WAMAE & ALLEN
Advocates Commissioners for Oaths Notaries Public and Patent Agents

Jurisdiction	KENYA
Date	11TH NOVEMBER 2022
Law Firm	WAMAE & ALLEN ADVOCATES
Name and Position of the person in charge	CHARLES W. WAMAE – MANAGING PARTNER KENNEDY KITHINJI – SENIOR ASSOCIATE VIRGINIAH N. GICHUHI – PRINCIPAL ASSOCIATE
Contact Information	Charles@wamaeallen.com; Kennedy@wamaeallen.com; Virginiah@wamaeallen.com;

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

"Yes." Generally, the Constitution of Kenya 2010 has a general provision granting rights to privacy, however, in respect of regulation of personal data, the main laws regulating Data Protection legislation are the Data Protection Act, 2019 and the Data Protection Regulations 2021.

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

"Yes" as stated above, The Constitution of Kenya 2010; The Data Protection Act 2019 and the Data Protection Regulations 2021 are the laws regulating Data Protection.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

"Yes"

Presently, protection of personal information is codified in various statutes and the Constitution of Kenya (2010). The statutes being: -

a) The Data Protection Act, No. 24 of 2019 and Regulations thereto;
b) The Access to Information Act, No. 31 of 2016; and
c) The Evidence Act, No. 22 of 2022.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I... (please add a reply column as necessary,)

The title of the law ： THE DATA PROTECTION ACT, NO. 24 OF 2019

① The definition of "Personal Information"	Section 2 of the Data Protection Act defines "**personal data**" as, "any information relating to an identified or identifiable natural person"
② The scope in which the law applies	The Data Protection Act has a mandate over private, public and individual. The Act defines **"data controller (DC)"**as 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. The Act defines **"data processor (DP)"** to mean a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller Further, the Act defines **"processing"** to mean 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, organization, structuring; (b)storage, adaptation or alteration; (c)retrieval, consultation or use; (d)disclosure by transmission, dissemination, or otherwise making available; or (e)alignment or combination, restriction, erasure or destruction.
③ The territorial scope	The Data Protection Act covers both local and international data processing. Section 4 (b) of the Act provides as follows: - "This Act applies to the processing of personal data by 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 processing personal data of data subjects located in Kenya."
④ URL (please provide the URL officially posted by the government,	http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019#part_I

English page is preferred, if available)	
⑤ The **effective** date *	25th November, 2019

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：ACCESS TO INFORMATION ACT, No. 31 OF 2016

① The definition of "Personal Information"	The Access to Information Act in section 2 defines "personal information" as information about an identifiable individual, including, but not limited to— (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, age, physical, psychological or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual; (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; (c) any identifying number, symbol or other particular assigned to the individual; (d) the fingerprints, blood type, address, telephone or other contact details of the individual; (e) a person's opinion or views over another person; (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) any information given in support or in relation to an award or grant proposed to be given to another person; (h) contact details of an individual.
② The scope in which the law applies	The Act covers both public and private sectors. Section 3(b) of the Act provides as follows: "The object and purpose of this Act is to provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information on request in line with the constitutional principles"
③ The territorial scope	KENYA
④ URL (please provide the URL officially posted by the	http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2031%20of%202016

government, English page is preferred, if available)	
⑤ The **effective** date*	21st September 2016

* If the law has been amended, please fill in the effective date of the amended law.

The title of the law ：EVIDENCE ACT, NO. 22 of 2022

① The definition of "Personal Information"	N/A
② The scope in which the law applies	Privileged advocate-client communication
③ The territorial scope	KENYA
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%2080
⑤ The **effective** date*	8th December 1963

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtran

sborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Section 25 of the Data Protection Act provides for this principle under Sub-sections:

a. that every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject and;

b. that every data controller or data processor shall ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to any data subject;

c. that every data controller or data processor shall ensure that personal data is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

…

e. that every data controller or processor shall ensure that personal data is collected only where a valid explanation is provided whenever information relating to family or private affairs is required.

