given herein is for informal guidance only and neither AUDA-NEPAD nor EndCode, nor any company or organisation stated within this paper makes any expressed or implied warranty, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, or process disclosed.

AUDA-NEPAD nor EndCode bear no responsibility for any use that may be made of this report. Should you have any queries about the content within this report, please contact AUDA-NEPAD.

About EndCode

EndCode is a specialist advisory firm - servicing local, regional and international organisations navigating technology laws and policies in Africa. EndCode believes that it can promote access to the benefits of technology and innovation on the continent by growing the body of insights available in technology law and policy areas. EndCode is distinguished by its multidisciplinary expertise in law, policy, research and advocacy in the technology environment.