Additionally, Section 39 of the Data Protection Act, ensures that Data Controllers/Data processors shall only retain personal data only as long as may be reasonably necessary to satisfy purpose for which it is processed unless the retention is authorized by law, reasonably necessary for a lawful purpose, authorized/ consented by data subject or for historical, statistical, journalistic literature and art/ research purposes. The provision further provides that a DC/DP shall erase delete, anonymize or pseudonymize personal data

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

Section 25 of the Data Protection Act provides for this principle as follows:

(c) that every data controller or data processor shall ensure that personal data

is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(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;

Additionally, the Act has provided that under Section 40 for the right to data subjects for rectification and erasure of data to ensure its accuracy.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Section 29 (c) of the Data Protection Act, provides that a data controller or data processor shall, **before** collecting personal data, in so far as practicable, inform the data subject of the purpose for which the personal data is being collection.

Section 25 of the Data Protection Act provides for this principle under Subsection c & d as follows:

c. that every data controller or data processor shall ensure that personal data is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes

d. that every data controller or data processor shall ensure that personal data is adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

Additionally, Section 30 of the Data Protection Act provides for this principle. It provides for what is lawful processing of personal data by Data Controllers/Data Processors. DC/DPs shall not process personal data (a) unless the data subject consents to one or more specified purposes; or (b) the processing is necessary performance of a contract, for compliance with the law, to protect vital interests that relate to public interest; performance of tasks by a public authority, among others; and (c) Further processing is in accordance with the purpose of the collection;

The same is applicable even in instances of further processing of personal data.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

Section 25 of the Data Protection Act provides for this principle under Subsections c & d as follows:

c. that every data controller or data processor shall ensure that personal data is collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes.

d. that every data controller or data processor shall ensure that personal data is adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

Additionally, Section 39 of the Data Protection Act provides for limitation for of retention of personal data. This ensures that Data Controllers/Data processors shall only retain personal data only as long as may be reasonably necessary to satisfy purpose for which it is processed unless the retention is authorized by law, reasonably necessary for a lawful purpose, authorized/ consented by data subject or for historical, statistical, journalistic literature and art/ research purposes. The provision further provides that a DC/DP shall erase delete, anonymize or pseudonymize personal data

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Section 19(2)(e) of the Data Protection Act places as duty on DC/DPs whilst undertaking their application for registration should provide particulars risk, safeguards, security measures and mechanisms to ensure the protections of personal data.

Section 25 of the Data Protection Act provides for this principle under subsections h;

h. that every data controller or data processor shall ensure that personal data is not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

Section 29 does provide that data controllers and data processors have a duty to notify data subjects of their rights, that data is being collected, the purpose of the collections, transfer of data, description of technical and organisational security measures, that data is being collected pursuant to an law whether manadatory or voluntarily, and consequences of non-compliance by data subject.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

The Access of Information Act of Kenya enables a party the authority to raise such questions seeking to know if they have a DC/DPs holds any data of a particular data subject.

Section 26 of the Data Protection Act further enables an Individual the right to access their personal data in the custody of data controller or data processor.

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

Section 25 of the Data Protection Act provides for the mandatory application of the principles.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.

(a) Collection Limitation Principle
(b) Data Quality Principle
(c) Purpose Specification Principle
(d) Use Limitation Principle
(e) Security Safeguards Principle
(f) Openness Principle
(g) Individual Participation Principle
(h) Accountability Principle

We note that under Sections 51-55 the Data Protection Act has provided general exemptions to its application however the exceptions are in respect of national security or disclosure is under a written law.

Additional, exceptions are given to where the data is used for journalism. Literature, research, history and statistics, exceptions by the Data Commissioner, data sharing codes between government departments or public sector agencies.

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege)** to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

Section 51(2) the act has provided general exemptions to its application however the exceptions are in respect of national security or public interest, and/or disclosure

is under a written law. Also, under Section 54 exceptions by the Data Commissioner who is also deemed as public officer can be issued to particular instance for exception in compliance with the Act.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Name: Office of the Data Protection Commissioner

Address: 30920 Waiyaki Way, Nairobi

Telephone: +254778048164

Website: https://www.odpc.go.ke/

Other information if any: N/A